INFORMATION SECURITY

Patrick McClanahan
San Joaquin Delta College

Information Secuirty

The LibreTexts libraries are Powered by NICE CXone Expert and was supported by the Department of Education Open Textbook Pilot Project, the California Education Learning Lab, the UC Davis Office of the Provost, the UC Davis Library, the California State University Affordable Learning Solutions Program, and Merlot. This material is based upon work supported by the National Science Foundation under Grant No. 1246120, 1525057, and 1413739.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation nor the US Department of Education.

TABLE OF CONTENTS

Licensing

*A detailed breakdown of this resource's licensing can be found in **Back Matter/Detailed Licensing**.*

CHAPTER OVERVIEW

1: Information Security Defined

1.1 Information Security

Information Security

Information security, sometimes shortened to **infosec**, is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or at least reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording or devaluation of information. It also involves actions intended to reduce the adverse impacts of such incidents. Protected information may take any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge). Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity. This is largely achieved through a structured risk management process that involves:

- Identifying information and related assets, plus potential threats, vulnerabilities and impacts;
- Evaluating the risks;
- Deciding how to address or treat the risks i.e. to avoid, mitigate, share or accept them;
- Where risk mitigation is required, selecting or designing appropriate security controls and implementing them;
- Monitoring the activities, making adjustments as necessary to address any issues, changes and improvement opportunities.

To standardize this discipline, academics and professionals collaborate to offer guidance, policies, and industry standards on password, antivirus software, firewall, encryption software, legal liability, security awareness and training, and so forth. This standardization may be further driven by a wide variety of laws and regulations that affect how data is accessed, processed, stored, transferred and destroyed. However, the implementation of any standards and guidance within an entity may have limited effect if a culture of continual improvement isn't adopted.

Definition

Various definitions of information security are suggested below, summarized from different sources:

1. "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009)[3]
2. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010)[4]
3. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008)[5]
4. "Information Security is the process of protecting the intellectual property of an organisation." (Pipkin, 2000)[6]
5. "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDermott and Geer, 2001)[7]
6. "A well-informed sense of assurance that information risks and controls are in balance." (Anderson, J., 2003)[8]
7. "Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties." (Venter and Eloff, 2003)[9]
8. "Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: *confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability.*" (Cherdantseva and Hilton, 2013)[2]
9. Information and information resource security using telecommunication system or devices means protecting information, information systems or books from unauthorized access, damage, theft, or destruction (Kurose and Ross, 2010).

Overview

At the core of information security is information assurance, the act of maintaining the confidentiality, integrity and availability (CIA) of information, ensuring that information is not compromised in any way when critical issues arise. These issues include but are not limited to natural disasters, computer/server malfunction, and physical theft. While paper-based business operations are still prevalent, requiring their own set of information security practices, enterprise digital initiatives are increasingly being emphasized, with information assurance now typically being dealt with by information technology (IT) security specialists. These specialists apply information security to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to acquire critical private information or gain control of the internal systems.

The field of information security has grown and evolved significantly in recent years. It offers many areas for specialization, including securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning, electronic record discovery, and digital forensics. Information security professionals are very stable in their employment. As of 2013 more than 80 percent of professionals had no change in employer or employment over a period of a year, and the number of professionals is projected to continuously grow more than 11 percent annually from 2014 to 2019.

Adapted from:

1.1.1 Information Security vs Cybersecurity

Difference Between Information Security and Cybersecurity

The terms cybersecurity and information security are often used interchangeably.As they both are responsible for security and protecting the computer system from threats and information breaches and often cybersecurity and information security are so closely linked that they may seem synonymous and unfortunately, they are used synonymously.

If we talk about data security it's all about securing the data from malicious user and threats. Another question is that what is the difference between data and information? One important point is data is unformatted, or unorganized information. For example "100798" is data and if we know that it's the date of birth of a person then it is information because it has a context.

CYBER SECURITY	INFORMATION SECURITY
It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized user, access and data modification or removal in order to provide confidentiality, integrity, and availability.
It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with protection of data from any form of threat.
Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Cybersecurity deals with danger against cyberspace.	Information security deals with the protection of data from any form of threat.
Cybersecurity strikes against cyber crimes, cyber frauds and law enforcement.	Information security strives against unauthorized access, disclosure modification and disruption.
On the other hand cyber security professionals with cyber security deals with advanced persistent threat.	Information security professionals is the foundation of data security and security professionals associated with it prioritize resources first before dealing with threats.
It deals with threats that may or may not exist in the cyber realm such as a protecting your social media account, personal information, etc.	It deals with information assets and integrity confidentiality and availability.

Adapted from:
"Difference between Cyber Security and Information Security" by Stranger1, Geeks for Geeks is licensed under CC BY-SA 4.0

1.1.2 Information Security vs Network Security

Information vs Network Security

Network Security

Network Security is the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles large amount of data, has a degree of solutions against many cyber threats.

Cyber Security

Cyber Security is the measures to protect our system from cyber attacks and malicious attacks. It is basically to advance our security of the system so that we can prevent unauthorized access of our system from attacker. It protects the cyberspace from attacks and damages. Cyberspace can be hampered by inherent vulnerabilities that cannot be removed sometimes.

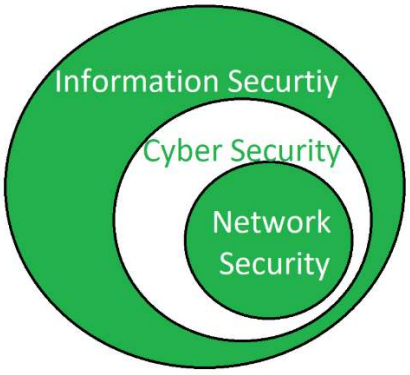


Figure 1: Information vs Cyber vs Netwrok Security. ("3 Security" by pp_pankaj, Geeks for Geeks is licensed under CC BY-SA 4.0)

Difference between Network Security and Cyber Security:

Network Security	Cyber Security
It protects the data flowing over the network.	It protects the data residing in the devices and servers.
It is a subset of cyber security.	It is a subset of information security.
It protects anything in the network realm.	It protects anything in the cyber realm.
It deals with the protection from DOS attacks.	It deals with the protection from cyber attacks.
Network Security strikes against trojans.	Cyber Security strikes against cyber crimes and cyber frauds.
It includes viruses and worms.	It includes phishing and pre-texting.
Network security ensures to protect the transit data only.	Cyber security ensures to protect entire digital data.
It secures the data travelling across the network by terminals.	It deals with the protection of the data resting.

Adapted from:
"Difference between Network Security and Cyber Security" by pp_pankaj, Geeks for Geeks is licensed under CC BY-SA 4.0

1.2 Threats to Information Security

Threats

Information security threats can in many forms: software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. This page contains a great deal of important information. There is a similar article by Cisco that covers these same topics, it may be a bit more up to date. Find it at: "What Is the Difference: Viruses, Worms, Trojans, and Bots?"

A threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

Software attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not the same, the only similarity is that they are all malicious software.

Malware is a combination of 2 terms, Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or a anything that is designed to perform malicious operations on system.

The best-known types of malware, viruses and worms, are known for the manner in which they spread, rather than any specific types of behavior.

1. **Virus –** A computer virus is software usually hidden within another seemingly innocuous program that can produce copies of itself and insert them into other programs or files, and that usually performs a harmful action (such as destroying data).[21] An example of this is a PE infection, a technique, usually used to spread malware, that inserts extra data or executable code into PE files.[22]
2. **Worm** - a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers. When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behavior will continue. Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on the law of exponential growth, thus controlling and infecting more and more computers in a short time. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
3. **Trojan horse** - is a harmful program that misrepresents itself to masquerade as a regular, benign program or utility in order to persuade a victim to install it. A Trojan horse usually carries a hidden destructive function that is activated when the application is started. The term is derived from the Ancient Greek story of the Trojan horse used to invade the city of Troy by stealth.[25][26][27][28][29]

   Trojan horses are generally spread by some form of social engineering, for example, where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a routine form to be filled in), or by drive-by download. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller (phoning home) which can then have unauthorized access to the affected computer, potentially installing additional software such as a keylogger to steal confidential information, cryptomining software or adware to generate revenue to the operator of the trojan.[30] While Trojan horses and backdoors are not easily detectable by themselves, computers may appear to run slower, emit more heat or fan noise due to heavy processor or network usage, as may occur when cryptomining software is installed. Cryptominers may limit resource usage and/or only run during idle times in an attempt to evade detection.

   Unlike computer viruses and worms, Trojan horses generally do not attempt to inject themselves into other files or otherwise propagate themselves.[31]

   In spring 2017 Mac users were hit by the new version of Proton Remote Access Trojan (RAT)[32] trained to extract password data from various sources, such as browser auto-fill data, the Mac-OS keychain, and password vaults.[33]

4. **Bots –** can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need of human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet.**

Malware is referenced by several terms, depending on how it operates within the larger categories specified above. Below is a short description of many of the most well known types of malware.

1. **Adware –** is not exactly malicious but it can breach the privacy of a user. Adware displays ads on computer's desktop or inside individual programs. They often come attached with free software downloaded from a variety os web sites. They monitor the sites the user visits, determines those topics of interest to the user, and then display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
2. **Spyware –** is software that monitors the users activity on computer and provides the collected information to a pre-determined adversary. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they installs themselves and sits silently to avoid detection.
   One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.
3. **Ransomware –** is a type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. A message will be displayed asking for money as ransom in exchange for the key to enable the user to unlock the computer.
4. **Scareware –** masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
5. **Rootkits –** are designed to gain administrative privileges in the user's system. Once administrative access is gained, the adversary access to all data and files, allowing them to veiw, download or destroy whatever the adversary wants.
6. **Zombies –** work similar to Spyware. The infection mechanism is the same but zombies can sit dormant waiting for the adversary to issue commands or perhaps waiting for a specific task to be completed by the user themselves.

No matter what they look like, or how they accomplish their work, malware is intent on disrupting or destroying data. The adversary is interested in one or more of the following:

- **Theft of intellectual property** means violation of intellectual property rights like copyrights, patents etc.
- **Identity theft** means to act someone else to obtain person's personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.
- **Theft of equipment and information** is increasing these days due to the mobile nature of devices and increasing information capacity.
- **Sabotage** means destroying company's website to cause loss of confidence on part of its customer.
- **Information extortion** means theft of company's property or information to receive payment in exchange. For example ransomware may lock victims file making them inaccessible thus forcing victim to make payment in exchange. Only after payment victim's files will be unlocked.

With each day that passes there are new and more malicious threats. Below is the brief description of these new generation threats.

- **Technology with weak security –** With the advancement in technology, new technology gadgets are being released in the market, and most of them provide some sort of networking or remote access capabilities. Very few have any secure built in or have any thought about following information security principles.
- **Social media attacks –** the adversary identifies and infects a cluster of websites that persons of a particular organization visit, allowing the adversary to steal information.
- **Mobile Malware –** the reality is that malware is not limited to desktop/laptop systems. With the plethora of apps that are available from the mobile device app stores, there is a huge opportunity for user's to inadvertently download malware onto their mobile devices..
- **Outdated Security Software –** with new threats emerging everyday, updating a system with the latest patches, especially security patches should be a high priority in order to maintain a fully secured environment.
- **Corporate data on personal devices –** many organizations allow employees to "bring your own device" (BYOD). Devices like laptops, tablets, even the use of USB drives, and cloud storage in the workplace can create serious security breaches.
- **Social Engineering –** is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install a malicious software- that will give them control of your computer. For example

email or message from your friend, that was probably not sent by your friend. Criminal can access your friends device and then by accessing the contact list he can send infected email and message to all contacts. Since the message/ email is from a known person recipient will definitely check the link or attachment in the message, thus unintentionally infecting the computer. There is an AWESOME video example of social engineering - it is only about 3:00 minutes long. (I apologize for the single curse word that is used right at the end of the video)

Adapted from:

1.3 Models of Security - CIA / Parkerian Hexad

CIA Triad

Information security is not only about securing information from unauthorized access. Information security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be anything like your profile on social media, your data in mobile phone, your biometrics etc. Thus information security spans so many areas like cryptography, mobile computing, forensics, online social media etc.

Information Security programs are built around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

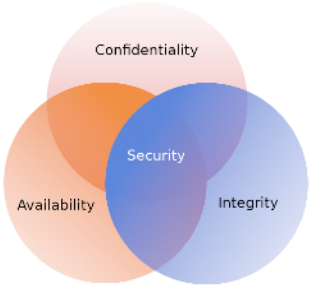


Figure 1: CIA Triad. ("CIA Triad" by Patrick McClanahan is licensed under CC BY-SA 4.0)

These are the objectives which should be kept in mind while working in the information security realm.

Confidentiality

Confidentiality means that only the authorized individuals/systems can view sensitive or classified information. Data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to your information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it. Encryption standards include **AES**(Advanced Encryption Standard) and **DES** (Data Encryption Standard). Another way to protect your data is through a VPN tunnel. VPN stands for Virtual Private Network and helps the data to move securely over the network.

Integrity

The next thing to talk about is integrity. Well, the idea here is making sure that data has not been modified. Corruption of data is a failure to maintain data integrity. To check if our data has been modified or not, we make use of a hash function.

We have two common types : SHA (Secure Hash Algorithm) and MD5(Message Direct 5). Now MD5 is a 128-bit hash and SHA is a 160-bit hash if we're using SHA-1. There are also other SHA methods that we could use like SHA-0, SHA-2, SHA-3.

Let's assume Host 'A' wants to send data to Host 'B' maintaining integrity. A hash function will run over the data and produce an arbitrary hash value **H1** which is then attached to the data. When Host 'B' receives the packet, it runs the same hash function over the data which gives a hash value **H2**. Now, if **H1** = **H2**, this means that data's integrity has been maintained and the contents were not modified.

Availability

This means that the data should be readily available to its users. This applies to systems and to networks - not simply the data, but the technology necessary to obtain and view the data need to be available. To ensure availability, the network/system administrator should maintain hardware, make regular upgrades, have a plan for fail-over and prevent bottleneck in a network. Attacks such as DoS or DDoS may render a network unavailable as the resources of the network gets exhausted. The impact may be significant to the companies and users who rely on the network as a business tool. Thus, proper measures should be taken to prevent such attacks.

Along with the 3 objectives that make up the CIA triad, there are 3 additional concepts that are often mentioned in regards to information security. In fact the ISO/IEC 27001, an international standard on how to manage information security, mentions the following concepts as part of an organizations information security management plan. These 3 additional concepts are:

- **Non-repudiation –** means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example in cryptography it is sufficient to show that message matches the digital signature signed with sender's private key and that sender could have a sent a message and nobody else could have altered it in transit. Data Integrity and Authenticity are pre-requisites for Non repudiation.
- **Authenticity –** means verifying that users are who they say they are and that each input arriving at destination is from a trusted source.This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission. For example if take above example sender sends the message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the 2 value matches then it is known as valid transmission with the authentic or we say genuine message received at the recipient side
- **Accountability –** means that it should be possible to trace actions of an entity uniquely to that entity. For example as we discussed in Integrity section Not every employee should be allowed to do changes in other employees data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority for example Director of college and person that is allotted that change will be able to do change after verifying his bio metrics, thus timestamp with the user(doing changes) details get recorded. Thus we can say if a change goes like this then it will be possible to trace the actions uniquely to an entity.

At the core of information security is information assurance, which means the act of maintaining CIA of information, ensuring that information is not compromised in any way when critical issues arise. These issues are not limited to natural disasters, computer/server malfunctions etc.

Thus, the field of information security has grown and evolved significantly in recent years. It offers many areas for specialization, including securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning etc.

Parkerian Hexad

The Parkerian hexad is a set of six elements of information security proposed by Donn B. Parker in 1998. The Parkerian hexad adds three additional attributes to the three classic security attributes of the CIA triad (confidentiality, integrity, availability).

Figure 1: Parkerian Hexad. ("Advice: Security vs. Utility " by L. Marzigliano is in the Public Domain)

The Parkerian Hexad added the following three additional elements:

Authenticity

Authenticity refers to the veracity of the claim of origin or authorship of the information. For example, one method for verifying the authorship of a hand written document is to compare the handwriting characteristics of the document to a sampling of others which have already been verified. For electronic information, a digital signature could be used to verify the authorship of a digital document using public-key cryptography (could also be used to verify the integrity of the document).

Possession

Possession or control: Suppose a thief were to steal a sealed envelope containing a bank debit card and its personal identification number. Even if the thief did not open that envelope, it's reasonable for the victim to be concerned that the thief could do so at any time. That situation illustrates a loss of control or possession of information but does not involve the breach of confidentiality.

Utility

Utility means usefulness. For example, suppose someone encrypted data on disk to prevent unauthorized access or undetected modifications–and then lost the decryption key: that would be a breach of utility. The data would be confidential, controlled, integral, authentic, and available–they just wouldn't be useful in that form. Similarly, conversion of salary data from one currency into an inappropriate currency would be a breach of utility, as would the storage of data in a format inappropriate for a specific computer architecture; e.g., EBCDIC instead of ASCII or 9-track magnetic tape instead of DVD-ROM. A tabular representation of data substituted for a graph could be described as a breach of utility if the substitution made it more difficult to interpret the data. Utility is often confused with availability because breaches such as those described in these examples may also require time to work around the change in data format or presentation. However, the concept of usefulness is distinct from that of availability.These attributes of information are atomic in that they are not broken down into further constituents; they are non-overlapping in that they refer to unique aspects of information. Any information security breach can be described as affecting one or more of these fundamental attributes of information.

Adapted from:
"What is Information Security?" by rashi_garg, Geeks for Geeks is licensed under CC BY-SA 4.0

1.4 Attacks - Types of Attacks

Types of Attacks

In an Information Security context there are 4 broad based categories of attacks:

1. Fabrication
2. Interception
3. Interruption
4. Modification

Fabrication

As stated above, *fabrication* is one of the four broad-based categories used to classify attacks and threats. A fabrication attack creates illegitimate information, processes, communications or other data within a system.

Often, fabricated data is inserted right alongside authentic data. When a known system is compromised, attackers may use fabrication techniques to gain trust, create a false trail, collect data for illicit use, spawn malicious or extraneous processes. In addition, fabricated data may reduce confidence in genuine data with the affected system.

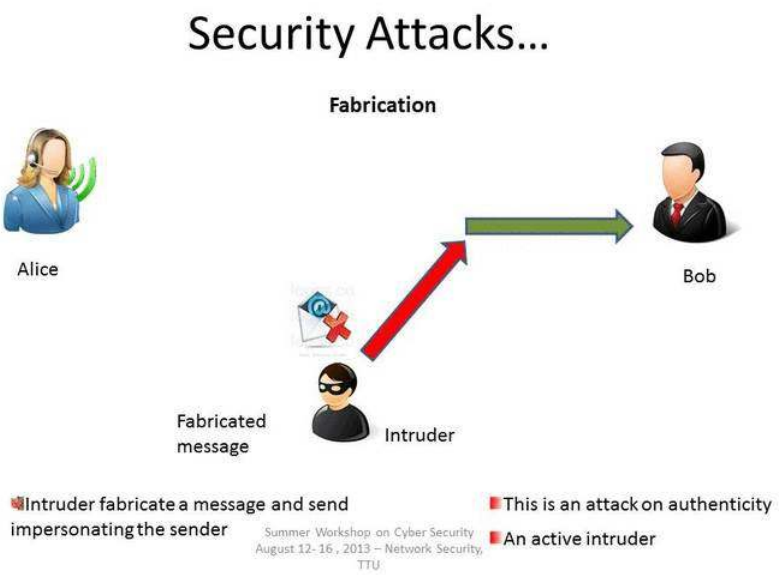


Figure 1: Fabrication Attack. ("Secuity Attacks: Fabriaction" by Unknown, CS Dept - Texas Tech University is licensed under CC BY-SA 4.0)

Examples of Fabrication attacks include:

- SQL Injection
- Route Injection
- User / Credential Counterfeiting
- Log / Audit Trail Falsification
- Email Spoofing

Mitigate the attack :

- Use of Authentication and authorization mechanisms
- Using Firewalls
- Use Digital Signatures - Digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document.

Interception

An interception is where an unauthorized individual gains access to confidential or private information. **Interception attacks** are attacks against network the **confidentiality** objective of the CIA Triad.

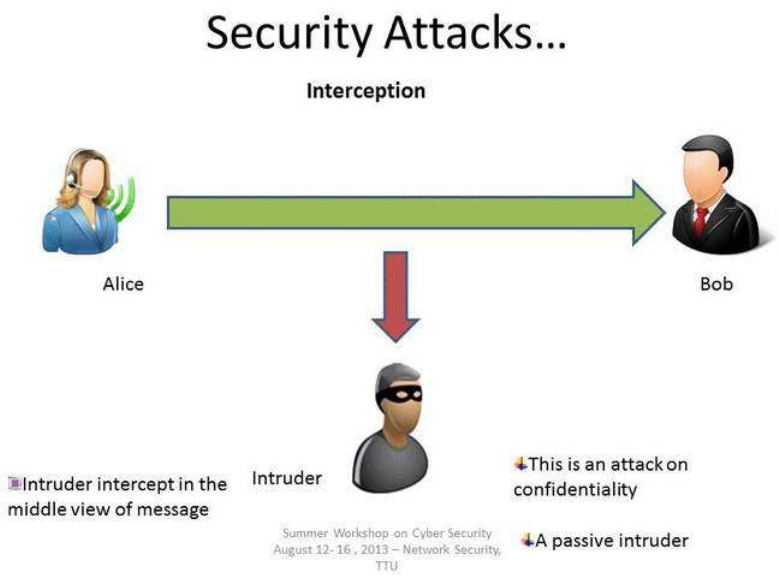


Figure 1: Interception Attacks. ("Security Attacks: Interception" by Unknown, CS Dept - Texas Tech University is licensed under CC BY-SA 4.0)

Examples of Interception attacks:

- Eavesdropping on communication.
- Wiretapping telecommunications networks.
- Illicit copying of files or programs.
- Obtaining copies of messages for later replay.
- Packet sniffing and key logging to capture data from a computer system or network.

Mitigate the attack :

- Using Encryption - SSL, VPN, 3DES, BPI+ are deployed to encrypts the flow of information from source to destination so that if someone is able to snoop in on the flow of traffic, all the person will see is ciphered text.
- Traffic Padding - It is a function that produces cipher text output continuously, even in the absence of plain text. A continuous random data stream is generated. When plaintext is available, it is encrypted and transmitted. When input plaintext is not present, the random data are encrypted and transmitted. This makes it impossible for an attacker to distinguish between tree data flow and noise and therefore impossible to deduce the amount of traffic.

Interruption

In an interruption attack, a network service is made degraded or unavailable for legitimate use. They are the attacks against the availability of the network.

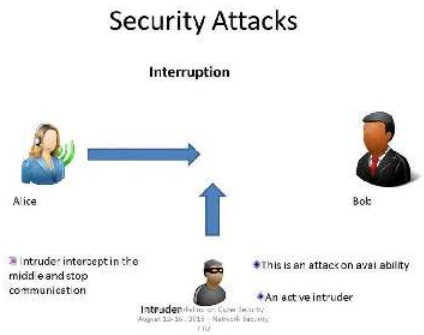


Figure 1: Interruption Attack. ("Security Attacks: Interruption" by Unknown, CS Dept - Texas Tech University is licensed under CC BY-SA 4.0)

Examples of Interruption attacks :

- Overloading a server host so that it cannot respond.
- Cutting a communication line.
- Blocking access to a service by overloading an intermediate network or network device.
- Redirecting requests to invalid destinations.
- Theft or destruction of software or hardware involved.

Mitigate the attack:

- Use Firewalls - Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. Modern stateful firewalls like Check Point FW1 NGX and Cisco PIX have a built-in capability to differentiate good traffic from DoS attack traffic.
- Keeping backups of system configuration data properly.
- Replication.

Modification

Modification is an attack against the integrity of the information. Basically there is three types of modifications.

- Change: Change existing information. The information is already existed but incorrect. Change attacks can be targeted at sensitive information or public information.
- Insertion: When an insertion attack is made, information that did not previously exist is added. This attack may be mounted against historical information or information that is yet to be acted upon.
- Deletion : Removal of existing information.

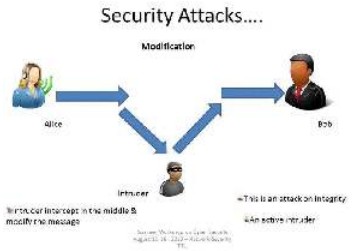


Figure 1: Modification Attack. ("Security Attacks: Modification" by Unknown, CS Dept - Texas Tech University is licensed under CC BY-SA 4.0)

Examples of Modification attacks include:

- Modifying the contents of messages in the network.
- Changing information stored in data files.
- Altering programs so they perform differently.
- Reconfiguring system hardware or network topologies.

Mitigate the attack :

- Introduction of intrusion detection systems (IDS) which could look for different signatures which represent an attack.
- Using Encryption mechanisms
- Traffic padding
- Keeping backups
- Use messaging techniques such as checksums, sequence numbers, digests, authentication codes

Adapted from:
"Network Security" by Unknown, CS Dept - Texas Tech University is licensed under CC BY-SA 4.0

1.5: Vulnerabilities

Vulnerability

A vulnerability is a weaknesses in a system that provides adversaries the opportunity to compromise assets. All systems have vulnerabilities. Even though the technologies and tools are improving the number of vulnerabilities are increasing. Vulnerabilities come from 4 main sources: hardware, software, network and procedural vulnerabilities.

1. Hardware Vulnerability:
A hardware vulnerability is a weakness which can used to attack the system hardware through physically or remotely.
For example:

1. Old version of systems or devices
2. Unprotected storage
3. Unencrypted devices, etc.

2. Software Vulnerability:
A software error happen in development or configuration such as the execution of it can violate the security policy.
For examples:

1. Lack of input validation
2. Unverified uploads
3. Cross-site scripting
4. Unencrypted data, etc.

3. Network Vulnerability:
A weakness happen in network which can be hardware or software.
For examples:

1. Unprotected communication
2. Malware or malicious software (e.g.:Viruses, Keyloggers, Worms, etc)
3. Social engineering attacks
4. Misconfigured firewalls

4. Procedural Vulnerability:
A weakness happen in an organization operational methods.
For examples:

1. Password procedure – Password should follow the standard password policy.
2. Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

Adapted from:
"Vulnerabilities in Information Security" by theinthaythimg, Geeks for Geeks is licensed under CC BY-SA 4.0

1.6: Risk

Risk in Cybersecurity

There are many threats actors in the world including nation states, criminal syndicates and various enterprises, hacktivists and insiders. These advisaries have a variety of motivation often include financial gain, corporate or government espionage, and military advantage. These concern is the launch of cyber attacks through the exploitation of vulnerabilities. There are a number of vulnerabilities in both hardware and software that can be exploited from outside or inside. The vulnerability could be unpatched software, unsecured access points, and poorly configured systems. The consequence is the harm caused to an exploited organization by a cyberattack, the organization will have to face a lot of things including a loss of sensitive data. It will affect the company's customer base, reputation, financial standing and may lose a great deal of customers. The consequence can be very costly to the organization. Cyber risk is commonly defined as exposure to harm or loss resulting from breaches of or attacks on information systems.

Risk Management

A risk is nothing but intersection of assets, threats and vulnerability.

```
A+T+V = R
```

NIST SP 800-30 Risk Management Guide for Information Technology Practitioners defines risk as a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

So the main components of Risk Assessment are:

- Threats
- Vulnerability
- Impact (i.e. potential loss)
- Likelihood of occurrence (i.e. the probability that an event – threat successful exploit of a vulnerability – will occur)

Threats are anything that can exploit a vulnerability accidentally or intentionally and destroy or damage an asset. An asset can be anything: people, property or information. An asset is what we are trying to protect and a threat is what we are trying to protect against. Vulnerability means a gap or weakness in our protection efforts.

Threat Source is the exploitation of a vulnerability or a situation either intentionally or unintentionally.

The complete process of Risk Management can be divided into following stages:

1. Context Establishment
2. Risk Assessment
3. Risk Management/ Mitigation
4. Risk Communication
5. Risk Monitoring and Review
6. IT Evaluation and Assessment

1. Context Establishment –
In this step information about the organization and basic criteria, purpose, scope and boundaries of risk management activities are obtained. In addition to this data, it is important to gather details about the organization in charge of risk management activities.

Organization's mission, values, structure, strategy, locations and cultural environment are studied to have a deep understanding of it's scope and boundaries.
The constraints (budgetary, cultural, political, technical) of the organization are to be collected and documented as guide for next steps.

The main role inside organization in charge of risk management activities can be seen as:

- Senior Management

- Chief information officer (CIO)
- System and Information owners
- the business and functional managers
- the Information System Security Officer (ISSO) or Chief information security officer (CISO)
- IT Security Practitioners
- Security Awareness Trainers

2. Risk Assessment –

Risk Management is a recurrent activity, on the other hand Risk assessment is executed at discrete points and until the performance of the next assessment. Risk Assessment is the process of evaluating known and postulated threats and vulnerabilities to determine expected loss. It also includes establishing the degree of acceptability to system operations.

Risk Assessment receives input and output from Context establishment phase and output is the list of assessed risk risks, where risks are given priorities as per risk evaluation criteria.

1. **Risk Identification –**
   In this step we identify the following:

   Thus output includes the following:

   - assets
   - threats
   - existing and planned security measures
   - vulnerabilities
   - consequence
   - related business processes
   - list of asset and related business processes with associated list of threats, existing and planned security measures
   - list of vulnerabilities unrelated to any identified threats
   - list of incident scenarios with their consequences
2. **Risk Estimation –**
   There are 2 methods for Risk Assessment:

   1. Quantitative Risk Assessment – This methodology is not mostly used by the organizations except for the financial institutions and insurance companies. Quantitative risk is mathematically expressed as Annualised Loss Expectancy (ALE). ALE is the expected monetary loss that can be expected for an asset due to a risk being realised over a one-year period.

   2. Qualitative Risk Assessment – Qualitative Risk Assessment defines likelihood, impact values and risk in subjective terms, keeping in mind that likelihood and impact values are highly uncertain. Qualitative risk assessments typically give risk results of “High”, “Moderate” and “Low”. Following are the steps in Qualitative Risk Assessment:

   - **Identifying Threats:** Threats and Threat-Sources must be identified. Threats should include threat-source to ensure accurate estimation. It is important to compile a list of all possible threats that are present across the organization and use this list as the basis for all risk management activities. Some of the examples of threat and threat-source are:
     - Natural Threats- floods, earthquakes etc.
     - Human Threats- virus, worms etc.
     - Environmental Threats- power failure, pollution etc.
   - **Identifying Vulnerabilities:** Vulnerabilities are identified by numerous means. Some of the tools are:
     - Vulnerability Scanners – This is the software the compare the operating system or code for flaws against the database of flaw signatures.
     - Penetration Testing – Human Security analyst will exercise threats against the system including operational vulnerabilities like Social Engineering.
     - Audit of Operational and Management Controls – Operational and management controls are reviewed by comparing the current documentation to best practices for example ISO 17799 and by comparing actual practices against current documented processes.

- **Relating Threats to Vulnerabilities:** This is the most difficult and mandatory activity in Risk Assessment. T-V pair list is established by reviewing the vulnerability list and pairing a vulnerability with every threat that applies, then by reviewing the threat list and ensuring that all the vulnerabilities that that threat-action/threat can act against have been identified.
- **Defining Likelihood:** Likelihood is the probability that a threat caused by a threat-source will occur against a vulnerability. Sample Likelihood definitions can be like:

  Low -0-30% chance of successful exercise of Threat during a one year period

  Moderate – 31-70% chance of successful exercise of Threat during a one year period

  High – 71-100% chance of successful exercise of Threat during a one year period

  This is just a sample defination. Organization can use their own definitaion like Very Low, Low, Moderate, High, Very High.

- **Defining Impact:** Impact is best defined in terms of impact upon confidentiality, integrity and availability. Sample definitions for impact are as follows:

	Confidentiality	**Integrity**	**Availability**
Low	Loss of Confidentiality leads to **Limited effect** on organization	Loss of Integrity leads to **Limited effect** on organization	Loss of Availability leads to **Limited effect** on organization
Medium	Loss of Confidentiality leads to **Serious effect** on organization	Loss of Integrity leads to **Serious effect** on organization	Loss of Availability leads to **Serious effect** on organization
High	Loss of Confidentiality leads to **Severe effect** on organization	Loss of Integrity leads to **Severe effect** on organization	Loss of Availability leads to **Severe effect** on organization

- **Assessing Risk:** Assessing risk is the process to determine the likelihood of the threat being exercised against the vulnerability and the resulting impact from a successful compromise. Sample Risk Determination Matrix is as follows:

		Impact		
		High	Moderate	Low
Likelihood	High	High	High	Moderate
	Moderate	High	Moderate	Low
	Low	Moderate	Low	Low

- **Risk Evaluation**

  The risk evaluation process receives as input the output of risk analysis process. It first compares each risk level against the risk acceptance criteria and then prioritize the risk list with risk treatment indications.

3. **Risk Mitigation/ Management**

   Risk Mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Since eliminating all risk in an organization is close to impossible thus, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease risk to an acceptable level.

   As per NIST SP 800 30 framework there are 6 steps in Risk Mitigation.

- **Risk Assumption:** This means to accept the risk and continue operating the system but at the same time try to implement the controls to
- **Risk Avoidance:** This means to eliminate the risk cause or consequence in order to avoid the risk for example shutdown the system if the risk is identified.
- **Risk Limitation:** To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
- **Risk Planning:** To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- **Research and Acknowledgement:** In this step involves acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.
- **Risk Transference:** This means to transfer the risk to compensate for the loss for example purchasing insurance guarantees not 100% in all cases but alteast some recovery from the loss.

4. **Risk Communication**
   The main purpose of this step is to communicate, give an understanding of all aspects of risk to all the stakeholder's of an organization. Establishing a common understanding is important, since it influences decisions to be taken.
5. **Risk Monitoring and Review**
   Security Measures are regularly reviewed to ensure they work as planned and changes in the environment don't make them ineffective. With major changes in the work environment security measures should also be updated.Business requirements, vulnerabilities and threats can change over the time. Regular audits should be scheduled and should be conducted by an independent party.
6. **IT Evaluation and Assessment**
   Security controls should be validated. Technical controls are systems that need to tested and verified. Vulnerability assessment and Penetration test are used for verifying status of security controls. Monitoring system events according to a security monitoring strategy, an incident response plan and security validation and metrics are fundamental activities to assure that an optimal level of security is obtained. It is important to keep a check on new vulnerabilities and apply procedural and technical controls for example regularly update software.

Adapted from:
"Risk Management for Information Security | Set-1" by rashi_garg, Geeks for Geeks is licensed under CC BY-SA 4.0
"Risk Management for Information Security | Set-2" by rashi_garg, Geeks for Geeks is licensed under CC BY-SA 4.0

1.4.1: Risk and Vulnerabilities

Risks and Vulnerabilities

As an Officer, a leader and manager, one of your jobs will be to assess and manage risk; fortunately you have been managing risk your entire life and continue to do so each day. All we are doing here is honing your risk management skills with a more formalized process and applying that process to the Cyber Domain.

Learning Outcomes

After completing this discussion and the activities you should be able to:

- Explain what a formalized risk assessment process supports/allows
- Describe the general steps of a risk assessment process
- Explain the factors of assessing risks
- Apply the risk assessment process to cyber domain scenarios

Introduction

You assess and manage risk on a daily basis, and you have been doing so your entire life. Why do we look both ways before we walk across a road? Because there is a risk of being hit by a car. The impact of a pedestrian being hit by a car is high (serious injury or death) so we mitigate (reduce) the risk of being hit by looking both ways before we cross the road. Just as in the physical world, there are threats in the cyberspace.

Terminology

risk

A measure of the extent to which an entity is threatened by a potential circumstance or event.

impact

An adverse effect that results from an event occurring.

vulnerability

A weakness in a system that can be exploited by a threat that adversely affects the system, results in an adverse impact. [general context]

A weakness in an information system that can be exploited to compromise a pillar of cyber security. [cyber domain context]

threat

An actor or event with the potential to adversely impact an information system.

capability

The knowledge and skill set required by a threat to carry out an event.

opportunity

The resources and positioning required by a threat to carry out an action.

intent

The motivation of a threat to carry out an action.

The Risk Management Tradeoff

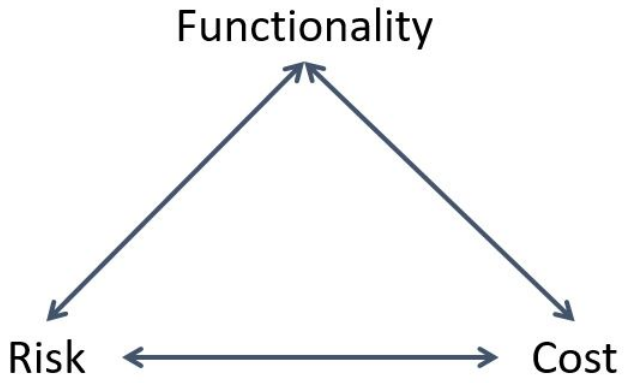


Figure 1.4.1.1: Functionality, Risk, Cost. ("Functionality, Risk, Cost" by Unknown, U.S. Naval Academy - Cyber Science Dept is in the Public Domain, CC0)

There is a fundamental tension between the services an information system provides (functionality), and security. A building with no doors or windows is quite secure, but pretty limited in its utility. Similarly, an information system with no way for data to flow in or out is very secure, but it is unable to provide a service. The more services you provide/allow, the more ways in and out of your system that need securing. Thus, for each service one needs to weigh the value of the service against the security implications of providing/allowing it. We weigh the *risk* against the *functionality* (benefits) and *cost* to make a decision on how to proceed.

Often times there is no one right answer as to whether a service should be provided/allowed, and the answer is highly situational. The amount of risk that is acceptable for your grandmother's computer is likely different than the computer used by the Chief of Naval Operations (CNO).

What process do we need to go through to assess risk? What are the factors we need to consider? You already have an intuition of what many of the important factors are. What are the benefits of providing or using the service? What are the impacts if the service is compromised? What vulnerabilities are there in providing or using the service? What threats are working to compromise the service? What are the risks inherent in providing/allowing that service? This requires a better understanding of the factors that comprise risk, and leads to developing a repeatable process to assess risk.

Risk Factors

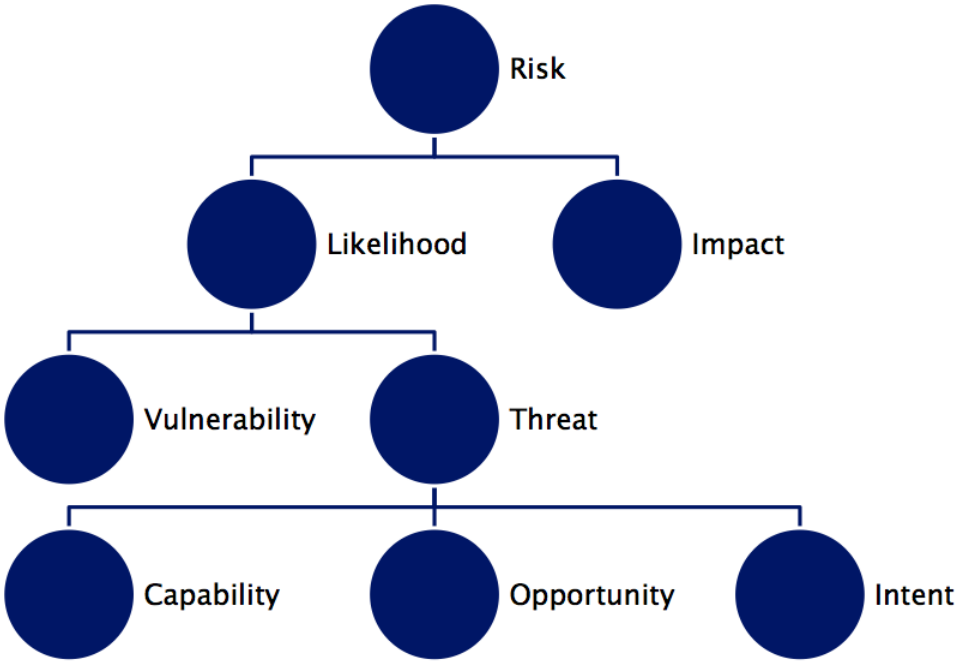


Figure 1.4.1.1: DoD Risk Model. ("DoD Risk Model" by Unknown, U.S. Naval Academy - Cyber Science Dept is in the Public Domain, CC0)

In the cyber domain, just as in all domains, there are various factors that go into assessing risk. Risk Assessment can be viewed as a function with inputs, a process, and outputs. In general risk is viewed as a function of *likelihood of occurrence of an event* and *impact of an event*, `risk( likelihood, impact )` .

Intuitively, if we increase the likelihood of a negative event occurring, the risk severity increases, and vice versa. This is also the case with impact, if the impact of a negative event occurring increases, the risk severity increases.

Likelihood of Occurrence

Likelihood of occurrence can be decomposed into two main components: *threat* and *vulnerability*. Threat is any circumstance or event that has the potential to adversely impact our system. Threat can be adversarial (purposely caused by a person) or non-adversarial (caused by an accident or natural event such as a hurricane). Vulnerability represents a weakness in an information system that can be exploited, often by an adversarial threat actor.

Not all vulnerabilities are equal, there are factors that we can assess a vulnerability with. The risk assessment team will ask and answer questions such as (*OWASP*):

- (Discoverable) How easy is it for an adversary to discover the vulnerability?
- (Exploitable) How easy is it for an adversary to exploit the vulnerability?
- (Awareness) How well known is the vulnerability?
- (Detectable) How likely is an exploit to be detected?

Just as vulnerabilities, threats are also assessed using various factors. The risk assessment team will ask and answer questions such as (*OWASP*):

- (Capability) How technically skilled is an adversary?
- (Capability) How much does the adversary know about the target system?
- (Opportunity) Does the adversary have the resources (technology) to exploit a vulnerability?
- (Opportunity) Is the adversary in a position to exploit a vulnerability?
- (Intent) How motivated is an adversary to find and exploit a vulnerability?
- (Intent) Does the actor performing the exploit intend harm?

Impact

Impact assessments focus on the resulting damage if a vulnerability is exploited. A single vulnerability may have multiple impacts within the cyber domain, both technological and non-technological. We can apply concepts from conventional operations such as: deceive, deny, disrupt, degrade, and destroy.

Technical impacts are associated to the Pillars of Cyber Security. For example, if the password file for a web based service is compromised, the Authentication pillar is impacted.

Non-technical impacts are associated with the operations and relationships of an organization:

- (Personnel) To what extent are personnel put in physical danger if the vulnerability is exploited?
- (Equipment) To what extent is equipment put in physical danger if the vulnerability is exploited?
- (Operations) To what extent will the success of operations be endangered?
- (Capabilities) To what extent will the capabilities of the organization be damaged?
- (Reputation) To what extent will the organization's reputation be damaged?
- (Financial) What will the financial damage to the organization be?

The *to what extent* part of assessing impact is not always simple to quantify or qualify.

Common Vulnerability Scoring System

```
The National Institute of Standards and Technology (NIST) maintains the National Vulne
tools provided with the NVD is the Common Vulnerability Scoring System (CVSS). The CVS
efforts.
Example: CVSS – ShellShock
```

The Risk Management Process

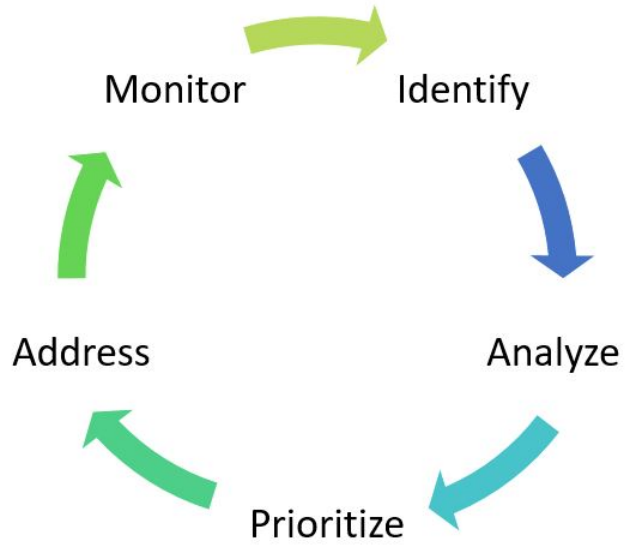


Figure 1.4.1.1: Risk Management Process. ("Risk Management Process" by Unknown, U.S. Naval Academy - Cyber Science Dept is in the Public Domain, CC0)

A common first question when presented with a formalized process is: *Why is this process necessary?*. Following a formalized method allows for the a given process to be repeated; the repeatability allows us to assess process changes and determine if improvement efforts actually achieved the desired results or not. In other words, formalized processes allow us to compare and contrast.

There a number of different methods for assessing risk, most of the methods include a feedback (process improvement) step at the end, making a risk assessment a continual cyclic process. The following are general steps to assessing and managing risk:

Risk assessment begins with identifying risks associated with a task or system. We will use crossing a road as an example. Here are some of the risks associated with crossing a road:

1. **Identify Risks**

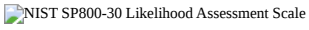
   Risk assessment begins with identifying risks associated with a task or system. We will use crossing a road as an example. Here are some of the risks associated with crossing a road:

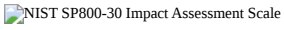
Risk
Trip and fall
Hit by bike
Hit by car
Fined for jaywalking

   We can look at risk from the viewpoint of the pedestrian or from the driver. In the cyber domain we look at risk from the offensive or defensive viewpoint. In fact, being proficient at assessing and managing risks in the cyber domain requires looking at risks from both an offensive and defensive perspective; a yin and yang.

2. **Analyze the Risk**

   Risks are assessed to determine severity based on the event's likelihood and impact. Risks can be assessed using a quantitative (assigned a numeric value) or a qualitative scale (assigned to a category such as low or high). The tables below are extracted from NIST SP800-30 and provide general guidance on how to define likelihood and impact both qualitatively and quantitatively.

   
   NIST SP800-30 Likelihood Assessment Scale

   
   NIST SP800-30 Impact Assessment Scale

   Going back to the crossing the road example, we can now assign a qualitative value to each of the risks that were identified in the first step.

Risk	Likelihood of Occurrence	Impact
Trip and fall	Low (2)	Very Low (0)
Hit by bike	Moderate (5)	Moderate (5)
Hit by car	High (8)	High (8)
Fined for jaywalking	Low (2)	Very Low (0)

3. **Prioritize the Risk**

   Organizations do not have infinite resources and therefore cannot eliminate or even address all possible risks. Risks must be prioritized by severity so that an appropriate strategy can be developed in line with resource constraints. Generally this just consists of ordering the identified risks from most severe to least severe by assigning quantitative values based on the qualitative values above.

Priority	Risk	Likelihood of Occurrence	Impact
1	Hit by car	High (8)	High (8)
2	Hit by bike	Moderate (5)	Moderate (5)
3	Fined for jaywalking	Low (2)	Very Low (0)
4	Trip and fall	Low (2)	Very Low (0)

4. **Address the Risk**

Once a risk has been identified, assigned a severity, and prioritized we can determine how the risk will be addressed. There are four strategies for addressing risk:

Note that ignoring risk is not a legitimate strategy. The table below shows our road crossing example with risk strategies applied.

Priority	Risk	Likelihood of Occurrence	Impact	Strategy
1	Hit by car	High	High	Control - Look both ways before crossing
2	Hit by bike	Moderate	Moderate	Control - Look both ways before crossing
3	Fined for jaywalking	Low	Very Low	Avoid - Only cross at designated crosswalks
4	Trip and fall	Low	Very Low	Accept

It is impossible to nullify risk; there is risk in any action. Any risk that remains after a strategy has been applied is known as *residual risk*. For example, we choose to control our risk of being hit by a car by looking both ways before crossing. While this greatly reduces our risk it does not eliminate it. There is residual risk that a car may suddenly accelerate or take some other unexpected action.

4. **Monitor the Risk**

Risk management is a process. After strategies have been applied to each risk they need to be continually monitored to determine their effectiveness. Questions to ask include:

- Are you using resources effectively?
- Is the risk management strategy working as expected?
- Have any new risks been identified?
- Have any risks changed?
- Have any new threats or vulnerabilities been identified?
- Are new controls available?

If you can answer yes to any of those questions the risk management process should be repeated and results updated. Regardless, the risk management process should be executed on a periodic basis.

Review Questions

1. Why use formalized risk assessments?
2. In your own words, describe each term given pertaining to risk assessments.
3. What is the risk management trade off?
4. What are the general steps of a risk assessment and how can they be applied to cyber?

References

1. OWASP. *OWASP Risk Rating Methodology*. retrieved: 30 Oct 2014.
2. *Risk Equation*
3. National Institute for Standards and Technology (NIST) Special Publication 800-30: Guide for Conducting Risk Assessments

Adapted from:
"Risks and Vulnerabilities" by Unknown, U.S. Naval Academy - Cyber Science Dept is in the Public Domain, CC0

1.7: Incidence Response

Incident Management in Cyber Security

In the field of cybersecurity, incident management can be defined as the process of identifying, managing, recording, and analyzing the security threats and incidents related to cybersecurity in the real world. This is a very important step after a cyber disaster or before a cyber disaster takes place in an IT infrastructure. This process includes knowledge and experience. Good incident management can reduce the adverse effects of cyber destruction and can prevent a cyber-attack from taking place. It can prevent the compromising of a large number of data leaks. An organization without a good incident response plan can become a victim of a cyber-attack in which the data of the organization can be compromised at large.

There is a five-step process for incident management in cybersecurity given by the ISO/IEC Standard 27035. They are as follows.

Step-1 :
The process of incident management starts with an alert that reports an incident that took place. Then comes the engagement of the incident response team (IRT). Prepare for handling incidents.

Step-2 :
Identification of potential security incidents by monitoring and report all incidents.

Step-3 :
Assessment of identified incidents to determine the appropriate next steps for mitigating the risk.

Step-4 :
Respond to the incident by containing, investigating, and resolving it (based on the outcome of step 3).

Step-5 :
Learn and document key takeaways from every incident.

Some tips for security incident management :

- Each and every organization needs to have a good and matured plan for the security incident management process, implementing the best process is very useful to make a comprehensive security incident management plan.
- Create a security incident management plan with supporting policies including proper guidance on how incidents are detected, reported, assessed, and responded. It should have a checklist ready. The checklist will be containing actions based on the threat. The security incident management plan has to be continuously updated with security incident management procedures as necessary, particularly with lessons learned from prior incidents.
- Creating an Incident Response Team (IRT) which will work on clearly defined roles and responsibilities. The IRT will also include functional roles like finance, legal, communication, and operations.
- Always create regular training and mock drills for security incident management procedures. This improves the functionality of the IRT and also keep them on their toes.
- Always perform a post-incident analysis after any security incident to learn from any success and failure and make necessary adjustments to the program and incident management processes when needed.

Necessary part of incident response :
Always make a habit of collecting evidence and analyze forensics which is a necessary part of incident response. For these circumstances, the following things are needed.

1. A well-defined policy to collect evidence to ensure that it is correct and very much sufficient to make it admissible in the Court of Law.
2. It is also importantly needed to have the ability to employ forensics as needed for analysis, reporting, and investigation.
3. The personnel of the IRT must be trained in cyber forensics, functional techniques and would also have some knowledge in the legal and governance.

1.8: Defense in Depth

Defense in depth is a concept used in Information security in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical security for the duration of the system's life cycle.

Background

The idea behind the defense in depth approach is to defend a system against any particular attack using several independent methods. It is a layering tactic, conceived. by the National Security Agency (NSA) as a comprehensive approach to information and electronic security. The term defense in depth in computing is inspired by a military strategy of the same name, but is quite different in concept. The military strategy revolves around having a weaker perimeter defense and intentionally yielding space to buy time, envelop, and ultimately counter-attack an opponent, whereas the information security strategy simply involves multiple layers of controls, but not intentionally ceding ground (cf. honeypot.)

Controls

Defense in depth can be divided into three areas: Physical, Technical, and Administrative.

Physical controls

Physical controls are anything that physically limits or prevents access to IT systems. Fences, guards, dogs, and CCTV systems and the like.

Technical controls

Technical controls are hardware or software whose purpose is to protect systems and resources. Examples of technical controls would be disk encryption, fingerprint readers, and authentication. Hardware technical controls differ from physical controls in that they prevent access to the contents of a system, but not the physical systems themselves.

Administrative controls

Administrative controls are an organization's policies and procedures. Their purpose is to ensure that there is proper guidance available in regards to security and that regulations are met. They include things such as hiring practices, data handling procedures, and security requirements.

Commonly used methods

Using more than one of the following layers constitutes an example of defense in depth.

System/application security:
Antivirus software
Authentication and password security
Encryption
Hashing passwords
Logging and auditing
Multi-factor authentication
Vulnerability scanners
Timed access control
Internet Security Awareness Training
Sandboxing
Intrusion detection systems (IDS)

Network security:
Firewalls (hardware or software)

Demilitarized zones (DMZ)
Virtual private network (VPN)

Physical security:
Biometrics
Data-centric security
Physical security (e.g. deadbolt locks)

CHAPTER OVERVIEW

2: Authenticate and Identify

2.1: Identification

Identification - what is it?

Identification is basically the process of someone claiming to be a specific person. They can identify themselves as “Pat,” show an id card of some type card with a name on it or have an email address showing their name.

In the current context of online transactions, users “identify” themselves by providing a name, an email address or phone number to a web request. For example, using a process of identification alone, as long as a buyer has the card’s proper information that is associated with the card being used, the user is pretty much accepted as is.

A business that allows identification by itself is essentially saying, "We have no reason to doubt that you are indeed the the person you claim to be", despite having not independently verified if the information is truthful. It’s like asking, “Who are you?” and simply accepting whatever answer is given. For transactions where there is not a lot at stake, like registering for a class or checking out a book, simply having someone declare their identity without providing any verification may be good enough.

It is becoming more and more frequent that identification alone is adequate. It’s like having a username without a password.

So how can we determine the person is who they say they are? That’s where verification comes in.

What is Verification?

Verification goes beyond the basic question, “Who are you?” Identity verification goes the extra mile and asks, “Are you really who you say you are?” the response needs to provide, with a high degree of confidence that, the answer is accurate.

The most accurate way to verify someone's identity is to request and validate more than one form of identification against the person standing in front of you, with at least one of them being a photo ID. A driver's license, a Social Security card, a valid passport, or military photograph identification are some forms of identification. Verifying someone’s identity to a high degree of certainty takes effort. At a time when service providers want to provide a “frictionless” onboarding process, some may cut corners and require a low barrier to entry. Typical social media accounts, for example, only ask new users to provide a name, email address, username and password. A phone number may be thrown in there for good measure.

Depending on the organization and the level of assurance needed, a university ID or other non-government issued identification card may suffice for one form of ID. Identity verification in the electronic sense, also called identity "proofing" or "vetting", is used to confirm an identity where the individual is not standing before you to show some sort of picture ID. In these cases, most organizations require a real-time process that validates the personal information provided by the individual.

Apply for an online bank account, though, and you may be expected to provide a social security number, photo ID or passport, and proof of your current address. The stakes associated with a bank account are much greater than those with a TikTok account, therefore the verification requirements are more stringent. In fact, in the financial sector alone, there are numerous regulatory acts to prevent fraudsters from setting up false bank accounts, laundering money, and other unseemly criminal activities. The compliance mandates associated with these regulations are not satisfied by traditional verification methods, which is why businesses are beginning to make a shift to pairing a customer’s identity information with one of their biometric markers at the point of onboarding.

2.2: Authentication

What is Authentication?

In security, authentication is the process of verifying whether someone (or something) is, in fact, who (or what) it is declared to be.

According the the National Institute of Standards and Technology authentication is defined as "Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system". Notice that this definition does not restrict authentication to human users. It includes processes, or devices

Authentication factors

The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something the user *knows*, something the user *has*, and something the user *is*. Each **authentication factor** covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.

Security research has determined that for a positive authentication, elements from at least two, and preferably all three, factors should be verified. The four factors (classes) and some of elements of each factor are:

- the knowledge factors: Something the user knows (e.g., a password, partial password, pass phrase, personal identification number (PIN), challenge response (the user must answer a question or pattern), security question).
- the ownership factors: Something the user possess (e.g., wrist band, ID card, security token, implanted device, cell phone with built-in hardware token, software token, or cell phone holding a software token).
- the inherence factors: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).
- the location factors: Somewhere the user is (e.g. connection to a specific computing network or using a GPS signal to identify the location).

Multi-factor authentication

Multi-factor authentication is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). It protects the user from an unknown person trying to access their data such as personal ID details or financial assets.

Authentication takes place when someone tries to log into a computer resource (such as a network, device, or application). The resource requires the user to supply the identity by which the user is known to the resource, along with evidence of the authenticity of the user's claim to that identity. Simple authentication requires only one such piece of evidence (factor), typically a password. For additional security, the resource may require more than one factor—multi-factor authentication, or two-factor authentication in cases where exactly two pieces of evidence are to be supplied.

The use of multiple authentication factors to prove one's identity is based on the premise that an unauthorized actor is unlikely to be able to supply the factors required for access. If, in an authentication attempt, at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and access to the asset (e.g., a building, or data) being protected by multi-factor authentication then remains blocked.

Knowledge

Knowledge factors are the most commonly used form of authentication. In this form, the user is required to prove knowledge of a secret in order to authenticate.

A password is a secret word or string of characters that is used for user authentication. This is the most commonly used mechanism of authentication. Many multi-factor authentication techniques rely on password as one factor of authentication. Variations include both longer ones formed from multiple words (a passphrase) and the shorter, purely numeric, personal identification number (PIN) commonly used for ATM access. Traditionally, passwords are expected to be memorized.

Many secret questions such as "Where were you born?" are poor examples of a knowledge factor because they may be known to a wide group of people, or be able to be researched.

Possession

Possession factors ("something only the user has") have been used for authentication for centuries, in the form of a key to a lock. The basic principle is that the key embodies a secret which is shared between the lock and the key, and the same principle underlies possession factor authentication in computer systems. A security token is an example of a possession factor.

Disconnected tokens have no connections to the client computer. They typically use a built-in screen to display the generated authentication data, which is manually typed in by the user. This type of token mostly use a "one-time password" that can only be used for that specific session.

Connected tokens are devices that are physically connected to the computer to be used. Those devices transmit data automatically. There are a number of different types, including card readers, wireless tags and USB tokens.

A software token (a.k.a. soft token) is a type of two-factor authentication security device that may be used to authorize the use of computer services. Software tokens are stored on a general-purpose electronic device such as a desktop computer, laptop, PDA, or mobile phone and can be duplicated. (Contrast hardware tokens, where the credentials are stored on a dedicated hardware device and therefore cannot be duplicated, absent physical invasion of the device.) A soft token may not be a device the user interacts with. Typically an X.509v3 certificate is loaded onto the device and stored securely to serve this purpose.

Inherent

These are factors associated with the user, and are usually biometric methods, including fingerprint, face, voice, or iris recognition. Behavioral biometrics such as keystroke dynamics can also be used.

Location

Increasingly, a fourth factor is coming into play involving the physical location of the user. While hard wired to the corporate network, a user could be allowed to login using only a pin code while off the network entering a code from a soft token as well could be required. This could be seen as an acceptable standard where access into the office is controlled.

Systems for network admission control work in similar ways where your level of network access can be contingent on the specific network your device is connected to, such as wifi vs wired connectivity. This also allows a user to move between offices and dynamically receive the same level of network access in each.

Mutual authentication

Mutual authentication or two-way authentication (not to be confused with two-factor authentication) refers to two parties authenticating each other at the same time in an authentication protocol. It was previously referred to as “mutual entity authentication,” as two or more entities verify the others' legality before any data or information is transmitted.

Mutual authentication is a desired characteristic in verification schemes that transmit sensitive data, in order to ensure data security. Mutual authentication is found in two types of schemes: username-password based schemes and certificate based schemes, and these schemes are often employed in the Internet of Things (IoT). Writing effective security schemes in IoT systems can become challenging, especially when needing schemes to be lightweight and have low computational costs. Mutual authentication is a crucial security step that can defend against many adversarial attacks, which otherwise can have large consequences if IoT systems (such as e-Healthcare servers) are hacked. In scheme analyses done of past works, a lack of mutual authentication had been considered a weakness in data transmission schemes.

2.3: Authentication Methods - Password

Password

A password, sometimes called a passcode, is a memorized secret, typically a string of characters, usually used to confirm a user's identity. Using the terminology of the NIST Digital Identity Guidelines, "the secret is memorized by a party called the claimant while the party verifying the identity of the claimant is called the verifier. When the claimant successfully demonstrates knowledge of the password to the verifier through an established authentication protocol, the verifier is able to infer the claimant's identity".

In general, a password is an arbitrary string of characters including letters, digits, or other symbols. If the permissible characters are constrained to be numeric, the corresponding secret is sometimes called a personal identification number (PIN).

Despite its name, a password does not need to be an actual word; indeed, a non-word (in the dictionary sense) may be harder to guess, which is a desirable property of passwords. A memorized secret consisting of a sequence of words or other text separated by spaces is sometimes called a passphrase. A passphrase is similar to a password in usage, but the former is generally longer for added security.

Choosing a secure and memorable password

The easier a password is for the owner to remember generally means it will be easier for an attacker to guess. However, passwords that are difficult to remember may also reduce the security of a system because (a) users might need to write down or electronically store the password, (b) users will need frequent password resets and (c) users are more likely to re-use the same password across different accounts. Similarly, the more stringent the password requirements, such as "have a mix of uppercase and lowercase letters and digits" or "change it monthly", the greater the degree to which users will subvert the system. Others argue longer passwords provide more security (e.g., entropy) than shorter passwords with a wide variety of characters.

In The Memorability and Security of Passwords, Jeff Yan et al. examine the effect of advice given to users about a good choice of password. They found that passwords based on thinking of a phrase and taking the first letter of each word are just as memorable as naively selected passwords, and just as hard to crack as randomly generated passwords.

Combining two or more unrelated words and altering some of the letters to special characters or numbers is another good method, but a single dictionary word is not. Having a personally designed algorithm for generating obscure passwords is another good method.

However, asking users to remember a password consisting of a "mix of uppercase and lowercase characters" is similar to asking them to remember a sequence of bits: hard to remember, and only a little bit harder to crack (e.g. only 128 times harder to crack for 7-letter passwords, less if the user simply capitalizes one of the letters). Asking users to use "both letters and digits" will often lead to easy-to-guess substitutions such as 'E' → '3' and 'I' → '1', substitutions which are well known to attackers. Similarly typing the password one keyboard row higher is a common trick known to attackers.

In 2013, Google released a list of the most common password types, all of which are considered insecure because they are too easy to guess (especially after researching an individual on social media):

- The name of a pet, child, family member, or significant other
- Anniversary dates and birthdays
- Birthplace
- Name of a favorite holiday
- Something related to a favorite sports team
- The word "password"

Factors in the security of a password system

The security of a password-protected system depends on several factors. The overall system must be designed for sound security, with protection against computer viruses, man-in-the-middle attacks and the like. Physical security issues are also a concern, from deterring shoulder surfing to more sophisticated physical threats such as video cameras and keyboard sniffers. Passwords should be chosen so that they are hard for an attacker to guess and hard for an attacker to discover using any of the available automatic attack schemes. See password strength and computer security for more information.

Nowadays, it is a common practice for computer systems to hide passwords as they are typed. The purpose of this measure is to prevent bystanders from reading the password; however, some argue that this practice may lead to mistakes and stress, encouraging users to choose weak passwords. As an alternative, users should have the option to show or hide passwords as they type them.

Effective access control provisions may force extreme measures on criminals seeking to acquire a password or biometric token. Less extreme measures include extortion, rubber hose cryptanalysis, and side channel attack.

Rate at which an attacker can try guessed passwords

The rate at which an attacker can submit guessed passwords to the system is a key factor in determining system security. Some systems impose a time-out of several seconds after a small number (e.g., three) of failed password entry attempts. In the absence of other vulnerabilities, such systems can be effectively secure with relatively simple passwords if they have been well chosen and are not easily guessed.

Many systems store a cryptographic hash of the password. If an attacker gets access to the file of hashed passwords guessing can be done offline, rapidly testing candidate passwords against the true password's hash value. In the example of a web-server, an online attacker can guess only at the rate at which the server will respond, while an off-line attacker (who gains access to the file) can guess at a rate limited only by the hardware on which the attack is running.

Passwords that are used to generate cryptographic keys (e.g., for disk encryption or Wi-Fi security) can also be subjected to high rate guessing. Lists of common passwords are widely available and can make password attacks very efficient. (See Password cracking.) Security in such situations depends on using passwords or passphrases of adequate complexity, making such an attack computationally infeasible for the attacker. Some systems, such as PGP and Wi-Fi WPA, apply a computation-intensive hash to the password to slow such attacks. See key stretching.

Limits on the number of password guesses

An alternative to limiting the rate at which an attacker can make guesses on a password is to limit the total number of guesses that can be made. The password can be disabled, requiring a reset, after a small number of consecutive bad guesses (say 5); and the user may be required to change the password after a larger cumulative number of bad guesses (say 30), to prevent an attacker from making an arbitrarily large number of bad guesses by interspersing them between good guesses made by the legitimate password owner. Attackers may conversely use knowledge of this mitigation to implement a denial of service attack against the user by intentionally locking the user out of their own device; this denial of service may open other avenues for the attacker to manipulate the situation to their advantage via social engineering.

Form of stored passwords

Some computer systems store user passwords as plaintext, against which to compare user logon attempts. If an attacker gains access to such an internal password store, all passwords—and so all user accounts—will be compromised. If some users employ the same password for accounts on different systems, those will be compromised as well.

More secure systems store each password in a cryptographically protected form, so access to the actual password will still be difficult for a snooper who gains internal access to the system, while validation of user access attempts remains possible. The most secure don't store passwords at all, but a one-way derivation, such as a polynomial, modulus, or an advanced hash function. Roger Needham invented the now common approach of storing only a "hashed" form of the plaintext password. When a user types in a password on such a system, the password handling software runs through a cryptographic hash algorithm, and if the hash value generated from the user's entry matches the hash stored in the password database, the user is permitted access. The hash value is created by applying a cryptographic hash function to a string consisting of the submitted password and, in many implementations, another value known as a salt. A salt prevents attackers from easily building a list of hash values for common passwords and prevents password cracking efforts from scaling across all users. MD5 and SHA1 are frequently used cryptographic hash functions, but they are not recommended for password hashing unless they are used as part of a larger construction such as in PBKDF2.

The stored data—sometimes called the "password verifier" or the "password hash"—is often stored in Modular Crypt Format or RFC 2307 hash format, sometimes in the /etc/passwd file or the /etc/shadow file.

The main storage methods for passwords are plain text, hashed, hashed and salted, and reversibly encrypted. If an attacker gains access to the password file, then if it is stored as plain text, no cracking is necessary. If it is hashed but not salted then it is

vulnerable to rainbow table attacks (which are more efficient than cracking). If it is reversibly encrypted then if the attacker gets the decryption key along with the file no cracking is necessary, while if he fails to get the key cracking is not possible. Thus, of the common storage formats for passwords only when passwords have been salted and hashed is cracking both necessary and possible

If a cryptographic hash function is well designed, it is computationally infeasible to reverse the function to recover a plaintext password. An attacker can, however, use widely available tools to attempt to guess the passwords. These tools work by hashing possible passwords and comparing the result of each guess to the actual password hashes. If the attacker finds a match, they know that their guess is the actual password for the associated user. Password cracking tools can operate by brute force (i.e. trying every possible combination of characters) or by hashing every word from a list; large lists of possible passwords in many languages are widely available on the Internet. The existence of password cracking tools allows attackers to easily recover poorly chosen passwords. In particular, attackers can quickly recover passwords that are short, dictionary words, simple variations on dictionary words, or that use easily guessable patterns. A modified version of the DES algorithm was used as the basis for the password hashing algorithm in early Unix systems. The crypt algorithm used a 12-bit salt value so that each user's hash was unique and iterated the DES algorithm 25 times in order to make the hash function slower, both measures intended to frustrate automated guessing attacks. The user's password was used as a key to encrypt a fixed value. More recent Unix or Unix-like systems (e.g., Linux or the various BSD systems) use more secure password hashing algorithms such as PBKDF2, bcrypt, and scrypt, which have large salts and an adjustable cost or number of iterations. A poorly designed hash function can make attacks feasible even if a strong password is chosen. See LM hash for a widely deployed and insecure example.

Adapted from:

2.3.1: Authentication Methods - Password (continued)

Password - continued

Procedures for changing passwords

Usually, a system must provide a way to change a password, either because a user believes the current password has been (or might have been) compromised, or as a precautionary measure. If a new password is passed to the system in unencrypted form, security can be lost (e.g., via wiretapping) before the new password can even be installed in the password database and if the new password is given to a compromised employee, little is gained. Some web sites include the user-selected password in an unencrypted confirmation e-mail message, with the obvious increased vulnerability.

Identity management systems are increasingly used to automate issuance of replacements for lost passwords, a feature called self service password reset. The user's identity is verified by asking questions and comparing the answers to ones previously stored (i.e., when the account was opened).

Some password reset questions ask for personal information that could be found on social media, such as mother's maiden name. As a result, some security experts recommend either making up one's own questions or giving false answers.

Password longevity

"Password aging" is a feature of some operating systems which forces users to change passwords frequently (e.g., quarterly, monthly or even more often). Such policies usually provoke user protest and foot-dragging at best and hostility at worst. There is often an increase in the people who note down the password and leave it where it can easily be found, as well as help desk calls to reset a forgotten password. Users may use simpler passwords or develop variation patterns on a consistent theme to keep their passwords memorable. Because of these issues, there is some debate as to whether password aging is effective. Changing a password will not prevent abuse in most cases, since the abuse would often be immediately noticeable. However, if someone may have had access to the password through some means, such as sharing a computer or breaching a different site, changing the password limits the window for abuse.

Number of users per password

Allotting separate passwords to each user of a system is preferable to having a single password shared by legitimate users of the system, certainly from a security viewpoint. This is partly because users are more willing to tell another person (who may not be authorized) a shared password than one exclusively for their use. Single passwords are also much less convenient to change because many people need to be told at the same time, and they make removal of a particular user's access more difficult, as for instance on graduation or resignation. Separate logins are also often used for accountability, for example to know who changed a piece of data.

Password security architecture

Common techniques used to improve the security of computer systems protected by a password include:

- Not displaying the password on the display screen as it is being entered or obscuring it as it is typed by using asterisks (*) or bullets (•).
- Allowing passwords of adequate length. (Some legacy operating systems, including early versions reducing security.)
- Requiring users to re-enter their password after a period of inactivity (a semi log-off policy).
- Enforcing a password policy to increase password strength and security.
    - Assigning randomly chosen passwords.
    - Requiring minimum password lengths.
    - Some systems require characters from various character classes in a password—for example, "must have at least one uppercase and at least one lowercase letter". However, all-lowercase passwords are more secure per keystroke than mixed capitalization passwords.
    - Employ a password blacklist to block the use of weak, easily guessed passwords
    - Providing an alternative to keyboard entry (e.g., spoken passwords, or biometric identifiers).

    - Requiring more than one authentication system, such as two-factor authentication (something a user has and something the user knows).
- Using encrypted tunnels or password-authenticated key agreement to prevent access to transmitted passwords via network attacks
- Limiting the number of allowed failures within a given time period (to prevent repeated password guessing). After the limit is reached, further attempts will fail (including correct password attempts) until the beginning of the next time period. However, this is vulnerable to a form of denial of service attack.
- Introducing a delay between password submission attempts to slow down automated password guessing programs.

Some of the more stringent policy enforcement measures can pose a risk of alienating users, possibly decreasing security as a result.

Password reuse

It is common practice amongst computer users to reuse the same password on multiple sites. This presents a substantial security risk, because an attacker needs to only compromise a single site in order to gain access to other sites the victim uses. This problem is exacerbated by also reusing usernames, and by websites requiring email logins, as it makes it easier for an attacker to track a single user across multiple sites. Password reuse can be avoided or minimised by using mnemonic techniques, writing passwords down on paper, or using a password manager.

It has been argued by Redmond researchers Dinei Florencio and Cormac Herley, together with Paul C. van Oorschot of Carleton University, Canada, that password reuse is inevitable, and that users should reuse passwords for low-security websites (which contain little personal data and no financial information, for example) and instead focus their efforts on remember long, complex passwords for a few important accounts, such as bank accounts.

Writing down passwords on paper

Historically, many security experts asked people to memorize their passwords: "Never write down a password". More recently, many security experts such as Bruce Schneier recommend that people use passwords that are too complicated to memorize, write them down on paper, and keep them in a wallet.

Password manager software can also store passwords relatively safely, in an encrypted file sealed with a single master password.

Adapted from:
"Password" by Multiple Contributors, Wikipedia is licensed under CC BY-SA 3.0

2.3.2: Authentication Methods - Biometrics

Biometrics

Biometrics are body measurements and calculations related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, keystroke, signature, behavioral profiling, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

Biometric functionality

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain et al. (1999) identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication.

- Universality means that every person using a system should possess the trait.
- Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
- Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.
- Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.
- Performance relates to the accuracy, speed, and robustness of technology used (see performance section for more details).
- Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
- Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.

Proper biometric use is very application dependent. Certain biometrics will be better than others based on the required levels of convenience and security. No single biometric will meet all the requirements of every possible application.

The block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person.[5] In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. The third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".

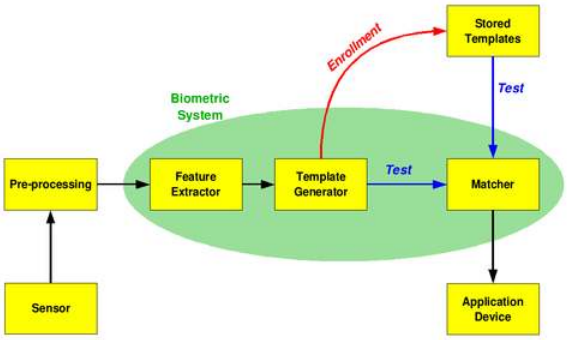


Figure 2.3.2.1: Biometric System ("Biometric System" by **Multiple Contributors**, Wikipedia is licensed under CC BY-SA 3.0)

Second, in identification mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

The first time an individual uses a biometric system is called enrollment. During enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block, necessary features are extracted. This step is an important step as the correct features need to be extracted in an optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the filesize and to protect the identity of the enrollee. However, depending on the scope of the biometric system, original biometric image sources may be retained such as the PIV-cards used in the Federal Information Processing Standard Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS 201).

During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for a specified use or purpose (e.g. entrance in a restricted area), though it is a fear that the use of biometric data may face mission creep. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. The selection of a biometric is based on user requirements and considers sensor and device availability, computational time and reliability, cost, sensor size, and power consumption.

Performance

The discriminating powers of all biometric technologies depend on the amount of entropy they are able to encode and use in matching. The following are used as performance metrics for biometric systems:

- False match rate (FMR, also called FAR = False Accept Rate): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs that are incorrectly accepted. In case of similarity scale, if the person is an imposter in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FMR, which thus also depends upon the threshold value.
- False non-match rate (FNMR, also called FRR = False Reject Rate): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs that are incorrectly

rejected.

- Receiver operating characteristic or relative operating characteristic (ROC): The ROC plot is a visual characterization of the trade-off between the FMR and the FNMR. In general, the matching algorithm performs a decision based on a threshold that determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FMR but increase the FNMR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviation scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).
- Equal error rate or crossover error rate (EER or CER): the rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.
- Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low-quality inputs.
- Failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- Template capacity: the maximum number of sets of data that can be stored in the system.

Adapted from:

2.3.3: Authentication Methods - Security Tokens

Security Tokens

A security token is a peripheral device used to gain access to an electronically restricted resource. The token is used in addition to or in place of a password. It acts like an electronic key to access something. Examples include a wireless keycard opening a locked door, or in the case of a customer trying to access their bank account online, the use of a bank-provided token can prove that the customer is who they claim to be.

Some tokens may store cryptographic keys that may be used to generate a digital signature, or biometric data, such as fingerprint details. Some may also store passwords. Some designs incorporate tamper resistant packaging, while others may include small keypads to allow entry of a PIN or a simple button to start a generating routine with some display capability to show a generated key number. Connected tokens utilize a variety of interfaces including USB, near-field communication (NFC), radio-frequency identification (RFID), or Bluetooth. Some tokens have an audio capability designed for vision-impaired people.

Password types

All tokens contain some secret information that is used to prove identity. There are four different ways in which this information can be used:

- **Static password token** - The device contains a password which is physically hidden (not visible to the possessor), but which is transmitted for each authentication. This type is vulnerable to replay attacks.
- **Synchronous dynamic password token** - A timer is used to rotate through various combinations produced by a cryptographic algorithm. The token and the authentication server must have synchronized clocks.
- **Asynchronous password token** - A one-time password is generated without the use of a clock, either from a one-time pad or cryptographic algorithm.
- **Challenge response token** - Using public key cryptography, it is possible to prove possession of a private key without revealing that key. The authentication server encrypts a challenge (typically a random number, or at least data with some random parts) with a public key; the device proves it possesses a copy of the matching private key by providing the decrypted challenge.

One-time passwords

Time-synchronized one-time passwords change constantly at a set time interval; e.g., once per minute. To do this some sort of synchronization must exist between the client's token and the authentication server. For disconnected tokens this time-synchronization is done before the token is distributed to the client. Other token types do the synchronization when the token is inserted into an input device. The main problem with time-synchronized tokens is that they can, over time, become unsynchronized. However, some such systems, such as RSA's SecurID, allow the user to resynchronize the server with the token, sometimes by entering several consecutive passcodes. Most also cannot have replaceable batteries and only last up to 5 years before having to be replaced – so there is additional cost.

Another type of one-time password uses a complex mathematical algorithm, such as a hash chain, to generate a series of one-time passwords from a secret shared key. Each password is unguessable, even when previous passwords are known. The open source OAuth algorithm is standardized; other algorithms are covered by US patents. Each password is observably unpredictable and independent of previous ones, whereby an adversary would be unable to guess what the next password may be, even with knowledge of all previous passwords.

Physical types

Tokens can contain chips with functions varying from very simple to very complex, including multiple authentication methods.

The simplest security tokens do not need any connection to a computer. The tokens have a physical display; the authenticating user simply enters the displayed number to log in. Other tokens connect to the computer using wireless techniques, such as Bluetooth. These tokens transfer a key sequence to the local client or to a nearby access point.

Alternatively, another form of token that has been widely available for many years is a mobile device which communicates using an out-of-band channel (like voice, SMS, or USSD).

Still other tokens plug into the computer, and may require a PIN. Depending on the type of the token, the computer OS will then either read the key from the token and perform a cryptographic operation on it, or ask the token's firmware to perform this operation.

A related application is the hardware dongle required by some computer programs to prove ownership of the software. The dongle is placed in an input device and the software accesses the I/O device in question to authorize the use of the software in question.

Commercial solutions are provided by a variety of vendors, each with their own proprietary (and often patented) implementation of variously used security features. Token designs meeting certain security standards are certified in the United States as compliant with FIPS 140, a federal security standard. Tokens without any kind of certification are sometimes viewed as suspect, as they often do not meet accepted government or industry security standards, have not been put through rigorous testing, and likely cannot provide the same level of cryptographic security as token solutions which have had their designs independently audited by third-party agencies.

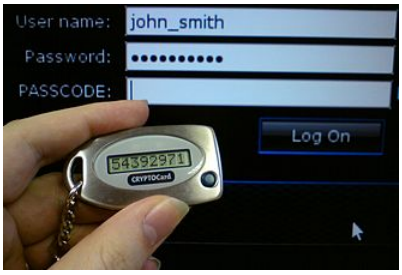


Figure **2.3.3.1**: A disconnected token. The number must be copied into the PASSCODE field by hand. ("Disconnected Token" by Multiple Contributors, Wikipedia is licensed under CC BY-SA 3.0)

Disconnected tokens

Disconnected tokens have neither a physical nor logical connection to the client computer. They typically do not require a special input device, and instead use a built-in screen to display the generated authentication data, which the user enters manually themselves via a keyboard or keypad. Disconnected tokens are the most common type of security token used (usually in combination with a password) in two-factor authentication for online identification.

Connected tokens

Connected tokens are tokens that must be physically connected to the computer with which the user is authenticating. Tokens in this category automatically transmit the authentication information to the client computer once a physical connection is made, eliminating the need for the user to manually enter the authentication information. However, in order to use a connected token, the appropriate input device must be installed. The most common types of physical tokens are smart cards and USB tokens, which require a smart card reader and a USB port respectively. Increasingly, Universal 2nd Factor (U2F) tokens, supported by the open specification group FIDO Alliance have become popular for consumers with mainstream browser support beginning in 2015 and supported by popular websites and social media sites.

Older PC card tokens are made to work primarily with laptops. Type II PC Cards are preferred as a token as they are half as thick as Type III.

The audio jack port is a relatively practical method to establish connection between mobile devices, such as iPhone, iPad and Android, and other accessories. The most well known device is called Square, a credit card reader for iPhone and Android.

Some use a special purpose interface (e.g. the crypto ignition key deployed by the United States National Security Agency). Tokens can also be used as a photo ID card. Cell phones and PDAs can also serve as security tokens with proper programming.

Smart cards

Many connected tokens use smart card technology. Smart cards can be very cheap (around ten cents) and contain proven security mechanisms (as used by financial institutions, like cash cards). However, computational performance of smart cards is often rather limited because of extreme low power consumption and ultra-thin form-factor requirements.

Smart-card-based USB tokens which contain a smart card chip inside provide the functionality of both USB tokens and smart cards. They enable a broad range of security solutions and provide the abilities and security of a traditional smart card without

requiring a unique input device. From the computer operating system's point of view such a token is a USB-connected smart card reader with one non-removable smart card present.

Contactless tokens

Unlike connected tokens, contactless tokens form a logical connection to the client computer but do not require a physical connection. The absence of the need for physical contact makes them more convenient than both connected and disconnected tokens. As a result, contactless tokens are a popular choice for keyless entry systems and electronic payment solutions such as Mobil Speedpass, which uses RFID to transmit authentication info from a keychain token. However, there have been various security concerns raised about RFID tokens after researchers at Johns Hopkins University and RSA Laboratories discovered that RFID tags could be easily cracked and cloned.

Another downside is that contactless tokens have relatively short battery lives; usually only 5–6 years, which is low compared to USB tokens which may last more than 10 years.[citation needed] Some tokens however do allow the batteries to be changed, thus reducing costs.

Bluetooth tokens

The Bluetooth Low Energy protocols serve for long lasting battery lifecycle of wireless transmission.

- The transmission of inherent Bluetooth identity data is the lowest quality for supporting authentication.
- A bidirectional connection for transactional data interchange serves for the most sophisticated authentication procedures.

However the automatic transmission power control antagonizes to attempts for radial distance estimates. The escape is available apart from the standardised Bluetooth power control algorithm to provide a calibration on minimally required transmission power.

Bluetooth tokens are often combined with a USB token, thus working in both a connected and a disconnected state. Bluetooth authentication works when closer than 32 feet (10 meters). When the Bluetooth link is not properly operable, the token may be inserted into a USB input device to function.

Another combination is with smart card to store locally larger amounts of identity data and process information as well. Another is a contactless BLE token that combines secure storage and tokenized release of fingerprint credentials.

In the USB mode of operation sign-off requires care for the token while mechanically coupled to the USB plug. The advantage with the Bluetooth mode of operation is the option of combining sign-off with distance metrics. Respective products are in preparation, following the concepts of electronic leash.

NFC tokens

Near-field communication (NFC) tokens combined with a Bluetooth token may operate in several modes, thus working in both a connected and a disconnected state. NFC authentication works when closer than 1 foot (0.3 meters). The NFC protocol bridges short distances to the reader while the Bluetooth connection serves for data provision with the token to enable authentication. Also when the Bluetooth link is not connected, the token may serve the locally stored authentication information in coarse positioning to the NFC reader and relieves from exact positioning to a connector.

Single sign-on software tokens

Some types of single sign-on (SSO) solutions, like enterprise single sign-on, use the token to store software that allows for seamless authentication and password filling. As the passwords are stored on the token, users need not remember their passwords and therefore can select more secure passwords, or have more secure passwords assigned. Usually most tokens store a cryptographic hash of the password so that if the token is compromised, the password is still protected.

Programmable tokens

Programmable tokens are marketed as "drop-in" replacement of mobile applications such as Google Authenticator (miniOTP[10]). They can be used as mobile app replacement, as well as in parallel as a backup.

CHAPTER OVERVIEW

3: Authorize and Access Control

3.1: What are access controls?

Access Controls

In computer security, general access control includes identification, authorization, authentication, access approval, and audit. A more narrow definition of access control would cover only access approval, whereby the system makes a decision to grant or reject an access request from an already authenticated subject (we will talk about the difference between authorization and authentication below), based on what the subject is authorized to access. Authentication and access control are often combined into a single operation, so that access is approved based on successful authentication, or based on an anonymous access token. Authentication methods and tokens include passwords, biometric scans, physical keys, electronic keys and devices, hidden paths, social barriers, and monitoring by humans and automated systems.

Services

Access control systems provide the essential services of authorization, identification and authentication (I&A), access approval, and accountability where:

- authorization specifies what a subject can do
- identification and authentication ensure that only legitimate subjects can log on to a system
- access approval grants access during operations, by association of users with the resources that they are allowed to access, based on the authorization policy
- accountability identifies what a subject (or all subjects associated with a user) did

Authorization

Authorization involves the act of defining access-rights for subjects. An authorization policy specifies the operations that subjects are allowed to execute within a system.

Most modern operating systems implement authorization policies as formal sets of permissions that are variations or extensions of three basic types of access:

- Read (R): The subject can
  - Read file contents
  - List directory contents
- Write (W): The subject can change the contents of a file or directory with the following tasks:
  - Add
  - Update
  - Delete
  - Rename
- Execute (X): If the file is a program, the subject can cause the program to be run. (In Unix-style systems, the "execute" permission doubles as a "traverse directory" permission when granted for a directory.)

These rights and permissions are implemented differently in systems based on discretionary access control (DAC) and mandatory access control (MAC).

Identification and authentication

Identification and authentication (I&A) is the process of verifying that an identity is bound to the entity that makes an assertion or claim of identity - in other words, if someone claims to be John Doe, they I&A make sure that it is indeed John Doe. The I&A process assumes that there was an initial validation of the identity, commonly called identity proofing. Various methods of identity proofing are available, ranging from in-person validation using government issued identification, to anonymous methods that allow the individual person/system to remain anonymous, but will be known to the system if they come back to login in the future. The method used for identity proofing and validation should provide an assurance level commensurate with the intended use of the identity within the system. Subsequently, the entity asserts an identity together with an authenticator as a means for validation. The only requirements for the identifier is that it must be unique within its security domain.

Authenticators, as were previously discussed, are commonly based on at least one of the following four factors:

- **Something you know**, such as a password or a personal identification number (PIN). This assumes that only the owner of the account knows the password or PIN needed to access the account.
- **Something you have**, such as a smart card or security token. This assumes that only the owner of the account has the necessary smart card or token needed to unlock the account.
- **Something you are**, such as fingerprint, voice, retina, or iris characteristics.
- **Where you are**, for example inside or outside a company firewall, or proximity of login location to a personal GPS device.

Access approval

Access approval is the function that actually grants or rejects access during operations.

During access approval, the system compares the formal representation of the authorization policy with the access request, to determine whether the request shall be granted or rejected. Moreover, the access evaluation can be done online/ongoing.

Accountability

Accountability uses system components such as audit trails (records) and logs, to associate a subject with its actions. The information recorded should be sufficient to map the subject to a controlling user. Audit trails and logs are important for

- Detecting security violations
- Re-creating security incidents

If no one is regularly reviewing your logs and they are not maintained in a secure and consistent manner, they may not be admissible as evidence in any type of legal proceedings.

Many systems can generate automated reports, based on certain predefined criteria or thresholds, known as clipping levels. For example, a level may be set to generate a report for the following:

- More than three failed logon attempts in a given period
- Any attempt to use a disabled user account

These reports help a system administrator or security administrator to more easily identify possible break-in attempts.

Adapted from:
"Computer access control" by Multiple Contributors, Wikipedia is licensed under CC BY-SA 3.0

3.2: Access Control - ACL

Access Control Lists

In any access-control model, the entities that can perform actions on the system are called subjects, and the entities representing resources to which access may need to be controlled are called objects. Subjects and objects should both be considered as software entities, rather than as human users: any human users can only have an effect on the system via the software entities that they control.

Although some systems equate subjects with user IDs, so that all processes started by a user by default have the same authority, this level of control is not fine-grained enough to satisfy the principle of least privilege, and arguably is responsible for the prevalence of malware in such systems (see computer insecurity).

In some models, for example the object-capability model, any software entity can potentially act as both subject and object.

As of 2014, access-control models tend to fall into one of two classes: those based on capabilities and those based on access control lists (ACLs).

- In a capability-based model, holding an unforge-able reference or capability to an object, that provides access to the object (roughly analogous to how possession of one's house key grants one access to one's house); access is conveyed to another party by transmitting such a capability over a secure channel.
- In an ACL-based model, a subject's access to an object depends on whether the subject's identity appears on a list associated with the object (roughly analogous to how a bouncer at a private party would check an ID to see if a name appears on the guest list); access is conveyed by editing the list. (Different ACL systems have a variety of different conventions regarding who or what is responsible for editing the list and how it is edited.)

Both capability-based and ACL-based models have mechanisms to allow access rights to be granted to all members of a group of subjects (often the group is itself modeled as a subject).

Filesystem ACLs

A filesystem ACL is a data structure (usually a table) containing entries that specify individual user or group rights to specific system objects such as executable programs, running processes, or files. These entries are known as access-control entries (ACEs) in the Microsoft Windows NT, OpenVMS, and Unix-like operating systems such as Linux, macOS, and Solaris. Each accessible object contains an identifier to its ACL. The privileges or permissions determine specific access rights, such as whether a user can read from, write to, or execute an object. In some implementations, an ACE can control whether or not a user, or group of users, may alter the ACL on an object.

Networking ACLs

On some types of proprietary computer-hardware (in particular routers and switches), an access-control list provides rules that are applied to port numbers or IP addresses that are available on a host or other layer 3, each with a list of hosts and/or networks permitted to use the service. Although it is additionally possible to configure access-control lists based on network domain names, this is a questionable idea because individual TCP, UDP, and ICMP headers do not contain domain names. Consequently, the device enforcing the access-control list must separately resolve names to numeric addresses. This presents an additional attack surface for an attacker who is seeking to compromise security of the system which the access-control list is protecting. Both individual servers as well as routers can have network ACLs. Access-control lists can generally be configured to control both inbound and outbound traffic, and in this context they are similar to firewalls.

Adapted from:
"Computer access control" by Multiple Contributors, Wikipedia is licensed under CC BY-SA 3.0
"Access-control list" by Multiple Contributors, Wikipedia is licensed under CC BY-SA 3.0

3.3: Access Control - Models

Access Control Models

Access control models are sometimes categorized as either discretionary or non-discretionary. The three most widely recognized models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC). MAC is non-discretionary. There are additional access control system but they are not as widely deployed as the top three.

Discretionary access control

Discretionary access control (DAC) is a policy determined by the owner of an object. The owner decides who is allowed to access the object, and what privileges they have.

Two important concepts in DAC are

- **File and data ownership**: Every object in the system has an owner. In most DAC systems, each object's initial owner is the subject that caused it to be created. The access policy for an object is determined by its owner.
- **Access rights and permissions**: These are the controls that an owner can assign to other subjects for specific resources.

Access controls may be discretionary in ACL-based or capability-based access control systems. (In capability-based systems, there is usually no explicit concept of 'owner', but the creator of an object has a similar degree of control over its access policy.)

Mandatory access control

Mandatory access control refers to allowing access to a resource if and only if rules exist that allow a given user to access the resource. It is difficult to manage, but its use is usually justified when used to protect highly sensitive information. Examples include certain government and military information. Management is often simplified (over what is required) if the information can be protected using hierarchical access control, or by implementing sensitivity labels. What makes the method "mandatory" is the use of either rules or sensitivity labels.

- **Sensitivity labels**: In such a system subjects and objects must have labels assigned to them. A subject's sensitivity label specifies its level of trust. An object's sensitivity label specifies the level of trust required for access. In order to access a given object, the subject must have a sensitivity level equal to or higher than the requested object.
- **Data import and export**: Controlling the import of information from other systems and export to other systems (including printers) is a critical function of these systems, which must ensure that sensitivity labels are properly maintained and implemented so that sensitive information is appropriately protected at all times.

Two methods are commonly used for applying mandatory access control:

- **Rule-based (or label-based) access control**: This type of control further defines specific conditions for access to a requested object. A Mandatory Access Control system implements a simple form of rule-based access control to determine whether access should be granted or denied by matching:
  - An object's sensitivity label
  - A subject's sensitivity label
- **Lattice-based access control**: These can be used for complex access control decisions involving multiple objects and/or subjects. A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object.

Few systems implement MAC; systems based on the operating systems XTS-400 and SELinux are examples of systems that do.

Role-based access control

Role-based access control (RBAC) is an access policy determined by the system, not by the owner. RBAC is used in commercial applications and also in military systems, where multi-level security requirements may also exist. RBAC differs from DAC in that DAC allows users to control access to their resources, while in RBAC, access is controlled at the system level, outside of the user's control. Although RBAC is non-discretionary, it can be distinguished from MAC primarily in the way permissions are handled. MAC controls read and write permissions based on a user's clearance level and additional labels. RBAC controls collections of

permissions that may include complex operations such as an e-commerce transaction, or may be as simple as read or write. A role in RBAC can be viewed as a set of permissions.

Three primary rules are defined for RBAC:

- **Role assignment**: A subject can execute a transaction only if the subject has selected or been assigned a suitable role.
- **Role authorization**: A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.
- **Transaction authorization**: A subject can execute a transaction only if the transaction is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can execute only transactions for which they are authorized.

Additional constraints may be applied as well, and roles can be combined in a hierarchy where higher-level roles subsume permissions owned by lower-level sub-roles.

Most IT vendors offer RBAC in one or more products.

Attribute-based access control

In attribute-based access control (ABAC), access is granted not based on the rights of the subject associated with a user after authentication, but based on the attributes of the user. The user has to prove so-called claims about his or her attributes to the access control engine. An attribute-based access control policy specifies which claims need to be satisfied in order to grant access to an object. For instance the claim could be "older than 18". Any user that can prove this claim is granted access. Users can be anonymous when authentication and identification are not strictly required. One does, however, require means for proving claims anonymously. This can for instance be achieved using anonymous credentials. XACML (extensible access control markup language) is a standard for attribute-based access control. XACML 3.0 was standardized in January 2013.

Break-Glass Access Control Models

Traditionally, access has the purpose of restricting access, thus most access control models follow the "default deny principle", i.e. if a specific access request is not explicitly allowed, it will be denied. This behavior might conflict with the regular operations of a system. In certain situations, humans are willing to take the risk that might be involved in violating an access control policy, if the potential benefit that can be achieved outweighs this risk. This need is especially visible in the health-care domain, where a denied access to patient records can cause the death of a patient. Break-Glass (also called break-the-glass) try to mitigate this by allowing users to override access control decision. Break-Glass can either be implemented in an access control specific manner (e.g. into RBAC), or generic (i.e., independent from the underlying access control model).

Adapted from:
"Computer access control" by Multiple Contributors, Wikipedia is licensed under CC BY-SA 3.0

3.4: Physical Controls

Physical Security

The term access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. Physical access control can be achieved by a human (a guard, bouncer, or receptionist), through mechanical means such as locks and keys, or through technological means such as access control systems like the mantrap. Within these environments, physical key management may also be employed as a means of further managing and monitoring access to mechanically keyed areas or access to certain small assets.

Physical access control is a matter of who, where, and when. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. Historically, this was partially accomplished through keys and locks. When a door is locked, only someone with a key can enter through the door, depending on how the lock is configured. Mechanical locks and keys do not allow restriction of the key holder to specific times or dates. Mechanical locks and keys do not provide records of the key used on any specific door, and the keys can be easily copied or transferred to an unauthorized person. When a mechanical key is lost or the key holder is no longer authorized to use the protected area, the locks must be re-keyed.

Electronic access control

Electronic access control (EAC) uses computers to solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. The electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked.

When a credential is presented to a reader, the reader sends the credential's information, usually a number, to a control panel, a highly reliable processor. The control panel compares the credential's number to an access control list, grants or denies the presented request, and sends a transaction log to a database. When access is denied based on the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as a flashing red LED for an access denied and a flashing green LED for an access granted.

The above description illustrates a single factor transaction. Credentials can be passed around, thus subverting the access control list. For example, Alice has access rights to the server room, but Bob does not. Alice either gives Bob her credential, or Bob takes it; he now has access to the server room. To prevent this, two-factor authentication can be used. In a two factor transaction, the presented credential and a second factor are needed for access to be granted; another factor can be a PIN, a second credential, operator intervention, or a biometric input.

There are three types (factors) of authenticating information:

- something the user knows, e.g. a password, pass-phrase or PIN
- something the user has, such as smart card or a key fob
- something the user is, such as fingerprint, verified by biometric measurement

Passwords are a common means of verifying a user's identity before access is given to information systems. In addition, a fourth factor of authentication is now recognized: someone you know, whereby another person who knows you can provide a human element of authentication in situations where systems have been set up to allow for such scenarios. For example, a user may have their password, but have forgotten their smart card. In such a scenario, if the user is known to designated cohorts, the cohorts may provide their smart card and password, in combination with the extant factor of the user in question, and thus provide two factors for the user with the missing credential, giving three factors overall to allow access.

Adapted from:
"Access control" by Multiple Contributors, Wikipedia is licensed under CC BY-SA 3.0

3.4.1: Physical Controls (continued)

Credential

A credential is a physical/tangible object, a piece of knowledge, or a facet of a person's physical being that enables an individual access to a given physical facility or computer-based information system. Typically, credentials can be something a person knows (such as a number or PIN), something they have (such as an access badge), something they are (such as a biometric feature), something they do (measurable behavioral patterns) or some combination of these items. This is known as multi-factor authentication. The typical credential is an access card or key-fob, and newer software can also turn users' smartphones into access devices.

There are many card technologies including magnetic stripe, bar code, Wiegand, kHz proximity, -bit card-swipe, contact smart cards, and contactless smart cards. Also available are key-fobs, which are more compact than ID cards, and attach to a key ring. Biometric technologies include fingerprint, facial recognition, iris recognition, retinal scan, voice, and hand geometry. The built-in biometric technologies found on newer smartphones can also be used as credentials in conjunction with access software running on mobile devices. In addition to older more traditional card access technologies, newer technologies such as Near field communication (NFC), Bluetooth low energy or Ultra-wideband (UWB) can also communicate user credentials to readers for system or building access.

Access control system components

Components of an access control system include:

- An access control panel (also known as a controller)
- An access-controlled entry, such as a door, turnstile, parking gate, elevator, or other physical barrier
- A reader installed near the entry. (In cases where the exit is also controlled, a second reader is used on the opposite side of the entry.)
- Locking hardware, such as electric door strikes and electromagnetic locks
- A magnetic door switch for monitoring door position
- Request-to-exit (RTE) devices for allowing egress. When a RTE button is pushed, or the motion detector detects motion at the door, the door alarm is temporarily ignored while the door is opened. Exiting a door without having to electrically unlock the door is called mechanical free egress. This is an important safety feature. In cases where the lock must be electrically unlocked on exit, the request-to-exit device also unlocks the door.

Security risks

The most common security risk of intrusion through an access control system is by simply following a legitimate user through a door, and this is referred to as tailgating. Often the legitimate user will hold the door for the intruder. This risk can be minimized through security awareness training of the user population or more active means such as turnstiles. In very high-security applications this risk is minimized by using a sally port, sometimes called a security vestibule or mantrap, where operator intervention is required presumably to assure valid identification.tation needed

The second most common risk is from levering a door open. This is relatively difficult on properly secured doors with strikes or high holding force magnetic locks. Fully implemented access control systems include forced door monitoring alarms. These vary in effectiveness, usually failing from high false positive alarms, poor database configuration, or lack of active intrusion monitoring. Most newer access control systems incorporate some type of door prop alarm to inform system administrators of a door left open longer than a specified length of time.tation needed

The third most common security risk is natural disasters. In order to mitigate risk from natural disasters, the structure of the building, down to the quality of the network and computer equipment vital. From an organizational perspective, the leadership will need to adopt and implement an All Hazards Plan, or Incident Response Plan. The highlights of any incident plan determined by the National Incident Management System must include Pre-incident planning, during incident actions, disaster recovery, and after-action review.

Spoofing locking hardware is fairly simple and more elegant than levering. A strong magnet can operate the solenoid controlling bolts in electric locking hardware. Motor locks, more prevalent in Europe than in the US, are also susceptible to this attack using a

doughnut-shaped magnet. It is also possible to manipulate the power to the lock either by removing or adding current, although most Access Control systems incorporate battery back-up systems and the locks are almost always located on the secure side of the door.tation needed

Access cards themselves have proven vulnerable to sophisticated attacks. Enterprising hackers have built portable readers that capture the card number from a user's proximity card. The hacker simply walks by the user, reads the card, and then presents the number to a reader securing the door. This is possible because card numbers are sent in the clear, no encryption being used. To counter this, dual authentication methods, such as a card plus a PIN should always be used.

Many access control credentials unique serial numbers are programmed in sequential order during manufacturing. Known as a sequential attack, if an intruder has a credential once used in the system they can simply increment or decrement the serial number until they find a credential that is currently authorized in the system. Ordering credentials with random unique serial numbers is recommended to counter this threat.

Finally, most electric locking hardware still has mechanical keys as a fail-over. Mechanical key locks are vulnerable to bumping.

Adapted from:

CHAPTER OVERVIEW

4: Accountability and Auditing

4.1: Accountability

When we are discussing accountability we need to define what that really means. An acceptable meaning would be to hold people accountable for their actions, to be able to trace all activities in the corporate environment back to the source of those activities. This means the is the ability to use identification, authentication, and authorization processes in order to know which user a given event is associated with and what permissions allowed them to carry it out.

It can be quite easy to criticize accountability and its associated auditing tools. It could be argued that implementing surveillance techniques is like having Big Brother watching over your every move. This might be true in certain instances - if people are monitored excessively, it is possible to create an unhealthy environment.

Accountability Benefits

When people are held accountable, it can keep the corporate environment secure in several ways: it enables a principle called nonrepudiation, it deters those who would otherwise misuse resources, and it detects and prevents intrusions. The processes are used to ensure accountability and can also assist in the preparation materials for legal proceedings.

Non-repudiation

In general, non-repudiation involves associating actions or changes with a unique individual. For example, a secure area may use a key card access system where non-repudiation would be violated if key cards were shared or if lost and stolen cards were not immediately reported. Similarly, the owner of a computer account must not allow others to use it, such as by giving away their password, and a policy should be implemented to enforce this.

In digital security, non-repudiation means:

- A service that provides proof of the integrity and origin of data.
- An authentication that can be said to be genuine with high confidence.
- An authentication that the data is available under specific circumstances, or for a period of time: data availability.

Proof of data integrity is typically the easiest of these requirements to accomplish. A data hash such as SHA2 usually ensures that the data will not be changed undetectably. Even with this safeguard, it is possible to tamper with data in transit, either through a man-in-the-middle attack or phishing. Because of this, data integrity is best asserted when the recipient already possesses the necessary verification information, such as after being mutually authenticated.

The common method to provide non-repudiation in the context of digital communications or storage is Digital Signatures, a more powerful tool that provides non-repudiation in a publicly verifiable manner. Message Authentication Codes (MAC), useful when the communicating parties have arranged to use a shared secret that they both possess, does not give non-repudiation. A misconception is that encrypting, per se, provides authentication "If the message decrypts properly then it is authentic" - Wrong! MAC can be subject to several types of attacks, like: message reordering, block substitution, block repetition, ... Thus just providing message integrity and authentication, but not non-repudiation. To achieve non-repudiation one must trust a service (a certificate generated by a trusted third party (TTP) called certificate authority (CA)) which prevents an entity from denying previous commitments or actions (e.g. sending message A to B). The difference between MAC and Digital Signatures, one uses symmetric keys and the other asymmetric keys (provided by the CA). Note that the goal is not to achieve confidentiality: in both cases (MAC or digital signature), one simply appends a tag to the otherwise plaintext, visible message. If confidentiality is also required, then an encryption scheme can be combined with the digital signature, or some form of authenticated encryption could be used. Verifying the digital origin means that the certified/signed data likely came from someone who possesses the private key corresponding to the signing certificate. If the key used to digitally sign a message is not properly safeguarded by the original owner, digital forgery can occur.

Deterrence

Deterrence is a strategy to influence the behaviour of people to follow a certain policy using the fear of sanctions. Deterrence is a strategy to influence the behaviour of people to follow a certain policy using the fear of sanctions. Therefore, it is composed of two main concepets: the certainty of sanctions and the severity of those sanctions . In other words, people desert unwelcome actions if

they feel the probability of being apprehended is high (certainty of sanctions) and/or the extent of the potential penalty is to high (severity of sanctions).

From the viewpoint of the certainty of sanctions, in the past we have seen employees were aware that sanctions existed as a result of violations and the presence of detection efforts was quite effective in deterring the abuse of information systems and the violation of security policies. Recently, it is reported that security policies are violated when the benefit of violation is more substantial than the sanction that would be imposed, or a neutralization technique is involved . The implication is that organizations should not rely solely on employee awareness of sanctions because violations will occur regardless of the emphasis on the sanctions. Organizations are required to use detection as a practical method to increase the probability of being able to identify every violation. The most powerful way of increasing the certainty of sanctions is to find every violation and identifying the violator. Therefore, the certainty of sanctions should be viewed from the perspectives of detection as well as awareness.

Regarding the severity of sanctions, the sort of sanctions considered was solely punishment with various degrees. It can be argued that the sole application of punishment has no influence on deterring violations . The method of sanctions began to extend from simple punishment, to include other methods such as shame, informal sanctions, self-control, moral beliefs, and general deterrence based on rational choice . So, the severity of sanctions needs to be approached not only from the existing concept of the intensity of sanctions, but should also include a variety of sanctions.

Intrusion Detection and Prevention

The evolution of malicious software (malware) poses a critical challenge to the design of intrusion detection systems (IDS). Malicious attacks have become more sophisticated and the foremost challenge is to identify unknown and obfuscated malware, as the malware authors use different evasion techniques for information concealing to prevent detection by an IDS. In addition, there has been an increase in security threats such as zero-day attacks designed to target internet users. Therefore, computer security has become essential as the use of information technology has become part of our daily lives.

Intrusion can be defined as any kind of unauthorised activities that cause damage to an information system. This means any attack that could pose a possible threat to the information confidentiality, integrity or availability will be considered an intrusion. For example, activities that would make the computer services unresponsive to legitimate users are considered an intrusion. An IDS is a software or hardware system that identifies malicious actions on computer systems in order to allow for system security to be maintained (Liao et al., 2013a). The goal of an IDS is to identify different kinds of malicious network traffic and computer usage, which cannot be identified by a traditional firewall. This is vital to achieving high protection against actions that compromise the availability, integrity, or confidentiality of computer systems. IDS systems can be broadly categorized into two groups: Signature-based Intrusion Detection System (SIDS) and Anomaly-based Intrusion Detection System (AIDS).

Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPS have become a necessary addition to the security infrastructure of nearly every organization.

IDPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPS can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

Intrusion prevention systems (**IPS**), also known as **intrusion detection and prevention systems** (**IDPS**), are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it, and attempt to block or stop it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection, or blocking traffic from the offending IP address. An

IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues, and clean up unwanted transport and network layer options.

Admissibility of Records

Admissible evidence, in a court of law, is any testimonial, documentary, or tangible evidence that may be introduced to a factfinder—usually a judge or jury—to establish or to bolster a point put forth by a party to the proceeding. For evidence to be admissible, it must be relevant and "not excluded by the rules of evidence", which generally means that it must not be unfairly prejudicial, and it must have some indicia of reliability. The general rule in evidence is that all relevant evidence is admissible and all irrelevant evidence is inadmissible.

A record should correctly reflect what was communicated or decided or what action was taken. Records management policies, procedures and practices should lead to authoritative records that have the following characteristics:

- **Authenticity**—An authentic record is one that can be proven to:
  – Be what it purports to be
  – Have been created or sent by the person purported to have created or sent it
  – Have been created or sent at the time purported
- **Reliability**—A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities. Records should be created at the time of the transaction or incident to which they relate, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.
- **Integrity**—The integrity of a record refers to it being complete and unaltered. It is necessary that a record be protected against unauthorized alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.
  If the information is going to be used in a criminal proceeding, organizations must be able to identify who has had access to a particular record at any given time from collection, to creation of the evidence copy, to presentation as evidence. The evidentiary weighting of records will be substantially reduced if the chain of custody cannot be adequately established or is discredited.
- **Usability**—A useable record is one that can be located, retrieved, presented and interpreted. It should be directly connected to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of activities should be maintained.

The topic of electronic record management is a course in itself, and is to broad to be completely covered in this chapter.

4.2: Auditing

An information security audit is an audit on the level of information security in an organization. It is an independent review and examination of system records, activities and related documents. These audits are intended to improve the level of information security, avoid improper information security designs, and optimize the efficiency of the security safeguards and security processes. Within the broad scope of auditing information security there are multiple types of audits, multiple objectives for different audits, etc. Most commonly the controls being audited can be categorized to technical, physical and administrative. Auditing information security covers topics from auditing the physical security of data centers to auditing the logical security of databases, and highlights key components to look for and different methods for auditing these areas.

When centered on the Information technology (IT) aspects of information security, it can be seen as a part of an information technology audit. It is often then referred to as an information technology security audit or a computer security audit. However, information security encompasses much more than IT.

Internal audit versus external audit

Every audit conducted is either an external audit or an internal audit.

An external audit is conducted by a certified professional independent from the organization being audited. The intention of performing an external audit is to gather the most impartial results possible. External auditors provide a variety of services. They review an organization's information systems, security procedures, financial reporting, and compliance methodology to determine efficacy and identify security gaps.

An internal audit is generally used as a management tool to improve internal processes and controls. Internal audits are to be completed independently and objectively, to ensure compliance of a given business operation to standards set by the organization, regulatory body, or government.

The main features of an internal audit are:

- They're voluntary.
- They're conducted internally by a member of your business/organization.

Adapted from:
"Information security audit" by Various authors, Wikipedia is licensed under CC BY-SA 3.0

4.2.1: Information Security Audit

Phases of the Audit process

An information security audit is comprised of 6 steps. Depending on what source is consulted, there may be more or less than 6 steps, they may be named differently, and they may be in a slightly different order.

Preliminary audit assessment

The auditor is responsible for assessing the current technological maturity level of a company during the first stage of the audit. This stage is used to assess the current status of the company and helps identify the required time, cost and scope of an audit. First, identify the minimum security requirements:

- Security policy and standards
- Organizational and Personal security
- Communication, Operation and Asset management
- Physical and environmental security
- Access control and Compliance
- IT systems development and maintenance
- IT security incident management
- Disaster recovery and business continuity management
- Risk management

The auditor also has the task of gathering knowledge and inputs on the following aspects of the object to be audited:

- Organization’s operating environment and its function.
- The criticality of the IT system, whether it is a mission-critical system or a support system
- Structure of the organization
- Nature of software and hardware in use
- Nature and extent of the perils affecting the organization

Planning & preparation

The auditor should plan a company's audit based on the information found in previous step. Planning an audit helps the auditor obtain sufficient and appropriate evidence for each company's specific circumstances. It helps predict audit costs at a reasonable level, assign the proper manpower and time line and avoid misunderstandings with clients.

An auditor should be adequately educated about the company and its critical business activities before conducting a data center review. The objective of the data center is to align data center activities with the goals of the business while maintaining the security and integrity of critical information and processes. To adequately determine whether the client's goal is being achieved, the auditor should perform the following before conducting the review:

- Meet with IT management to determine possible areas of concern
- Review the current IT organization chart
- Review job descriptions of data center employees
- Research all operating systems, software applications, and data center equipment operating within the data center
- Review the company's IT policies and procedures
- Evaluate the company's IT budget and systems planning documentation
- Review the data center's disaster recovery plan

Adapted from:
"Information security audit" by Various authors, Wikipedia is licensed under CC BY-SA 3.0

4.2.2: Information Security Audit (continued)

Establishing audit objectives

In this step, the auditor outlines the objectives of the audit. Auditors consider multiple factors that relate to data center procedures and activities that potentially identify audit risks in the operating environment and assess the controls in place that mitigate those risks. The initial risk assessment forms an important part of the process and answers questions pertaining to three primary security goals, confidentiality, integrity, and reliability. After thorough testing and analysis, the auditor is able to adequately determine if the data center maintains proper controls and is operating efficiently and effectively.

Risk assessment consists of ranking the potential threats from low to high, or other scientific or complex metrics. The ranking depends on the severity of the issue with respect to the extent of damage it can cause or the ease of exploitation. Vulnerabilities that are easy to exploit and those causing a high degree of damage must be ranked comparatively higher.

Following is a list of objectives the auditor should review:

- Personnel procedures and responsibilities, including systems and cross-functional training
- Change management processes are in place and followed by IT and management personnel
- Appropriate back up procedures are in place to minimize downtime and prevent loss of important data
- The data center has adequate physical security controls to prevent unauthorized access to the data center
- Adequate environmental controls are in place to ensure equipment is protected from fire and flooding
- Review of security infrastructure and systems
- Review of IT systems to gain assurance of the safety
- Examine the development process and procedures involved at various stages of the system
- Evaluation of the performance of a specific program or system

Audit objectives and scope are not limited to the aspects mentioned above. It should be able to cover all the critical areas of the security aspect, such as security settings, passwords, firewall security, user rights, physical access security, and so on.

Performing the review

Collecting evidence is required in order to satisfy data center audit objectives. This involves traveling to the data center location and observing processes and within the data center.

The three main types of audit evidence include:

- Documentary audit evidence
- Analysis
- Observed process and existence of physical items

Physical verification implies the actual investigation or inspection of tangible assets by the auditor. The following methods can be used for the collection of audit evidence.

The following review procedures should be conducted to satisfy the pre-determined audit objectives:

- Data centre personnel – All data center personnel should be authorized to access the data center (key cards, login ID's, secure passwords, etc.). Datacenter employees are adequately educated about data center equipment and properly perform their jobs. Vendor service personnel are supervised when doing work on data center equipment. The auditor should observe and interview data center employees to satisfy their objectives.
- Equipment – The auditor should verify that all data center equipment is working properly and effectively. Equipment utilization reports, equipment inspection for damage and functionality, system downtime records and equipment performance measurements all help the auditor determine the state of data center equipment. Additionally, the auditor should interview employees to determine if preventative maintenance policies are in place and performed.
- Policies and Procedures – All data center policies and procedures should be documented and located at the data center. Important documented procedures include data center personnel job responsibilities, back up policies, security policies, employee termination policies, system operating procedures and an overview of operating systems.

- Physical security / environmental controls – The auditor should assess the security of the client's data center. Physical security includes bodyguards, locked cages, man traps, single entrances, bolted-down equipment, and computer monitoring systems. Additionally, environmental controls should be in place to ensure the security of data center equipment. These include Air conditioning units, raised floors, humidifiers and uninterruptible power supply.
- Backup procedures – The auditor should verify that the client has backup procedures in place in the case of system failure. Clients may maintain a backup data center at a separate location that allows them to instantaneously continue operations in the instance of system failure

Adapted from:
"Information security audit" by Various authors, Wikipedia is licensed under CC BY-SA 3.0

4.2.3: Information Security Audit (continued)

Preparing the Audit Report

After the audit examination is completed, the audit findings and suggestions for corrective actions can be communicated to responsible stakeholders in a formal meeting. This ensures better understanding and support of the audit recommendations. It also gives the audited organization an opportunity to express its views on the issues raised.

Writing a report after such a meeting and describing where agreements have been reached on all audit issues can greatly enhance audit effectiveness. Exit conferences also help finalize recommendations that are practical and feasible.

Issuing the review report

The data center review report should summarize the auditor's findings and be similar in format to a standard review report. The review report should be dated as of the completion of the auditor's inquiry and procedures. It should state what the review entailed and explain that a review provides only "limited assurance" to third parties.

Typically, a data center review report consolidates the entirety of the audit. It also offers recommendations surrounding proper implementation of physical safeguards and advises the client on appropriate roles and responsibilities of its personnel. Its contents may include:

- The auditors' procedures and findings
- The auditors' recommendations
- Objective, scope, and methodologies
- Overview/conclusions

The report may optionally include rankings of the security vulnerabilities identified throughout the performance of the audit and the urgency of the tasks necessary to address them. Rankings like "high", "low", and "medium" can be used to describe the imperativeness of the tasks.

Adapted from:
"Information security audit" by Various authors, Wikipedia is licensed under CC BY-SA 3.0

4.3: Audited Systems

Network vulnerabilities

- Interception: Data that is being transmitted over the network is vulnerable to being intercepted by an unintended third party who could put the data to harmful use.
- Availability: Networks have become wide-spanning, crossing hundreds or thousands of miles which many rely on to access company information, and lost connectivity could cause business interruption.
- Access/entry point: Networks are vulnerable to unwanted access. A weak point in the network can make that information available to intruders. It can also provide an entry point for viruses and Trojan horses.

Controls

- Interception controls: Interception can be partially deterred by physical access controls at data centers and offices, including where communication links terminate and where the network wiring and distributions are located. Encryption also helps to secure wireless networks.
- Availability controls: The best control for this is to have excellent network architecture and monitoring. The network should have redundant paths between every resource and an access point and automatic routing to switch the traffic to the available path without loss of data or time.
- Access/entry point controls: Most network controls are put at the point where the network connects with an external network. These controls limit the traffic that passes through the network. These can include firewalls, intrusion detection systems, and antivirus software.

The auditor should ask certain questions to better understand the network and its vulnerabilities. The auditor should first assess the extent of the network is and how it is structured. A network diagram can assist the auditor in this process. The next question an auditor should ask is what critical information this network must protect. Things such as enterprise systems, mail servers, web servers, and host applications accessed by customers are typically areas of focus. It is also important to know who has access and to what parts. Do customers and vendors have access to systems on the network? Can employees access information from home? Lastly, the auditor should assess how the network is connected to external networks and how it is protected. Most networks are at least connected to the internet, which could be a point of vulnerability. These are critical questions in protecting networks.

Segregation of duties

When you have a function that deals with money either incoming or outgoing it is very important to make sure that duties are segregated to minimize and hopefully prevent fraud. One of the key ways to ensure proper segregation of duties (SoD) from a systems perspective is to review individuals' access authorizations. Certain systems such as SAP claim to come with the capability to perform SoD tests, but the functionality provided is elementary, requiring very time-consuming queries to be built and is limited to the transaction level only with little or no use of the object or field values assigned to the user through the transaction, which often produces misleading results. For complex systems such as SAP, it is often preferred to use tools developed specifically to assess and analyze SoD conflicts and other types of system activity. For other systems or for multiple system formats you should monitor which users may have superuser access to the system giving them unlimited access to all aspects of the system. Also, developing a matrix for all functions highlighting the points where proper segregation of duties has been breached will help identify potential material weaknesses by cross-checking each employee's available accesses. This is as important if not more so in the development function as it is in production. Ensuring that people who develop the programs are not the ones who are authorized to pull it into production is key to preventing unauthorized programs into the production environment where they can be used to perpetrate fraud.

Adapted from:
"Information security audit" by Various authors, Wikipedia is licensed under CC BY-SA 3.0

4.4: Types of Audits

Encryption and IT audit

In assessing the need for a client to implement encryption policies for their organization, the Auditor should conduct an analysis of the client's risk and data value. Companies with multiple external users, e-commerce applications, and sensitive customer/employee information should maintain rigid encryption policies aimed at encrypting the correct data at the appropriate stage in the data collection process.

Auditors should continually evaluate their client's encryption policies and procedures. Companies that are heavily reliant on e-commerce systems and wireless networks are extremely vulnerable to theft and loss of critical information in transmission. Policies and procedures should be documented and carried out to ensure that all transmitted data is protected.

The auditor should verify that management has controls in place over the data encryption management process. Access to keys should require dual control, keys should be composed of two separate components and should be maintained on a computer that is not accessible to programmers or outside users. Furthermore, management should attest that encryption policies ensure data protection at the desired level and verify that the cost of encrypting the data does not exceed the value of the information itself. All data that is required to be maintained for an extensive amount of time should be encrypted and transported to a remote location. Procedures should be in place to guarantee that all encrypted sensitive information arrives at its location and is stored properly. Finally, the auditor should attain verification from management that the encryption system is strong, not attackable, and compliant with all local and international laws and regulations.

Logical security audit

Just as it sounds, a logical security audit follows a format in an organized procedure. The first step in an audit of any system is to seek to understand its components and its structure. When auditing logical security the auditor should investigate what security controls are in place, and how they work. In particular, the following areas are key points in auditing logical security:

- Passwords: Every company should have written policies regarding passwords, and employees' use of them. Passwords should not be shared and employees should have mandatory scheduled changes. Employees should have user rights that are in line with their job functions. They should also be aware of proper log on/ log off procedures. Also helpful are security tokens, small devices that authorized users of computer programs or networks carry to assist in identity confirmation. They can also store cryptographic keys and biometric data. The most popular type of security token (RSA's SecurID) displays a number that changes every minute. Users are authenticated by entering a personal identification number and the number on the token.
- Termination Procedures: Proper termination procedures so that, old employees can no longer access the network. This can be done by changing passwords and codes. Also, all id cards and badges that are in circulation should be documented and accounted for.
- Special User Accounts: Special User Accounts and other privileged accounts should be monitored and have proper controls in place.
- Remote Access: Remote access is often a point where intruders can enter a system. The logical security tools used for remote access should be very strict. Remote access should be logged.

Specific tools used in network security

Network security is achieved by various tools including firewalls and proxy servers, encryption, logical security and access controls, anti-virus software, and auditing systems such as log management.

Firewalls are a very basic part of network security. They are often placed between the private local network and the internet. Firewalls provide a flow-through for traffic in which it can be authenticated, monitored, logged, and reported. Some different types of firewalls include network layer firewalls, screened subnet firewalls, packet filter firewalls, dynamic packet filtering firewalls, hybrid firewalls, transparent firewalls, and application-level firewalls.

The process of encryption involves converting plain text into a series of unreadable characters known as the ciphertext. If the encrypted text is stolen or attained while in transit, the content is unreadable to the viewer. This guarantees secure transmission and is extremely useful to companies sending/receiving critical information. Once encrypted information arrives at its intended recipient, the decryption process is deployed to restore the ciphertext back to plaintext.

Proxy servers hide the true address of the client workstation and can also act as a firewall. Proxy server firewalls have special software to enforce authentication. Proxy server firewalls act as a middle man for user requests.

Antivirus software programs such as McAfee and Symantec software locate and dispose of malicious content. These virus protection programs run live updates to ensure they have the latest information about known computer viruses.

Logical security includes software safeguards for an organization's systems, including user ID and password access, authentication, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation.

Auditing systems, track and record what happens over an organization's network. Log Management solutions are often used to centrally collect audit trails from heterogeneous systems for analysis and forensics. Log management is excellent for tracking and identifying unauthorized users that might be trying to access the network, and what authorized users have been accessing in the network and changes to user authorities. Software that record and index user activities within window sessions such as ObserveIT provide a comprehensive audit trail of user activities when connected remotely through terminal services, Citrix and other remote access software.

Behavioral audit

Vulnerabilities in an organization's IT systems are often not attributed to technical weaknesses, but rather related to individual behavior of employees within the organization. A simple example of this is users leaving their computers unlocked or being vulnerable to phishing attacks. As a result, a thorough InfoSec audit will frequently include a penetration test in which auditors attempt to gain access to as much of the system as possible, from both the perspective of a typical employee as well as an outsider. A behavioral audit ensures preventative measures are in place such as a phishing webinar, where employees are made aware of what phishing is and how to detect it.

Adapted from:
"Information security audit" by Various authors, Wikipedia is licensed under CC BY-SA 3.0

4.5: Auditing Application Security

Application security

Application Security centers on three main functions:

- Programming
- Processing
- Access

When it comes to programming it is important to ensure proper physical and password protection exists around servers and mainframes for the development and update of key systems. Having physical access security at one's data center or office such as electronic badges and badge readers, security guards, choke points, and security cameras is vitally important to ensuring the security of applications and data. Then one needs to have security around changes to the system. Those usually have to do with proper security access to make the changes and having proper authorization procedures in place for pulling programming changes from development through test and finally into production.

With processing, it is important that procedures and monitoring of a few different aspects such as the input of falsified or erroneous data, incomplete processing, duplicate transactions and untimely processing are in place. Making sure that input is randomly reviewed or that all processing has proper approval is a way to ensure this. It is important to be able to identify incomplete processing and ensure that proper procedures are in place for either completing it or deleting it from the system if it was in error. There should also be procedures to identify and correct duplicate entries. Finally, when it comes to processing that is not being done on a timely basis one should back-track the associated data to see where the delay is coming from and identify whether or not this delay creates any control concerns.

Finally, access, it is important to realize that maintaining network security against unauthorized access is one of the major focuses for companies as threats can come from a few sources. First, one have internal unauthorized access. It is very important to have system access passwords that must be changed regularly and that there is a way to track access and changes so one is able to identify who made what changes. All activity should be logged. The second arena to be concerned with is remote access, people accessing one's system from the outside through the internet. Setting up firewalls and password protection to on-line data changes are key to protecting against unauthorized remote access. One way to identify weaknesses in access controls is to bring in a hacker to try and crack one's system by either gaining entry to the building and using an internal terminal or hacking in from the outside through remote access.

Adapted from:
"Information security audit" by Various authors, Wikipedia is licensed under CC BY-SA 3.0

CHAPTER OVERVIEW

6: Compliance , Laws and Regulations

6.1: Introduction

It is very important for information security professionals to understand the role laws and regulations play, as well as how compliance might impact the entities for which we work. We are faced with requirements within which we must operate as we protect our respective organizations. These laws and regulations come into play as we help to design new systems and applications, play a part in deciding on retention periods for retention of data, recommending encryption or tokenization of sensitive data, and the plethora of other activities that are part of being a security professional.

These requirements may also govern our processes or ability to collect information, pursue investigations, monitor networks, and any of a number of activities that we might wish to execute as part of our appointed roles. Companies that operate internationally may particularly feel the complexity of these issues, as the laws regarding data, employee information, use of encryption, and similar commonplace activities may actually change from one part of the enterprise to the next based on where they are located or the national laws based on the origin of data we are storing.

6.2: Laws and Regulations

Information technology law (also called cyberlaw) concerns the law of information technology, including computing and the internet. It is related to legal informatics, and governs the digital dissemination of both (digitized) information and software, information security and electronic commerce aspects and it has been described as "paper laws" for a "paperless environment". It raises specific issues of intellectual property in computing and online, contract law, privacy, freedom of expression, and jurisdiction.

Information technology regulation, also referred to as cybersecurity regulation, is made up of any directive that safeguards information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyber attacks like viruses, worms, Trojan horses, phishing, denial of service (DOS) attacks, unauthorized access (stealing intellectual property or confidential information) and control system attacks.

Specifically. within the context of information security, the laws and regulations with which information security professionals might need to concern themselves with is massive. In the physical world the same issues, although still potentially complex, are much more straightforward and more easily enforceable.

For example, let's consider a real storefront is vandalized. The attacker walks up to the front of the store, spray paints some graffiti all over the store, throws the can of paint on the sidewalk, and runs off. Due to the cost of repairing the damage the police investigate the crime. The police, being able to get the culprits fingerprint from the spraypaint can, are able to track him down, and the discover he is a serial vandal. In the course of the investigation, it is also discovered that the perpetrator is on a foreign student visa. Given the record of offenses, his visa is revoked and he is deported from the country.

Now let's look at the same example from a slightly different angle. In this case, we have an online storefront. that is - a web page, which is defaced. Investigators which are part of the information security department with the victim company are able to trace back though their logs and discover that the attack that compromised their web server originated from a Chinese IP address (much like fingerprints). Unfortunately, the defacement came from a different IP address, one belonging to Microsoft's Azure hosting service. Additionally, traffic from Amazon's hosting service, Rackspace, and a number of others are all found in the logs as well, all originating from different countries. At this point, the company has patched the vulnerability that they think allowed the attacker in and repaired the web site. They have a number of potential leads that they could follow up on, but no authority to pursue them. At this point, the incident is reported to the FBI and generally will not be pursued as an active investigation because it doesn't cross over the loss threshold they follow due to the high volume of cases.

Such scenarios are all too common in the information security industry. Laws in the world today follow geographic boundaries, boundaries which the Internet ignores making enforcement complex at best and impossible in some cases because the countries involved have few if any laws governing Internet use.

A brief, non-exhaustive, list of laws and regulations is shown below.

Broadly applicable laws and regulations

Sarbanes-Oxley Act (SOX)
Payment Card Industry Data Security Standard (PCI DSS)
Payment Service Directive, revised (PSD2)
Gramm-Leach-Bliley Act (GLBA)
Customs-Trade Partnership Against Terrorism (C-TPAT)
Free and Secure Trade Program (FAST)
Children's Online Privacy Protection Act (COPPA)
Fair and Accurate Credit Transaction Act (FACTA), including Red Flags Rule
Federal Rules of Civil Procedure (FRCP)
Industry-specific guidelines and requirements
Federal Information Security Management Act (FISMA)
North American Electric Reliability Corp. (NERC) standards
Title 21 of the Code of Federal Regulations (21 CFR Part 11) Electronic Records
Health Insurance Portability and Accountability Act (HIPAA)

The Health Information Technology for Economic and Clinical Health Act (HITECH)
Patient Safety and Quality Improvement Act (PSQIA, Patient Safety Rule)
H.R. 2868: The Chemical Facility Anti-Terrorism Standards Regulation

US state laws

California Consumer Privacy Act (CCPA)
California Privacy Rights Act (CPRA)
Colorado Privacy Act
Connecticut Data Privacy Act (CTDPA)
Maine Act to Protect the Privacy of Online Consumer Information
Maryland Personal Information Protection Act – Security Breach Notification Requirements – Modifications (House Bill 1154)
Massachusetts 201 CMR 17 (aka Mass Data Protection Law)
Massachusetts Bill H.4806 — An Act relative to consumer protection from security breaches
Nevada Personal Information Data Privacy Encryption Law NRS 603A
New Jersey — An ACT concerning disclosure of breaches of security and amending P.L.2005, c.226 (S. 51)
New York State Department of Financial Services, Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500)
New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act
Oregon Consumer Information Protection Act (OCIPA) SB 684
Texas – An Act relating to the privacy of personal identifying information and the creation of the Texas Privacy Protection Advisory Council
Utah Consumer Privacy Act
Virginia -- Consumer Data Protection Act (CDPA)
Washington – An Act Relating to breach of security systems protecting personal information (SHB 1071)

International laws

Personal Information Protection and Electronic Documents Act (PIPED Act, or PIPEDA) — Canada
Personal Information Protection Law (PIPL) — China
Law on the Protection of Personal Data Held by Private Parties — Mexico
General Data Protection Regulation (GDPR)

Adapted from:
"IT law" by Multiple Contributors, Wikipedia is licensed under CC BY-SA 3.0

SECTION OVERVIEW

6.3: Compliance

What are the Different Types of Compliance?

6.3.1: Regulatory Compliance

6.3.2: Industry Compliance

Compliance awareness is essential for businesses to grow and as they are exposed to new audits and challenges. Almost all business activities have corresponding compliance regulations and standards that must be met. These regulations pertain to a wide swath of business activities: data privacy, security, environmental concerns, finance, and numerous other business practices.

There are three main types of compliance; corporate, regulatory and industry. All three types of compliance involve a framework of regulations, practices, and rules that must be followed.

What is Compliance in Business?

Corporate compliance refers to the protocols, rules, and codes of conduct that a business carries out. A corporate compliance framework helps a business to maintain high operating standards and avoid internal conflicts.

The definition of compliance is “the action of complying with a command,” or “the state of meeting rules or standards.” In the corporate world, it’s defined as the process of making sure a company and it's employees follow all laws, regulations, standards, and ethical practices that apply to that organization and the industry they do business in.

Corporate compliance covers both internal policies and procedures and federal and state laws. Enforcing compliance helps a company prevent and detect rules violations, protecting the organization from fines and lawsuits. The compliance process should be ongoing. Many organizations consistently and accurately govern their compliance policies over time.

Some of the steps that can be taken to enforce corporate compliance include:

- Keep track of workplace industry standards
- Schedule regular internal audits
- Conduct regular employee training

The Purpose of a Corporate Compliance Program

The purpose is to protect a business. But the return on investment could be significant, helping a company avoid waste, fraud, abuse, discrimination, and other practices that disrupt operations and put any company at risk.

Corporate compliance program needs to be integrated with all compliance efforts enterprise-wide, from managing external regulations and internal policies to comprehensive employee training. By ensuring all departments and staff are working together to maintain standards, a company can mitigate the risk of significant failures and violations.

6.3.1: Regulatory Compliance

Regulatory Compliance

Regulatory compliance refers to a set of practices and regulations an organization must adhere to. These rules are set by law and implemented by a regulatory agency.

Regulatory compliance may also include:

- Data and privacy compliance regulations (HIPAA, COPPA, GDPR, etc.)
- Quality management regulations such as ISO 9001
- Employment regulations such as FMLA and OSHA

Regulatory Requirements

A regulatory requirement is a rule or law, that has been enacted by a government entity, which creates a legal obligation for an organization and increases its compliance burden.

A regulatory requirement usually applies to all organizations doing business in a particular city/county/state/country, to organizations doing busines in a particular industry, or to organizations who engage in a particular type of activity.

The United States government has numerous regulatory agencies that are mandated to oversee the activities of private companies in their respective industries. A few examples of such organizations:

- **The Securities and Exchange Commission (SEC)** – The SEC oversees securities exchanges, securities brokers and dealers, investment advisors, and mutual funds in an effort to promote fair dealing, the disclosure of important market information, and to prevent fraud.
- **The Federal Trade Commission (FTC)** – The FTC investigates and prevents unfair methods of competition, and unfair or deceptive acts or practices affecting commerce.
- **The Food and Drug Administration (FDA)** – The FDA is responsible for protecting the public health by ensuring the safety, efficacy, and security of human and veterinary drugs, biological products, and medical devices; and by ensuring the safety of our nation's food supply, cosmetics, and products that emit radiation.
- **The Occupational Health & Safety Administration (OSHA)** – OSHA ensure safe and healthful working conditions for workers by setting and enforcing standards and by providing training, outreach, education and assistance.

Why is Regulatory Compliance Important?

When organizations fail to meet regulatory compliance requirements they may face substantial fines or penalties depending on the exact nature of the offense. Government regulations also provide guidance that helps businesses succeed, and failure to comply often coincides with various kinds of business failures.

Other consequences of poor regulatory compliance can include:

- Suspension or debarment from bidding on government contracts
- Damage to the organization’s reputation as a trustworthy business partner
- Individual penalties or jail time for individuals who intentionally violate the law
- Disruption to business operations caused by investigations or legal proceedings

What are Examples of Regulatory Compliance?

We can point to a variety of regulations that impact most corporations operating in the United States, such as:

- **The Dodd-Frank Act** – a broad range of reforms affecting nearly every aspect of the financial system with the goal of preventing a repeat of the 2008 crisis and the need for future government bailouts.
- **The Sarbanes-Oxley(SOX) Act** – to protect investors from the possibility of fraudulent accounting activities by corporations.

6.3.2: Industry Compliance

What is Industry Compliance

There are situations where companies will face compliance with regulations which are not mandated by law through a governmental entity. Nonetheless there are severe repercussions on a company's ability to conduct business when they do not follow the requirements of various regulators within various industries. An excellent example of this is compliance with the PCI DSS, often simply referred to as PCI compliance. In this situation a body composed of credit card issuers (Visa, American Express, and MasterCard, among others) has set up specific set of security standards as a condition of processing the credit card transactions for cards issued by the members companies.

While the PCI SSC has no legal authority to compel compliance, it is a requirement for any business that processes credit or debit card transactions. PCI certification is also considered the best way to safeguard sensitive data and information, thereby helping businesses build long lasting and trusting relationships with their customers.

Although this organization cannot legally enforce compliance with their standards, their decree does have teeth. Merchants processing credit card transactions based on cards from PCI members, based on the number of transactions processed, must submit to yearly assessments of their security practices. For very low numbers of transactions, this is a very simple self-assessment process consisting of a short questionnaire. As the number of transactions grows, the requirements become progressively more stiff, culminating in visits by specially certified external assessors, mandated penetration tests, requirements for internal and external vulnerability scanning, and a great deal more. PCI compliance is divided into four levels, based on the annual number of credit or debit card transactions a business processes. The classification level determines what an enterprise needs to do to remain compliant.

- **Level 1**: Applies to merchants processing more than six million real-world credit or debit card transactions annually. Conducted by an authorized PCI auditor, they must undergo an internal audit once a year. In addition, once a quarter they must submit to a PCI scan by an Approved Scanning Vendor (ASV).
- **Level 2**: Applies to merchants processing between one and six million real-world credit or debit card transactions annually. They’re required to complete an assessment once a year using a Self-Assessment Questionnaire (SAQ). Additionally, a quarterly PCI scan may be required.
- **Level 3**: Applies to merchants processing between 20,000 and one million e-commerce transactions annually. They must complete a yearly assessment using the relevant SAQ. A quarterly PCI scan may also be required.
- **Level 4**: Applies to merchants processing fewer than 20,000 e-commerce transactions annually, or those that process up to one million real-world transactions. A yearly assessment using the relevant SAQ must be completed and a quarterly PCI scan may be required.

For those found to not be in compliance, penalties range from hefty fines to removal of the ability to process credit card transactions. We might suppose that, for a business that depended heavily on credit card transactions, such as a retail store, losing the ability to process credit cards would be a business-ending proposition.

There are numerous other organizations, that have similar requirements for dealing with data security within their specific industry.

SECTION OVERVIEW

6.4: Privacy

Information Privacy

Information privacy, data privacy or **data protection laws** provide a legal framework on how to obtain, use and store data of natural persons. The various laws around the world describe the rights of natural persons to control who is using its data. This includes usually the right to get details on which data is stored, for what purpose and to request the deletion in case the purpose is not given anymore.

Over 80 countries and independent territories, including nearly every country in Europe and many in Latin America and the Caribbean, Asia, and Africa, have now adopted comprehensive data protection laws.[1] The European Union has the General Data Protection Regulation (GDPR),[2] in force since May 25, 2018.

This course will not go into issues of international privacy laws, as they are different in each country. There is a great deal of information available online, the links on this page would be an excellent starting point for those wishing to delve into the international aspect of information privacy.

6.4.1: Information Privacy in the U.S.

6.4.2: Information Privacy in the U.S. (continued)

Adapted from:
"Information privacy law" by Multiple Contributors, Wikipedia is licensed under CC BY-SA 3.0

6.4.1: Information Privacy in the U.S.

U.S. Privacy Laws

The United States is notable for not having adopted a comprehensive information privacy law, but rather having adopted limited sectoral laws in some areas like the California Consumer Privacy Act (CCPA).[3]

These laws are based on fair information practice guidelines developed by the U.S. Department for Health, Education and Welfare (HEW) (later renamed Department of Health & Human Services (HHS)), by a Special Advisory Committee on Automated Personal Data Systems, under the chairmanship of computer pioneer and privacy pioneer Willis H. Ware. The report submitted by the Chair to the HHS Secretary titled "Records, Computers and Rights of Citizens (07/01/1973)",[4][5] proposes universal principles for the privacy and protection of consumer and citizen data:

- For all data collected, there should be a stated purpose.
- Information collected from an individual cannot be disclosed to other organizations or individuals unless specifically authorized by law or by consent of the individual.
- Records kept on an individual should be accurate and up to date.
- There should be mechanisms for individuals to review data about them, to ensure accuracy. This may include periodic reporting.
- Data should be deleted when it is no longer needed for the stated purpose.
- Transmission of personal information to locations where "equivalent" personal data protection cannot be assured is prohibited.
- Some data is too sensitive to be collected, unless there are extreme circumstances (e.g., sexual orientation, religion).

Data privacy is not highly legislated or regulated in the U.S.[20] In the United States, access to private data contained in, for example, third-party credit reports may be sought when seeking employment or medical care, or making automobile, housing, or other purchases on credit terms. Although partial regulations exist, there is no all-encompassing law regulating the acquisition, storage, or use of personal data in the U.S. In general terms, in the U.S., whoever can be troubled to key in the data, is deemed to own the right to store and use it, even if the data was collected without permission, except to any extent regulated by laws and rules such as the federal Communications Act's provisions, and implementing rules from the Federal Communications Commission, regulating use of customer proprietary network information (CPNI). For instance, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Children's Online Privacy Protection Act of 1998 (COPPA), and the Fair and Accurate Credit Transactions Act of 2003 (FACTA), are all examples of U.S. federal laws with provisions which tend to promote information flow efficiencies.

The Supreme Court interpreted the Constitution to grant a right of privacy to individuals in *Griswold v. Connecticut*.[21] Very few states, however, recognize an individual's right to privacy, a notable exception being California. An inalienable right to privacy is enshrined in the California Constitution's article 1, section 1, and the California legislature has enacted several pieces of legislation aimed at protecting this right. The California Online Privacy Protection Act (OPPA) of 2003 requires operators of commercial web sites or online services that collect personal information on California residents through a web site to conspicuously post a privacy policy on the site and to comply with its policy.

The safe harbor arrangement was developed by the United States Department of Commerce in order to provide a means for U.S. companies to demonstrate compliance with European Commission directives and thus to simplify relations between them and European businesses.[22]

Recently, lawmakers in several states have proposed legislations to change the way online businesses handle user information. Among those generating significant attention are several Do Not Track legislations and the Right to Know Act (California Bill AB 1291). The California Right to Know Act, if passed, would require every business which keeps user information to provide its user a copy of stored information when requested.[23] The bill faced heavy oppositions from trade groups representing companies such as Google, Microsoft, and Facebook, and failed to pass.[24]

On June 28, 2018 California legislature passed AB 375, the California Consumer Privacy Act of 2018, effective January 1, 2020.[25] If the law is not amended before it becomes effective, The California Consumer Privacy Act, AB. 375 — gives California

residents an array of new rights, starting with the right to be informed about what kinds of personal data companies have collected and why it was collected.

Adapted from:
"Information privacy law" by Multiple Contributors, Wikipedia is licensed under CC BY-SA 3.0

6.4.2: Information Privacy in the U.S. (continued)

Some of the more notable privacy laws that have been enacted in the United States are briefly touched on below.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996. HIPAA is also known as the Kennedy-Kassebaum Health Insurance Portability and Accountability Act (HIPAA-Public Law 104-191), effective August 21, 1996. The basic idea of HIPAA is that an individual who is a subject of individually identifiable health information should have:

- Established procedures for the exercise of individual health information privacy rights.
- The use and disclosure of individual health information should be authorized or required.

One difficulty with HIPAA is that there must be a mechanism to authenticate the patient who demands access to his/her data. As a result, medical facilities have begun to ask for Social Security Numbers from patients, thus arguably decreasing privacy by simplifying the act of correlating health records with other records.[27] The issue of consent is problematic under HIPAA, because the medical providers simply make care contingent upon agreeing to the privacy standards in practice.

FCRA

The Fair Credit Reporting Act applies the principles of the Code of Fair Information Practice to credit reporting agencies. The FCRA allows individuals to opt out of unwanted credit offers:

- Equifax (888) 567-8688 Equifax Options, P.O. Box 740123 Atlanta GA 30374-0123.
- Experian (800) 353-0809 or (888) 5OPTOUT P.O. Box 919, Allen, TX 75013
- TransUnion (800) 680-7293 or (888) 5OPTOUT P.O Box 97328, Jackson, MS 39238.

Because of the Fair and Accurate Credit Transactions Act, each person can obtain a free annual credit report.[28]

The Fair Credit Reporting Act has been effective in preventing the proliferation of specious so-called private credit guides. Before 1970,[*when?*][29] private credit guides offered detailed, if unreliable, information on easily identifiable individuals.[30][31] Before the Fair Credit Reporting Act, salacious unsubstantiated material could be included – and in fact, gossip was widely included in credit reports.[32] EPIC has a FCRA page. The Consumer Data Industry Association, which represents the consumer reporting industry, also has a website with FCRA information.

The Fair Credit Reporting Act provides consumers the ability to view, correct, contest, and limit the uses of credit reports. The FCRA also protects the credit agency from the charge of negligent release in the case of misrepresentation by the requester. Credit agencies must ask the requester the purpose of a requested information release, but need to make no effort to verify the truth of the requester's assertions. In fact, the courts have ruled that, "The Act clearly does not provide a remedy for an illicit or abusive use of information about consumers" (Henry v Forbes, 1976). It is widely believed that in order to avoid the FCRA, ChoicePoint was created by Equifax at which time the parent company copied all its records to its newly created subsidiary. ChoicePoint is not a credit reporting agency, and thus FCRA does not apply.[33]

The Fair Debt Collection Practices Act similarly limits dissemination of information about a consumer's financial transactions. It prevents creditors or their agents from disclosing the fact that an individual is in debt to a third party, although it allows creditors and their agents to attempt to obtain information about a debtor's location. It limits the actions of those seeking payment of a debt. For example, debt collection agencies are prohibited from harassment or contacting individuals at work. The Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (which actually gutted consumer protections, for example in case of bankruptcy resulting from medical cost) limited some of these controls on debtors.

ECPA

The Electronic Communications Privacy Act (ECPA) establishes criminal sanctions for interception of electronic communication. However, the legislation has been criticized for lack of impact due to loopholes.[34]

CHAPTER OVERVIEW

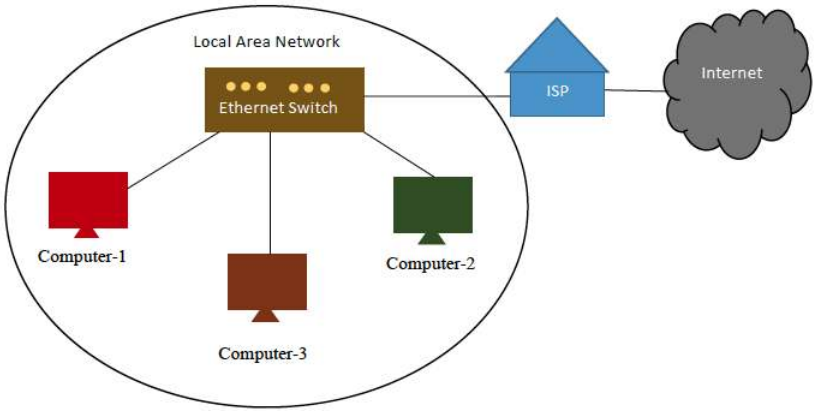
7: Network Fundamentals

7.1: Introduction

Network security and Information security used to be used interchangeably because it is the network that is at the core of most computer information. Recently information security has evolved beyond the network; however, it is still essentially the computer networks that enable information sharing especially in organizations. Therefore, a comprehensive understanding of computer networks will allow both novice and experienced personnel to have the tools necessary in the defense and protection of valuable assets.

Networking Basics

In its simplest form, a network is two or more computers that are connected together through either a wired or wireless medium so that they can more effectively share and exchange information in various forms. Computers can also share information without a network through media such as CD/DVDs, USB drives, external hard drives and such but this process is inefficient especially as the distance between the computers become greater.



In exchange for the benefits of the network some knowledge and set up must take place including use of hardware, software, configurations and troubleshooting. The purpose of using networks is about sharing three main entities: files, resources and application programs.

- File Sharing
  Networks allow one computer to share files with other computers and devices such as smartphones, tablets, smart TVs and others on the network regardless of their geographic location. This has essentially fueled the recent mobile evolution due to the ease of being to connect to the largest network in the world known as the Internet.
- Resource Sharing
  Computer resources such as printers and hard drives and others can also be access through the network. For example, a single printer attached to one computer can then be shared by all other computers so they can easily print from their individual location and not require multiple printer purchases. The same can be done with external hard drives used for backup and other purposes especially for companies that can to store their data in a single location instead of having their data scattered throughout the organization. As you may see leads to use of more powerful computer systems called a File Servers.
- Application Program
  Sharing Instead of having multiple copies of application programs on individual computer systems which would then require individual licenses and maintenance of them a single volume license could be purchased and maintained on one Application Server. This cuts down on maintenance time and costs in addition to revision updates. Antivirus and Anti malware programs one such example used in the industry today especially in environments with hundreds of individual computers. With the popularity of social media and constant connections the use of email and instant messaging programs allow for real-time communications. Without networks social networking companies such as Facebook and Twitter cannot really be as big and as popular as it is today. Online meetings, synchronous online classes and video conferencing are more real applications using networks. All one needs to connect to the network is a computer device that has a network interface card either wired or wireless that follows the rules of network functionality leading us into the next topic of the OSI and TCP/IP Models.

7.2: OSI and TCP/IP Models

Open Systems Interconnect Model

The Open System Interconnection (OSI) reference model was proposed by the International Organization for Standardization (ISO), a nonprofit organization that develops and publishes standards including information technology. It is headquartered in Geneva, Switzerland and comprised of 162-member countries. The OSI model for networking explains how networks function in an orderly and structured, seven-layered approach. The OSI model is a theoretical concept that is used for teaching and learning in the field of computer networking; and, serves as a general conceptual framework on how networked systems should operate to be able to work together.

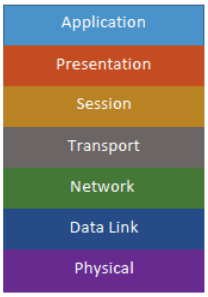


Figure **7.2.1**: OSI Model. ("Information Security" by Umar Khokhar Binh Tran is licensed under CC BY 4.0)

Let us look at this example of why the reference model is needed and how the layered approach is so valuable using this non-networking example: Mary who lives in Atlanta, Georgia would like to send some information to Bob who lives in Los Angeles, California via the United States Postal Service or snail mail like many IT folks like to call it. Here is the breakdown of what has to happen:

1. Mary, who lives in Atlanta has some information she would like to send to Bob, who lives in Los Angeles. She writes a letter and puts the information with the letter to get to Bob and decides to use the postal service.
2. Mary folds the letter with the information and puts it in an envelope which is the standard “protocol” for sending letters in the United States ready to be sent but now has to address the envelope.
3. Mary addresses the envelope with Bob’s name, street address, city and state information in the middle and put her return address on the top left which is the standard “protocol” for sending letters.
4. Mary must then purchase and put a stamp on the top right of the envelope per the stamp location standard “protocol”.
5. Mary then goes to the post office to drop it off or she can enable the flag at her home mailbox both of which are standard “protocols”.
6. The mail carrier obtains the envelope and brings it to the main sorting center in Atlanta and then it is sorted for the destination zip code which is in Los Angeles. The envelope is then placed on a plane to travel to Los Angeles main sorting center.
7. Upon arrival the letter then needs to be sorted according to Bob’s zip code and location for local delivery by the mail carrier.
8. The mail carrier then uses the street address to be sure to deliver it to Bob’s mailbox.
   Bob then receives the envelope, open it up, discard the envelope and retrieves the letter and information that Mary wanted to send to him.

As you can see there are a number of structured, orderly tasks that has to happen at each “layer” and one must be completed before the next layer take over. This layered approach may seem complex and in reality it is but it allows for each task to be handled separately thus allowing for more simplified troubleshooting. This “divide and conquer” strategy allows for solving big problems by breaking them down into smaller components and a change to one of the steps would not affect the entire process very much if at all.

Adapted from:
"Information Security" by Umar Khokhar Binh Tran, OpenALG is licensed under CC BY 4.0

7.2.1: OSI Model

Back to our networking concepts for example if we decided to use new fiber optic cables instead of older coaxial cables the delivery step the other steps in the entire process are not impacted. The OSI model divides network communications into seven layers as shown in the figure in order from the top:

7 – Application
6 – Presentation
5 – Session
4 – Transport
3 – Network
2 – Data Link
1 – Physical

We will briefly discuss each layer to give you a high-level understanding of what happens at each layer without getting into too much detail.

- Application Layer
  The Application layer (Layer 7) provides an interface for applications to access network services such as file sharing, message handling, database access and more. Protocols such as HTTP, HTTPS, FTP, DHCP, DNS, SMTP and many more operate here. Please keep in mind that the Application layer is not the application itself such as Microsoft Word or Adobe Photoshop but its connection to the network services. However, some user applications such as web browsers and email clients have integrated network functions with the application layer.
- Presentation Layer
  The Presentation layer (Layer 6) handles data formatting and translation. The Data from the Application layer is “presented” by protocol conversion, data encryption and decryption, data compression and decompression and data representation. For example, a web browser that connects to a secure Web server may need to encrypt and decrypt the data before it is transferred to the Web server.
- Session Layer
  The Session layer (Layer 5) sets up and holds ongoing communications called a “session” across the network so that applications on both sides can exchange data for as long as the session lasts. Synchronization and check pointing occur here as well as in the example of an audio or video stream used by a web-conferencing application.
- Transport Layer
  The Transport layer (Layer 4) manages the data transfer from one application across the network. One of the processes that happen here is the segmenting of the data streams in to small units called “segments” for travel over the network. The two primary protocols that operate at this layer is TCP and UDP. TCP is the connection-based, higher overhead protocol that uses hand-shaking thus is more reliable. UDP is the connection-less, less overhead and less reliable protocol.
- Network Layer
  The Network layer (Layer 3) handles logical network addressing such as translating Internet Protocol (IP) addresses into physical addresses (Media Access Control, MAC) addresses. It is responsible for performing the best route calculations to reach a certain destination and is the workhorse of the all networking. IP, ICMP, ARP, IPSec among other known protocols operate here. The data unit at this layer is called a “packet”.
- Data Link Layer
  The Data Link layer (Layer 2) works with “frames” as its data unit and it acts as a conduit between the Network layer and the Physical layer. Media Access Control (MAC) addresses can be found here as well as communication methods such as CSMA/CD and token passing. Network cards also operate here since they are programmed with MAC addresses as well as include the physical interface to the network.
- Physical Layer
  The Physical layer (Layer 1) is where the conversion of data into bit signals of 0 or 1 to be transferred over the medium. The type of signals can be pulses of light as in the case of fiber optic cabling, electrical pulses in the case of twisted-pair cable or radio waves in the case of wireless communications.

In summary the OSI model is an organized and helpful way to separate networking activities and associate them with protocols and functionality. It helps explain how data is formatted as it moves through the layers and aids in understanding the hardware, software and protocols at each step of the overall communication process.

7.2.2: Transmission Control Protocol/ Internet Protocol Model

The OSI model presents a great high-level overview of network communications but as mentioned earlier it is very theoretical and in many cases networking in the industry does not follow the OSI model.

However, the Transmission Control Protocol, Internet Protocol (TCP/IP) model or more commonly referred to as the TCP/IP Protocol Suite is used. Many experts describe the OSI model and theoretical whereas the TCP/IP model as practical.

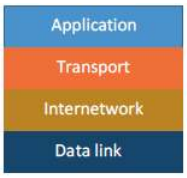


Figure **7.2.2.1**: TCP/IP Architecture. ("Information Security" by Umar Khokhar Binh Tran, OpenALG is licensed under CC BY 4.0)

A “protocol” is not specific to networking but refers to a set of rules and procedures for communication or behavior. For example, an employee must follow a set of protocols to be employed at an organization. Two people communicating must agree on a certain language or “protocol” to successfully communicate. In the past there were several protocols that were used in networking such as Windows specific NetBEUI, or Novell NetWare’s IPX/SPX but both are now obsolete. The TCP/IP protocol suite is the protocol of the Internet and the one that all current operating systems and systems run.

The TCP/IP protocol suite uses a similar layered approach like the OSI model but it is condensed into four layers instead of seven namely Application, Transport, Internetwork and Network access.

- Application-Layer Protocols
  The Application layer provides network services to user applications as well as provide authentication and data-formatting, data encryption and translation. Common protocols which we will discuss in further detail later include HTTP/HTTPS: Protocols of the World Wide Web and Email Protocols: POP3, IMAP and SMTP. DHCP and DNS are also very important Application layer protocols to overall network and Internet operation.
- Transport-Layer Protocols
  The Transport layer protocols include TCP and UDP just like in the OSI Transport layer and its role is to provide reliability to flow control to transfer large amounts of data. Segmenting, sequencing, flow control, acknowledgement and hand-shaking occur here.
- Internetwork-Layer Protocols
  The Internetwork layer protocols is where network configuration and the Internet Protocol (IP) operate. The layer defines and verifies IP addresses, routes packets through the networks, resolves MAC addresses to IP addresses, delivers packets effectively and efficiently. IPv4, IPv6, ICMP, ARP and IPSec are the more common protocols that operate at this layer.
- Network Access-Layer Protocols
  The Network Access layer technically does not include any protocols but rather technologies such as Ethernet. The layer is responsible for MAC address confirmation, defining of media access rules, de- encapsulation of frame, checking for errors and converting the signals to bits whether it is electrical, light pulses or radio waves.

As you can already see the TCP/IP suite more accurately aligns its protocols and functionality with real network services thus it is the more practical model used today.

7.3: Network Protocols

We already introduced the network security hardware devices so this section will continue address the network software or protocols with respect to security concepts. A network protocol is a set of standardized rules for proper communication between network devices and as mentioned earlier the most common protocol used today is the Transmission Control Protocol/Internet Protocol (TCP/IP).

TCP/IP is not a single protocol but consists of many protocols but the two most important protocols that make up its name are: TCP and IP. TCP is one of the main Transport Layer protocols in Layer 4 of the OSI model; whereas IP is one of the primary protocols that operate at the Network Layer, Layer 3 of the OSI model. There protocols work together because IP is responsible for network addressing and getting the packet on the right path or route to the destination; while TCP is responsible for transmissions control and reliable delivery of the packet.

- Transmission Control Protocol (TCP)
  If an application requires reliable data transfer, it uses TCP as the Transport-layer protocol. TCP provides reliability with the following features:
  - Establishing a connection
  - Segmenting large chunks of data
  - Ensuring flow control with acknowledgements

  Each feature is dependent on the fact that TCP is a connection-based protocol. TCP establishes a connection with the destination, the data is transferred, and the connection is released. A real-world example would be a cellphone call where a user dials a number, a connection is established with a slight delay and if the recipient answers a connection is established and held during the entity of the conversation.

  We will not get into the technical details of the TCP header in this chapter but TCP establishes the connection via the TCP Handshaking mechanism which is a three-step process. Each session is assigned a port number to keep track of the numerous numbers of network connections for the applications. Running the network command “netstat” will display the port numbers used and whether or not they are using TCP or UDP as well as private and public IP addresses.

- User Datagram Protocol (UDP)
  The other Transport Layer (Layer 4) protocol is UDP. UDP is an alternative protocol that is primarily used for establishing low-latency or loss-tolerating connections between applications on the Internet. UDP enables process-to-process communication by sending “datagrams” and used a “best-effort” delivery method. UDP does not need to establish a connection and thus does not provide flow and error control; therefore, is often referred to as connection-less whereas, TCP is connected-based.

  UDP also used port numbers to help distinguish different user requests and optionally offers a checksum to verify that data does arrive intact. A big difference between UDP and TCP is that packets may take different paths between the sender and receiver so some packets may be lost or may be received out of order.

  UDP is an ideal protocol for network applications in which perceived latency is critical such as in gaming, voice and video communications which can suffers some data loss without affecting overall quality.

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.253.1.238:49273     gb-printfac-01:49696   ESTABLISHED
  TCP    10.253.1.238:49642     52.242.210.82:https    ESTABLISHED
  TCP    10.253.1.238:53019     108.177.122.188:5228   ESTABLISHED
  TCP    10.253.1.238:54316     40.97.190.18:https     ESTABLISHED
  TCP    10.253.1.238:54317     40.97.190.18:https     ESTABLISHED
  TCP    10.253.1.238:54377     40.97.190.18:https     ESTABLISHED
  TCP    10.253.1.238:54427     bam-8:https            ESTABLISHED
  TCP    10.253.1.238:54500     va:https               ESTABLISHED
  TCP    10.253.1.238:54504     199.107.67.103:https   ESTABLISHED
  TCP    10.253.1.238:54603     52.96.28.2:https       ESTABLISHED
  TCP    10.253.1.238:54628     ec2-52-55-153-127:https  ESTABLISHED
  TCP    10.253.1.238:54729     40.97.127.130:https    ESTABLISHED
  TCP    10.253.1.238:55032     www:https              CLOSE_WAIT
  TCP    10.253.1.238:55033     40.97.230.2:https      TIME_WAIT
  TCP    10.253.1.238:55099     40.97.228.178:https    TIME_WAIT
  TCP    10.253.1.238:55101     40.97.228.178:https    TIME_WAIT
```

Figure **7.3.1**: TCP Traffic ("Information Security" by Umar Khokhar Binh Tran, OpenALG is licensed under CC BY 4.0)

- Domain Name System (DNS)
  The Domain Name System (DNS) is a TCP/IP protocol that resolves or maps a Fully Qualified Domain Name such as www.google.com with one of its corresponding IP addresses such as 64.233.177.103. The DNS database is organized in a tree-like hierarchy as shown in figure 2.6:

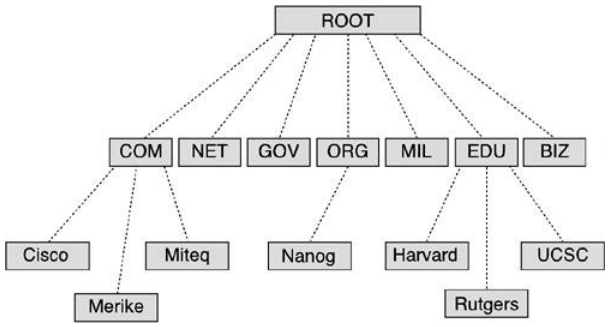


Figure **7.3.1**: Copy and Paste Caption here. (Copyright; author via source)

The top-level domains (TLDs) are organized into categories such as commercial (.com), nonprofit organizations (.org), government (.gov), education (.edu) or country of origin represented by a two-letter code such as Canada (.ca). The second-level domains are usually the names the companies or institutions. The host level represents individual computers or servers such as www which hosts all the web files or mail which maintains all the mailboxes.

Local DNS servers can be configured to the local organization websites for example www.company.com but they are also configured to know where the “root” servers are around the world in case they need to resolve addresses that are not in their local database. To help speed up this process some servers and clients make use of the DNS cache which stores the domain names and IP address pairs resolved recently in their local memory.

Because of its importance DNS is often the focus of security attacks. DNS poisoning results in substitute addresses so that the computer is redirected to another device and this can be done by the attacker at either the local host table, or the external DNS server. A variation of DNS poisoning involves replacing a MX (mail exchange) record resulting in all email being sent to the attacker instead of the proper MX server.

Finally, a DNS transfer attack tricks the server into giving information that the attacker could then use to map out the entire internal network of an organization that is linked to the DNS server. This can then be used in many ways to determine weaknesses in the network for other types of attacks.

- Internet Protocol (IP)
  The Internet Protocol (IP) is the heart of the TCP/IP protocol suite. IP addresses are defined at the Network Layer (Layer 3) of

the OSI model and the Internetwork Layer of the TCP/IP. This is where network routing takes place and without routing the Internet and World Wide Web as a whole would not exist. The Internetwork layer is responsible for several main functions:

An IP address is assigned to every computer and network device that uses TCP/IP protocols for communications. The purpose of the IP address is to identify the device at the Internetwork or Network layer and also to identify which network it resides on because there would be many networks or subnetworks in an organization. IP addresses work similar to the 10-digit phone number used in the U.S. where the first three represent the area code and the last seven represent the individual number. Each IP address can be broken down into the Network ID and the Host ID.

The next task is to determine the best path to get the packets from the sender to the receiver navigating all the networks in between them. Similar to the Interstates in the U.S. many large networks have many paths that can be taken to get from one location to another. This “routing” task is shared with all the routers in the world network which must communicate with each other to determine the best path at any particular time.

The network packet that sent or received includes both the physical (MAC) and logical (IP) source and destination addresses so when it gets to the final destination it will know which unique device defined by MAC address needs to get the end information. This task is assisted by another protocol called Address Resolution Protocol (ARP) which maintains a table of MAC addresses and their respective IP addresses.

- Defines and verifies IP addresses
- Routes packets through an internetwork
- Resolves MAC addresses to IP addresses
- Delivers packets efficiently

- Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is used to resolve a logical IP address to a physical MAC address. The IP protocol’s purpose to get the packet to the correct network and once in that particular network it can query the ARP cache or table to find the physical address to populate into the Data Link (Layer 2) frame for proper delivery.

```
Interface: 10.253.1.238 --- 0xe
  Internet Address      Physical Address      Type
  10.253.0.1            00-04-96-83-6d-91     dynamic
  10.253.7.199          04-e5-36-19-b5-5a     dynamic
  10.253.15.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.83.100.109        01-00-5e-53-64-6d     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure **7.3.1**: ARP Cache of the local computer ("Information Security" by Umar Khokhar Binh Tran, OpenALG is licensed under CC BY 4.0)

The process can be very complex and we will not go into its details in this chapter but one of the potential targets for attack is the ARP cache. In an attack called ARP poisoning or spoofing the attacker sends falsified ARP messages over the local area network, and by doing so the results allow the attacker to link their MAC address with the IP address of a victim server or computer on the network.

7.3: Networking Security Concepts

There are many aspects to network security and this chapter will directly address many of these concepts. However, the rest of the book may address security aspects that may be outside the realm of network security. At its core network security can be divided into two main areas of study and that being network hardware and network software or protocols. Network hardware includes the physical devices and their inherent software that allows them to function on the network. Network software or protocols include the standard methods of communication that the network hardware uses to transfer and share data across networks.

Network Security Hardware

The most fundamental level of security can and should be done through the use of security features that are found with certain network hardware devices. Since many devices operate at different levels of the OSI or TCP/IP models a layered security approach allows for greater defense and protection. In turn this would entail an attacker to compromise multiple network devices significantly decreasing their chances for success before the attack is discovered. We will continue with an overview of some of the more popular devices
and their capabilities.

Advanced switches also support Virtual Local Area Network (VLANs) which offer additional network with physical port security. With the proper type of switch and configuration these devices offer the first line of defense with respect to security leading up to the next network device

- Switches
  As of the last few years switches have replaced the obsolete hub device as the standard network device for connecting computers, printers, Voice over IP (VoIP) and other end devices. Hubs operated at Layer 1 – Physical Layer of the OSI model which meant that it just repeated all frames to all attached network devices. This not only increases unnecessary traffic but from a security standpoint allows for attackers to install software such as a protocol analyzer and capture packets that are sent through the network.

  Switches as do hubs also connect multiple devices but once the network becomes stable meaning computers and end devices are plugged into certain switch ports the switch learns through a switching table or mac address table where each device is connected. Switches operate at Layer 2 – Data Link Layer of the OSI so used Media Access Control (MAC) addresses to only forward frames to the end device through the specific port that device is connected to. Network monitoring is still necessary but this helps minimize data floating around the network that can be vulnerable to attackers.

- Routers
  Routers operate at Layer 3 – Network Layer of the OSI model and its purpose is to “route” packets across different computer networks. Routers view destination information in the packets it receives then consults with the routing table to send the packet to the next network towards the final destination. In doing so, routers have a built-in security function to filter specific types of network traffic going to specific networks.

  Routers are very complex devices with many configuration features and in many small type networks is the main security appliance for the entire organization. Routers come in various sizes and robustness depending on how much bandwidth and traffic they are designed to handle as well as the ability to configure Access Control Lists (ACLs) to determine rules for packet propagation through the network. Misconfiguration of ACLs could block certain network traffic and, in some cases, can cause the entire network to come to a screeching halt.

  Routers typically have their own operating system with a powerful central processing unit, random access memory as well as storage capabilities. Traditionally routers were wired devices but with the recent rapid mobile evolution wireless routers are now the dominant device used for households and small businesses. Router administrator passwords and security patches must be properly configured and maintained for them to be effective and protected again attackers.

- Firewalls
  Network Firewalls are devices designed to protect an entire network by inspecting packets and either allow or deny their entry. Hardware firewalls are usually located outside the internal network and is the first line of defense from the outside. The packets

are filtered by the firewall in one of two ways. The first is the “stateless packet filtering” method which looks at incoming packets and permits or denies it based on conditions that have been pre-defined by the network or security administrator. “Stateful packet filtering” is the second method which keeps a record of the connection between an internal computer and an external device and decides based on the connection as well as certain specific conditions.

The firewall has four different options it can “allow” the packet by letting it pass and continue on the network or it can “drop” the packet to prevent and not send any response to the sender. The firewall can “reject” the packet which prevents and also informs the sender and finally it can “ask” for user intervention the next course of action. There are also traditional rule-based firewalls as well more modern application-based firewalls also known as “next-generation firewalls” (NGFW)since they have more “intelligent” capabilities.

- Intrusion Detection Systems
  An intrusion detection system (IDS) is a device that can detect an attack as it occurs. IDS systems can use various different methods for monitoring and detection of attacks but it essentially involves real-time monitoring and examination of network traffic, activity, behaviors and transactions in order to detect any security related anomalies. The IDS device can be installed either on a local host or on the network and they use one of the four following methods:
  - Anomaly-based monitoring is designed for detecting statistical anomalies. Normally a baseline is established over a certain amount of time so whenever there is a significant deviation from this baseline an alarm or flag course be raised. This method is very fast but can lead to false positives if there are real non-security related spikes in the network activity. Additionally, anomaly-based monitoring requires high processing on the system so adequate hardware resources needs to be dedicated.
  - Signature-based monitoring looks at the network traffic and activities for well- known patterns such as antivirus scanning. One of the weaknesses of signature-based monitoring is that the signatures needs to be constantly updated leading to heavy network usage. If the signatures are too specific they may miss certain intrusions; whereas, if they are too general they will cause many false positives.
  - Behavior-based monitoring is a compromise of anomaly-based and signature-based monitoring by being adaptive and proactive instead of reactive. It analyzes the behavior of processes and programs on a system and alerts the user of any abnormal activity. One of the advantages is that is can help detect new attacks rather quickly even if there no new signature or definition exists.
  - Heuristic monitoring is the last method which uses a totally different approach. Instead of comparing actions as is done with anomaly-based and signature based or comparing behaviors as is done by behavior-based it use experience-based techniques. The question it attempts to answer is “if this action can be harmful to the system.” It them monitors for events such as port scanning and protocol captures which are potentially dangerous and alerts them accordingly.
- Intrusion Prevention Systems
  An Instruction Prevention System (IDS) as it implies not only monitors and alerts for malicious activities as does the IDS but it also can attempt to stop the attack. IDS systems are usually connected directly to certain network hardware devices or hosts where they can more quickly respond by blocking ports or packets deemed as dangerous in addition to reporting it back to the central monitoring system. Most IPS systems employ certain levels of intelligence so that they can provide a higher degree of accuracy regarding and speed in response to potential attacks.
- Unified Threat Management Security Appliance (UTM)
  Since there are many different types of network security hardware devices such as firewalls, Internet content filters, web security gateways, IDS and IPS devices managing them all can be very complex. A Unified Threat Management (UTM) security device combines several security functions and can offer an array of security functions including:
  - Antivirus and Antispyware
  - Antispam and Anti-Phishing
  - Bandwidth optimization
  - Content filtering
  - Encryption
  - Firewall
  - Intrusion Detection and Prevention
  - Web filtering

The Unified Threat Management device has also been referred to as the All-in-One Network Security Appliance.

CHAPTER OVERVIEW

8: Web Application and Wireless Network Attacks

8.1: Web Application Attacks

A web application is a type of application software which runs on a webserver and can be accessed through the internet e.g. Gmail, Google search engine, Apple /Google Maps and Microsoft 365 etc. In 1991, when the concept of web was introduced, web pages were static (Only readable and non-interactive) and the users can only read the contents of the websites. HTML (Hyper Text Markup Language) is mainly used to design such static webpages. In 2000, Web 2.0 was developed and dynamic web pages were introduced, which allows the users to interact with the web pages and based on user's input, can adjust the web content. To design a dynamic web page, besides HTML, we need to use many different technologies e.g. PhP, Javascript, VB Script, Database connector strings and python etc. The biggest advantage of using these scripting languages in designing of web pages is that one can design any security feature using the power of scripting languages. Sometimes when a user enters the data on a website, it directly stores that data in databases therefore the database connecting methods (Open Database Connectivity, Object linking & Embedding) are used to connect the web application to the database. Web application security is considered to be more difficult than protecting the networks. The typical network security devices such as Firewalls, Intrusion Detection Systems and Intrusion Prevention Systems which inspects the TCP/IP packets (filter them based on the defined rules) completely ignore the HTTP traffic. The attackers take advantage of this vulnerability and inject malicious tags or traffic and send it to application servers to deface a website, steal the contents of the database and gain unauthorized access to applications etc. Moreover, Zero Day Attacks (an attack that exploits the previously unknown vulnerability) are also the biggest threats to web applications which are growing significantly.

8.1.1: Web Applications Vulnerabilities

Thousands of web application vulnerabilities have been reported so far and cyber security analysts are continuously working to protect web applications from security attacks. The Open Web Application Security Project (OWASP) helps security professionals find and combat against web application vulnerabilities and attacks. They designed the web security vulnerabilities assessment tool (ZAP), guidelines for testing the webserver against vulnerabilities and also classifies web application attacks. Some of the critical and common web application vulnerabilities are: Injection vulnerabilities, Authentication weaknesses, Cross Site Scripting, Sensitive Data Exposure, Unvalidated redirects and directory traversal attacks. A detailed description of some of these vulnerabilities are discussed on the following pages.

8.1.1.1: Injection Vulnerabilities

Injection vulnerabilities occur when a web application accepts an untrusted and malicious data as input from the user without validating it. The Structured Query Language (SQL) injection attack is one of the most common type of attack which exploits the injection vulnerabilities and targets the SQL databases by injecting the malicious commands. The process of SQL injection attack is presented as follows:

1. The attacker clicks the forgot password option (to verify whether the webserver is vulnerable to SQL injection attack or not) and enters incorrect format of username or email address (e.g. instead of xyz@ggc.edu the attacker enters xyz?#= = 1). If the reply comes “Incorrect username format” then it means there is a filter (format checker) in place which validate the user input before getting it through the database. However, if reply comes “Error/User Not found”, this indicates the absence of the filter, which means the attacker can inject the malicious commands to webserver and manipulate the database.
2. The attacker then enters the SQL commands in the username field and performs the destructive actions e.g. steal and manipulate the data stored in the database.

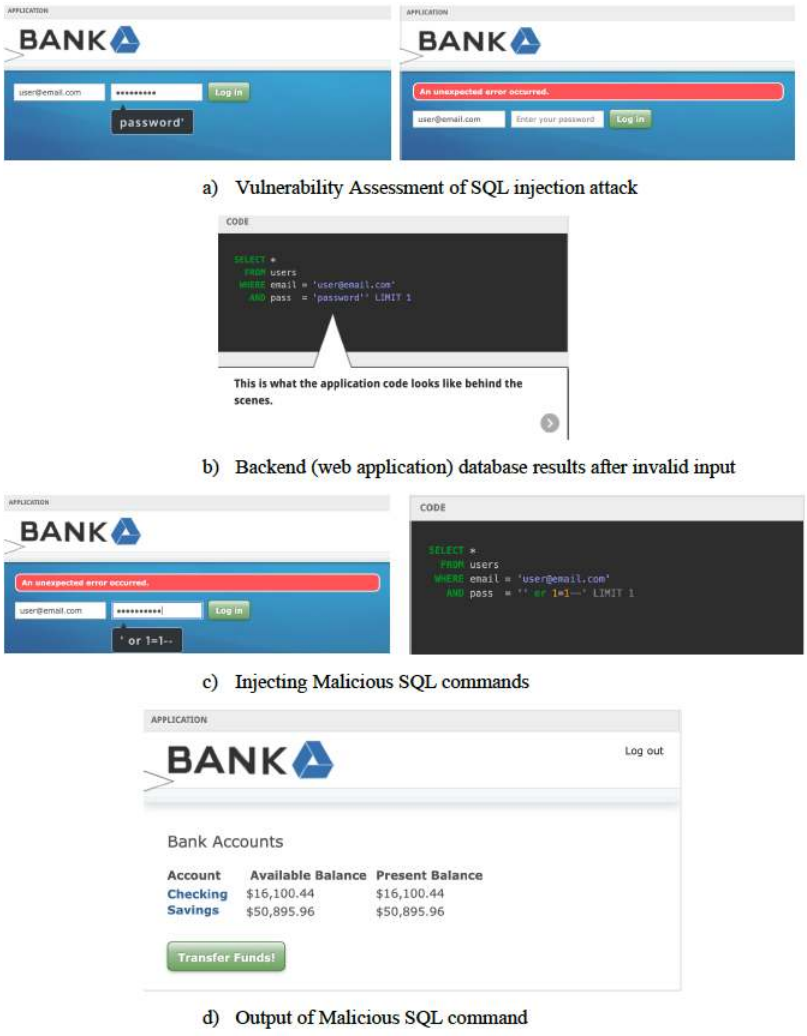
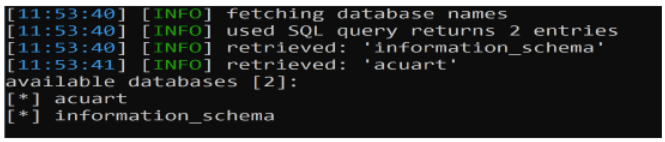


Figure **8.1.1.1.1**: Phases of SQL injection attack on a vulnerable web Application("Information Security" by Umar Khokhar Binh Tran is licensed under CC BY 4.0)

Sqlmap is the one of the most widely used tools for SQL injection attacks which automates the process of vulnerability assessment and injection of the SQL commands. The attacker just has to enter few commands and follow a simple four (4) steps process:

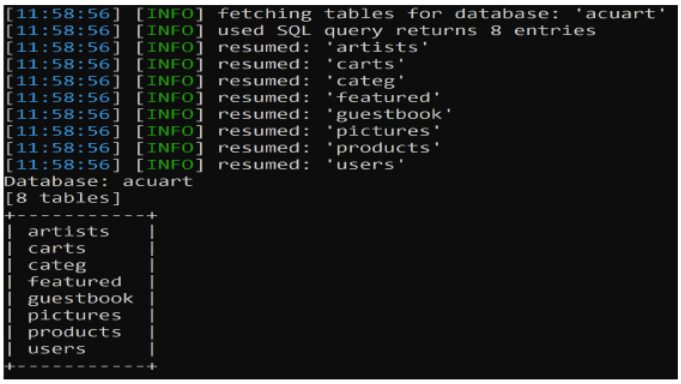
1. Identification of the databases
2. Choose a specific database and identify tables of that databases
3. Choose a specific table and identify the columns
4. Dump the columns

a) Identification of Databases



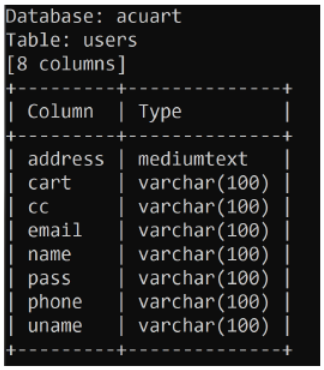
b) Available Databases on target webserver

c) Identification of Tables on the specified database

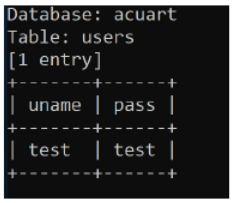


d) Available tables on specified database

e) Identification of Columns on the specified table



f) Columns on the table



g) Dump the tables

Figure 8.1.1.1.2:

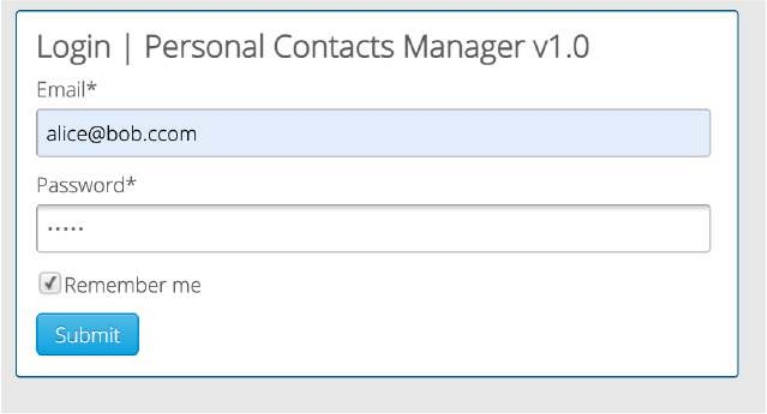
SQL injection attack using Sqlmap

8.1.1.2: Weak Authentication

Typically, most of the webservers use only knowledge authentication factor (Username & Password) to perform authentication of the users. As discussed in Chapter 4, the passwords are the weakest (yet the most popular) authentication parameter, if the password gets compromised then the attackers can get the unauthorized access to the user's confidential resources. Moreover, weak encryption schemes and weak session management makes authentication problems even worse and eventually open the roads for MIMAs. Figure 8.3 presents the interception of the data of a website using the insecure protocol (http).

8.1.1.3: Cross Site Scripting (XSS)

XSS attacks are just like injection attacks where the server accepts the untrusted input from the user/attacker and then lets the attacker manipulate the webserver operations.



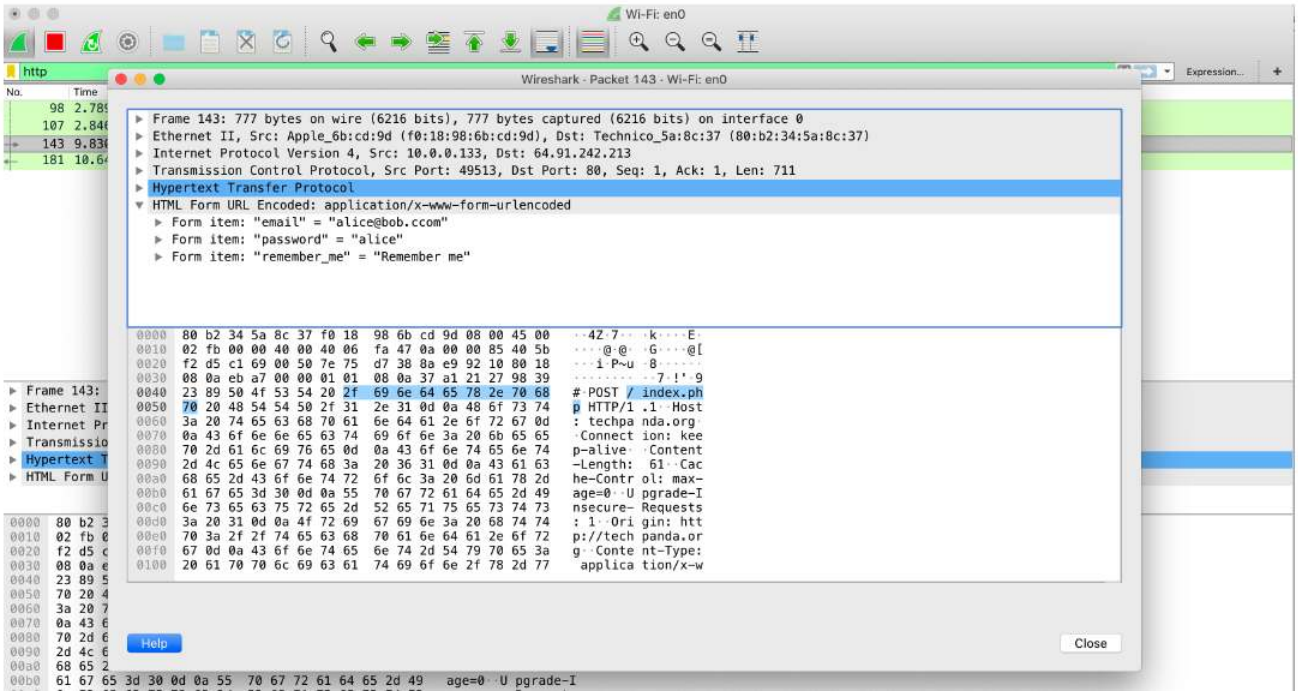


Figure **8.1.1.3.1**:

Interception using Wireshark

(<u>"Information Security"</u> by Umar Khokhar Binh Tran is licensed under CC BY 4.0)

There are two types of the XSS attacks: XSS Reflection and XSS Stored/Persistent:

- XSS Reflection: Firstly, the attacker finds a vulnerable website (which does not validate the user's input; typically blogging sites) then post a comment on a vulnerable website with underlying malicious script. When any user clicks the comment to respond then it can result in many malicious outcomes e.g.

- Steals the user browser's history or cookies
- Redirects the users to a crafted/fraudulent website
- Install a malicious software or Add-ons

- XSS Stored/Persistent: The XSS stored is more dangerous as compared to XSS reflection. In a XSS stored attack, the attacker injects the malicious scripts that are stored on vulnerable servers. Then, whoever visits that containment webserver, becomes the victim of the attack e.g. The attacker can store a cookies stealing script on the webserver and then anyone who visits the website, the malicious script forwards a copy of the session cookie to attacker. Figure 8.1 shows the session key stealing script.

8.1.1.4: Sensitive Data Exposure

Another common vulnerability of many of the web applications is sensitive data exposure which occurs because of information being cached on a local computer. For example, a client uses a public computer (Library or Internet café) to access his or her school's email or bank account then some of the sensitive information related to the user's account gets cached on the local memory. When the legitimate user logs off the system, an the attacker logs into the system and can access the user's account with the cached account information.

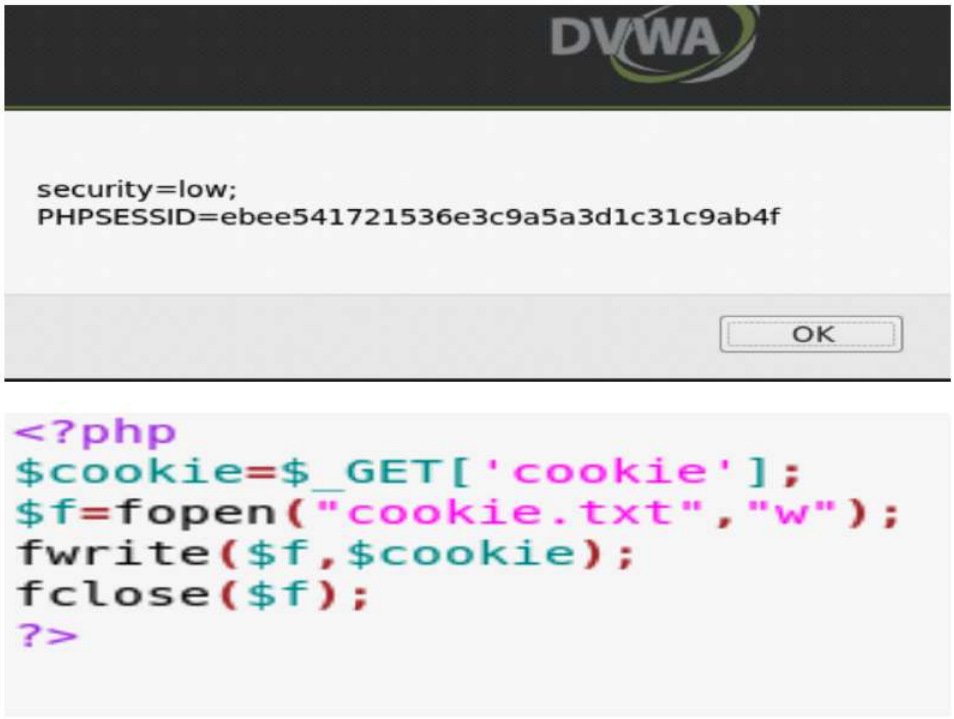


Figure **8.1.1.4.1**:

XSS attack session key stealing cookie

("Information Security" by Umar Khokhar Binh Tran is licensed under CC BY 4.0)

8.1.1.5: Unvalidated URLs/redirects:

Many blogging and social media websites, allow the users to post (embed) the URLs without any proper validation (whether the URLs are listed in the blacklists or not). This vulnerability leads to many social engineering and forgery attacks where the attackers redirect the users to his or her crafted site from a legitimate web application. Figure 8.5 presents an example of the malicious URL set up by the attacker.

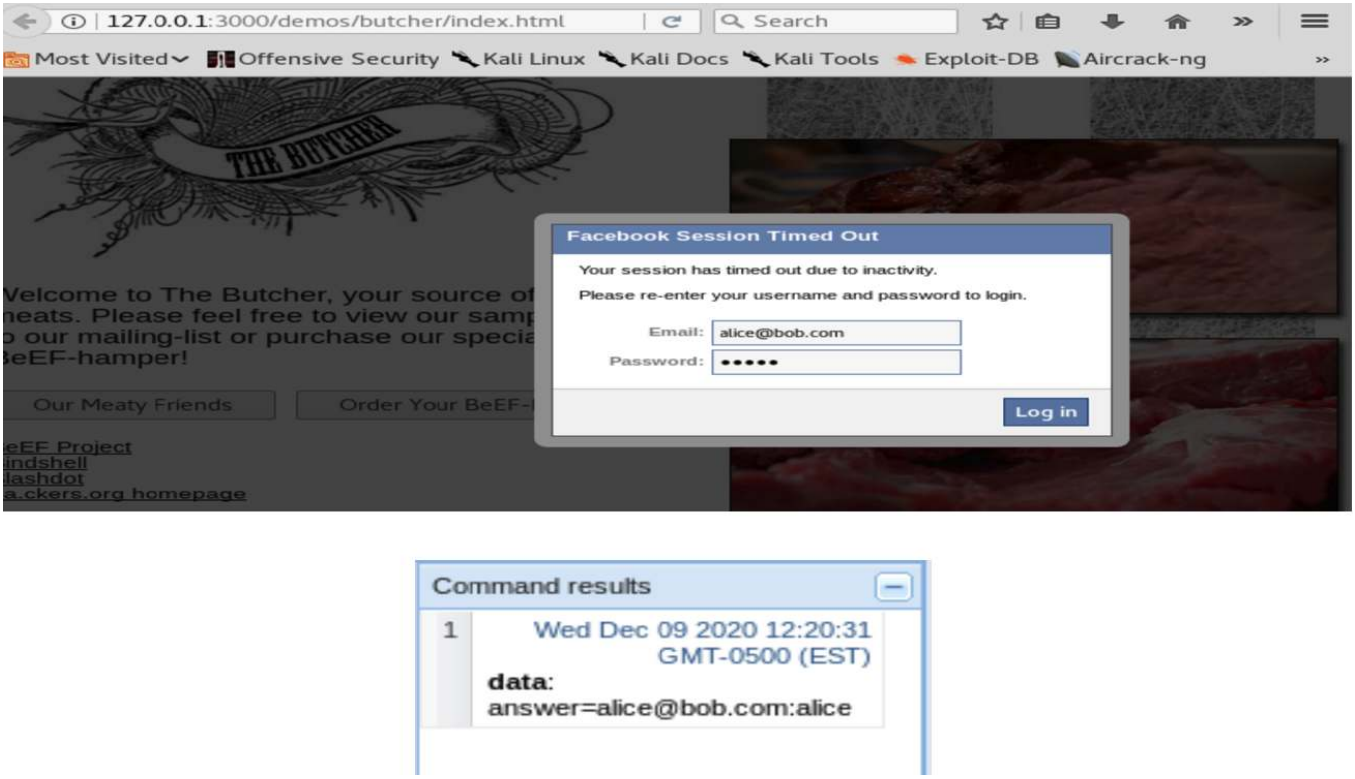


Figure **8.1.1.5.1**:

Malicious website crafted by the attacker

("Information Security" by Umar Khokhar Binh Tran is licensed under CC BY 4.0)

8.1.1.6: Directory Traversal Attack

In a directory traversal attack, the attacker accesses those directories and files which they are not authorized to access. The directory traversal attack typically exploits poor access control mechanisms of web applications. Figure 8.6 presents a directory traversal attack resulting from a vulnerable web application.

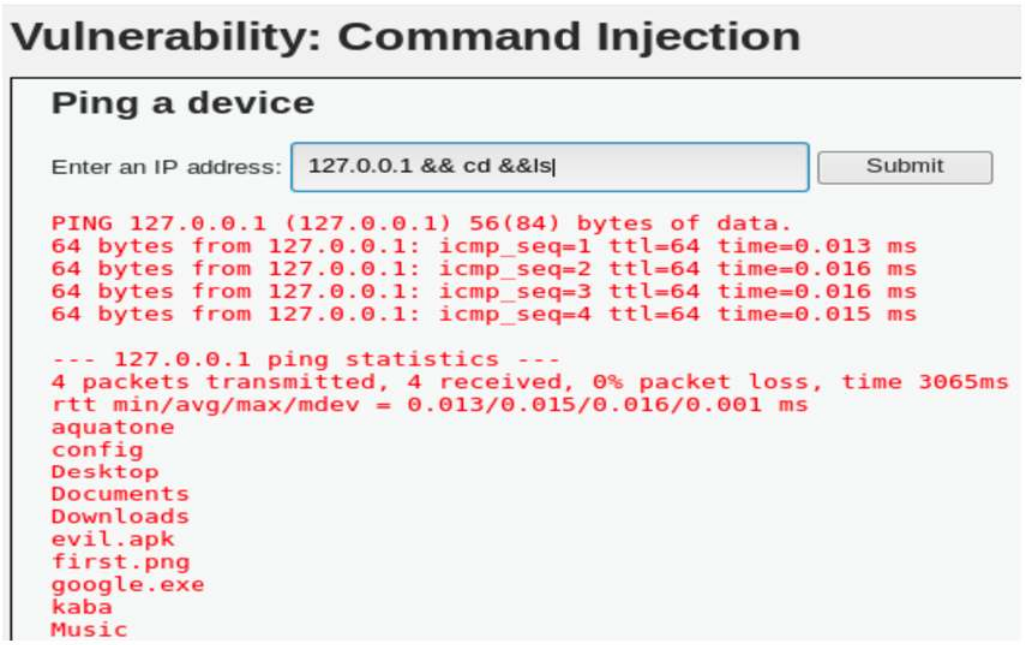


Figure **8.1.1.6.1**:

Directory Traversal (Command Injection) Attack

("Information Security" by Umar Khokhar Binh Tran is licensed under CC BY 4.0)

8.2: Wireless Networks Attacks

Wireless Communication Technologies (WCTs) e.g. Wireless Local Area Network (WLAN), Bluetooth and NFC etc. have started quickly replacing the wired networks. These WCTs have changed the way we use the Internet and manage digital resources. Besides, many of the benefits of WCTs, attackers have identified many pitfalls in protocols and structural vulnerabilities of WCTs especially Wifi (Wireless Fidelity) and Bluetooth. In this chapter, we will discuss some security attacks on Bluetooth and WLAN technologies. The details are presented on the following pages.

8.2.1: Bluetooth

Bluetooth is a WCT that uses short range radio signals and allows the exchange of information between a fixed and mobile device. The network which is established using Bluetooth technology is called Personal Area Network (PAN). When two (2) Bluetooth enables devices (one could be fixed and other mobile) come within the range of each other then one of the devices becomes “Master” and the other becomes “Slave”. The Master controls the overall communication and gives the instructions to the slave. The slave executes the instructions and returns the output. In the Bluetooth enabled car audio system, the cell phone acts as master while the car speakers act as slave. There are three (3) common Bluetooth security attacks; Bluejacking, Bluejacking and Bluebugging. The detailed description of these attacks is presented as follows:

- Bluejacking: Bluejacking is more of an annoying attack (rather than a harmful), in bluejacking, the attacker sends the unsolicited messages to the nearby Bluetooth-enabled devices. The bluejacking attack just displays a message on the victim’s device screen and does not make any connection with the remote device (Bluetooth device).
- Bluesnarfing: Bluesnarfing is a harmful attack in which, the attacker establishes a connection with the nearby Bluetooth-enabled device without the victim’s knowledge and accesses the internal data of the device. The attacker can copy the phone contacts, recent call logs, messages, emails and even the pictures stored on the device.
- Bluebugging: The most harmful attack as compared to other Bluetooth attacks is Bluebugging, in a bluebugging attack, the attacker first establishes a silent connection (without owner’s knowledge) with the victim’s device (e.g. Social Engineering techniques). After successful connection, the attacker installs a backdoor (malware) to bypass the authentication schemes and finally takes full control of the device. After having the full control over the device, the attacker can make phone calls from the victim’s device, activate call forwarding, change passwords or patterns and make copy the pictures or videos etc.

8.2.2: Wireless Local Area Network (WLAN) attacks

In 1997, IEEE (Institute of Electrical and Electronics Engineers) introduced the concept of WLAN under the project 802.11 and the term Wi-Fi was adapted in August 1999. This newly introduced way of connecting devices with Internet got a lot of attention and appreciation. Since, Wi-Fi involves wireless channels for communication information security was the only concern at that time, which IEEE tried to resolve with the integration of WEP (Wired Equivalent Privacy) security protocol with IEEE 802.11 standard. In 2003, several security analysts and researchers highlighted many vulnerabilities of the WEP protocol and raised the need of new security protocol. In 2003, IEEE proposed a new security protocol named; Wi-Fi Protected Access (WPA). In addition to encryption, WPA also introduced the key (password) based access control of the Wi-Fi routers which avoided the piggy backers to access the bandwidth. The WPA uses Temporal Key Integrity Protocol (TKIP) and validates the integrity of the exchanged messages which was better as compared to a CRC (Cyclic Redundancy Check) used in WEP. However, within six (6) months of its introduction, security analysts reported many pitfalls of the encryption scheme used in WPA which makes it even worse than WEP. Then in 2004, WPA2 was introduced which involves keybased router accessing mechanism and AES based encryption mode. In 2018, WPA3 was introduced as a replacement of WPA2. WPA3 mainly involves Simultaneous Authentication of Equals, offers forward secrecy and also ensures the protection of management frames. One of the inherent vulnerabilities of WLAN is the “undefined boundary” of the wireless network which allows the attackers to do multiple malicious activities e.g.

- Unauthorized scanning of the networks
- Interception
- Desynchronization attacks

To avoid most of the WLAN security threats, following two (2) recommendations are suggested:

- Disable broadcasting of SSID, once all legitimate devices are connected with WLAN.
- Use WPA2 or WPA3 to configure the WLAN.

In the following pages we discuss six main (6) security attacks of WLAN:

1. Rogue Access Points
2. Evil Twins
3. Intercepting the wireless data
4. Replay attacks
5. Denial of Service attacks
6. War Driving and Chalking

8.2.2.1: Rogue Access Points

Rogue Access Points (APs) are unauthorized APs installed by the attackers (sometimes by users as well) within the premises of the LAN. Since, the Rogue APs are not properly configured by the network administrators they allow the outsiders/adversaries to access the LAN and they can easily bypass security restrictions. Device authentication such as use of TACACS+, RADIUS+ and SAML can be used to avoid the Rogue APs.

8.2.2.2: Evil Twins

In Evil twins, the attackers use the SSID (Service Set Identifier) of the legitimate WLAN and set up an illegitimate AP in the close proximity usually where the range of the legitimate WLAN ends. The evil twins are installed outside the LAN and can be only detected/avoided using regular site surveys and network auditing.

8.2.2.3: Intercepting the Wireless Data

For data interception or Man in the Middle Attacks, typically the attacker joins the LAN, then use various packet sniffing e.g. Wireshark or Dsniff and MIMA tools such as Burp Suite and Ettercap to inject themselves between the victim and the webserver.

8.2.2.4: Replay Attacks

In replay attacks, the attacker captures the packets (traffic) of one authenticated (legitimate session) which could be in encrypted form and then replays them with one of the legitimate nodes in a later session to gain unauthorized access to the resources. Figure 8.7 presents the concept of the replay attack.

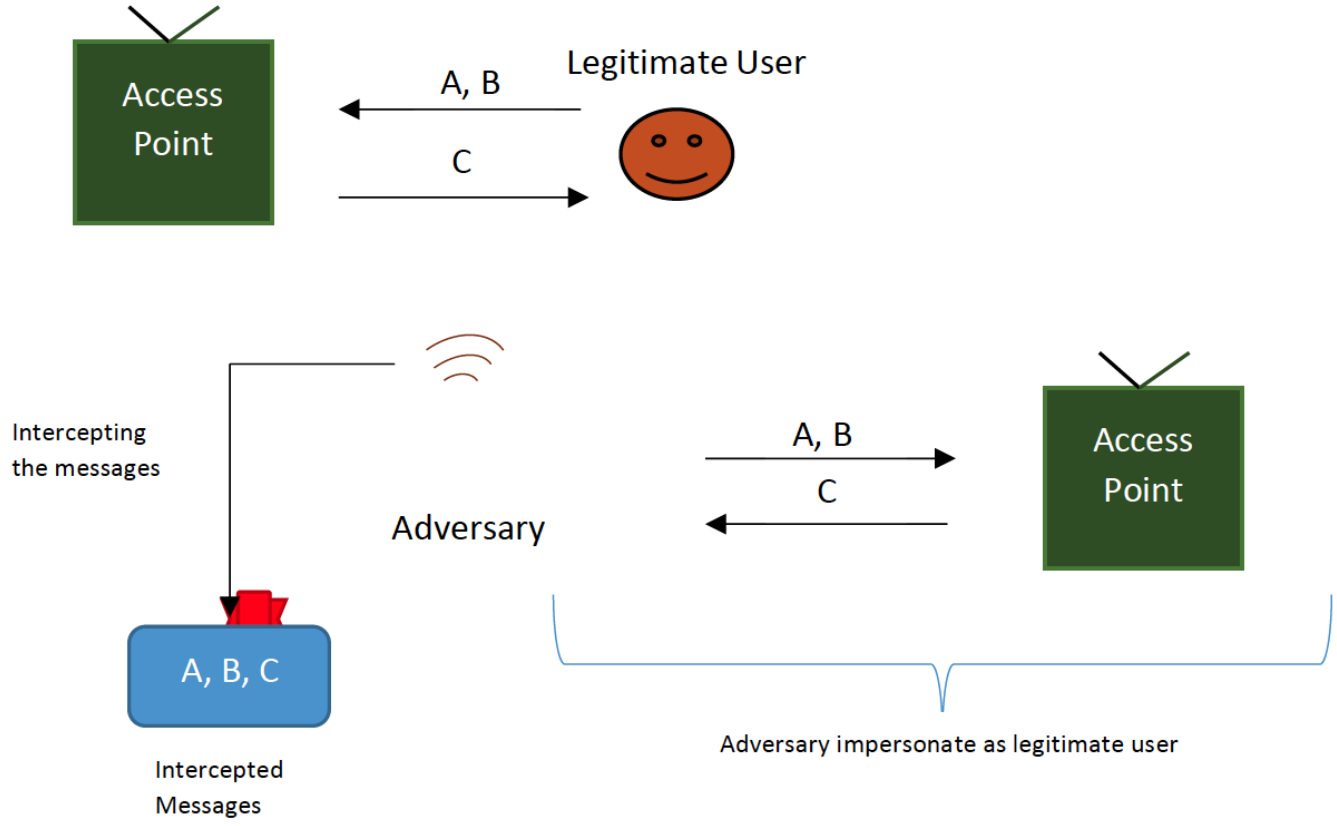


Figure **8.2.2.4.1**:

The concept of Replay Attack

("Information Security" by Umar Khokhar Binh Tran is licensed under CC BY 4.0)

8.2.2.5 Denial of Service

There can be two types of DoS attacks which can interrupt the WLAN normal operations: RF Jamming and Overwhelming the AP with manipulated field durations. In RF Jamming, the attacker generates and transmits excessive signals at 2.4 GHz & 5 GHz (Dual band Wi-Fi routers operate on this band) which eventually creates interference between the signals and makes it hard for the legitimate devices to communicate. The overwhelming of AP with manipulated field duration attack is a typical DoS attack which occupies the resources by sending unnecessary large packets which prevents the legitimate users to gain access of the resources.

8.2.2.6: War Driving and Chalking

In the war driving, the attacker uses the WLAN scanning tools (e.g. Kismet, Vistumbler and Acrylic Wi-Fi etc.) and drives down the streets to search for open access wireless networks. After finding the signal strengths, security protocol details and other relevant information about the WLAN, the attackers do the war chalking where they publish these details over internet (free blogging sides and social media etc.). Figure 8.8 shows the scanning of WLANs results using Vistumbler.

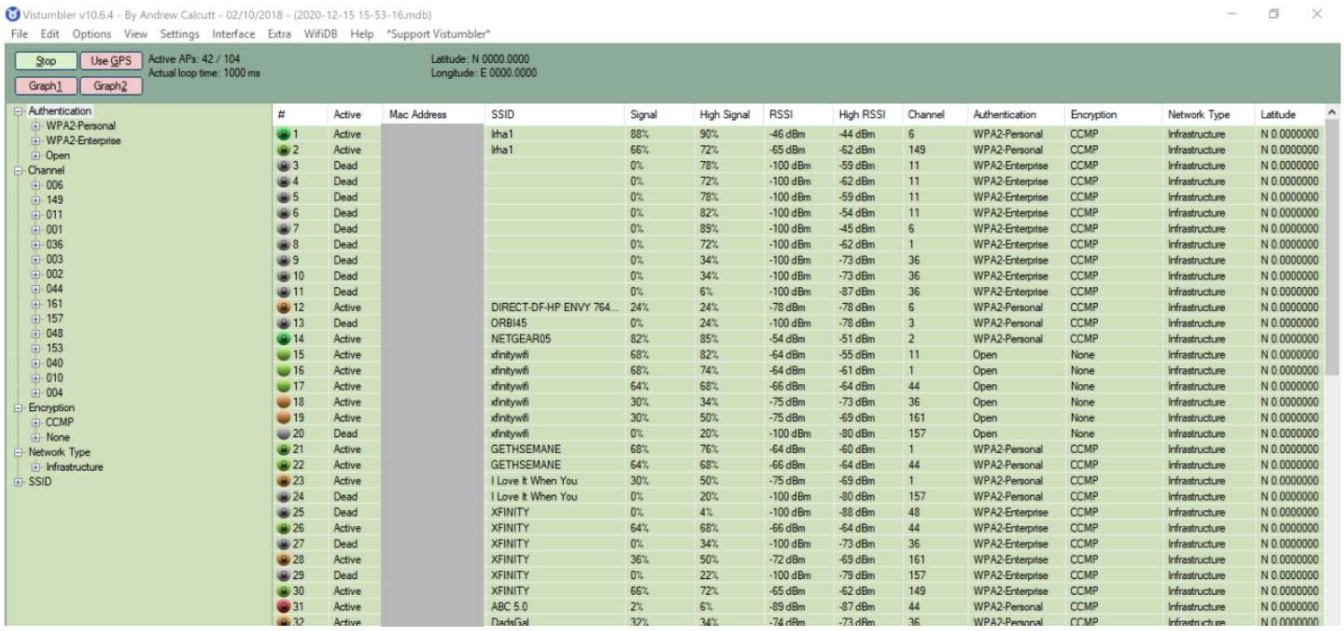


Figure **8.2.2.6.1**:

Scanning Results of WLANs using Vistumbler

("Information Security" by Umar Khokhar Binh Tran is licensed under CC BY 4.0)

CHAPTER OVERVIEW

9: Malware and Security Attacks

9.1 Malicious Attacks

The cyber-attacks are becoming very common now a days and nothing (Digital Systems) is 100% safe. The main reason of this dilemma is the presence of the juvenile hackers and script kiddies. In 2016, US law enforcement authorities sent a college student to prison for 20 years for hacking the US Vice presidential candidate's email account. There are many other similar hacking and data breaches examples. Although, these attacks grabbed the attention of news, media and public however, because of brand image & stocks most of the victims of these attacks don't publicize these attacks at all.

In 2013, Bloomsburg identified the top hacking countries, from where most of the security attacks are coming. In Bloomsburg's ranking, China was at the top with 41%, US ranked at 2nd with 10%, Turkey and Russian were placed at 3rd & 4th positions with 4.7% & 4.3% respectively. However, it doesn't mean that these countries have more hackers or security attackers but could have more proxy servers.

9.2: What we are trying to Protect

Mainly, we are trying to protect the following items from being compromised:

- Customer data: It includes the customer related specific information e.g. Name, SSN (Social Security Number), Phone number, address etc.IT Assets and Network Infrastructure: Unauthorized access of hardware (Computers, Scanner, Printers etc.) and Software applications.
- Financial data: Clients Bank accounts, Credit and debit card information etc.
- Service availability and Productivity: Continuous access of the resources to the legitimate users
- Reputation and Brand Image: The company reputation and brand image by avoiding the security breaches.

9.2.1 What is a Security Breach?

Any event that results in violation or that compromises the CIA of the system is called security breach. Some security breaches are accidental and some are intentional. Let us talk about the activities that cause the security breaches.

9.2.2 Activities that cause Security breaches

There are six (6) main activities through which CIA can be compromised or breached. The details of those activities are described as follows:

9.2.2.1 Denial of Service (DoS)

The DoS attack violates the Availability parameter of CIA. In DoS attack, the attacker overwhelms the system with excessive queries and prevent the legitimate users from gaining access of the resources. The DoS attack can be launched using techniques; Logic attack and Flooding. In the logic attack, the attacker use the software flaw to crash or hinder the performance while in the flooding attack, the attacker engages the system with unnecessary queries which makes it unavailable for legitimate users. The flooding attack can be classified into further two types: SYN Flood and Smurf attack.

- SYN Flood:
  In the SYN flood attack, the attackers exploit the vulnerability of the SYN protocol (TCP/IP) where after receiving the SYN request the server waits for the user's SYN ACK message. To better understand the SYN flood, firstly, lets understand the SYN protocol: As we know the TCP is a connection-oriented protocol, where the sender makes connection first before sending any packet. Assume that Alice wants to access a webserver (Á). So, Alice's computer will send a SYN Request to the Á and now if Á is up then it responds back with SYN ACK and opens a channel and waits for SYN ACK from Alice's computer. The SYN ACK makes sure that Alice's computer has received server's acknowledgment. After receiving SNY ACK from webserver, the Alice's computer responds back with SYN ACK and then the bi-directional communication starts. The figure 3.1 shows the working of SYN protocol. To launch SYN flood attack, the attacker firstly creates a Botnet (network of computers controlled by the hacker) and use the Botnet to initiate the SYN protocol. After receiving SNY request from the Botnet, the webserver responds back with SYN ACK and then waits for SYN ACK. The Botnet doesn't respond the server back but instead initiate a new SYN protocol and again after receiving SYN ACK, none of them respond the server back. The attacker repeats this process again and again unless the server runs out of resources and becomes unavailable for legitimate users. The figure 9.2 typical three way handshake.

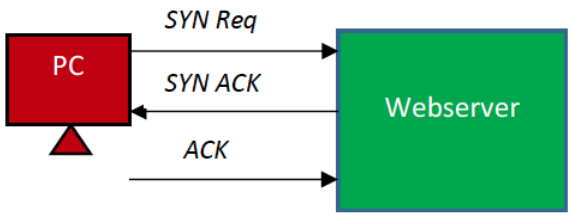


Figure 9.2.1: Three Way handshake (SYN Protocol) ("Information Security" by Umar Khokhar Binh Tran is licensed under CC BY 4.0)

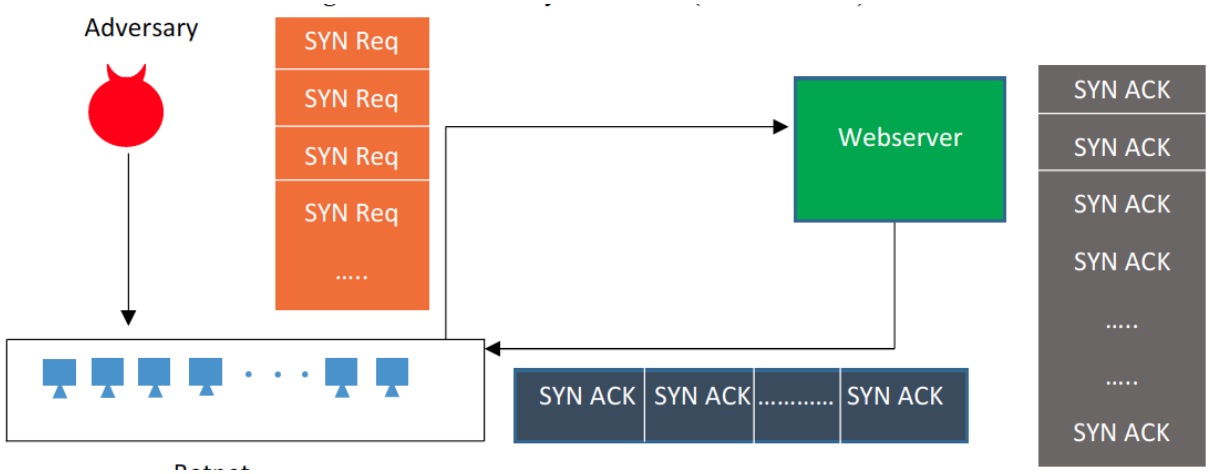


Figure **9.2.1**: SYN Flood ("Information Security" by Umar Khokhar Binh Tran is licensed under CC BY 4.0)

- Smurf attack:
  In smurf attack model, the attacker first joins the network with which the target is connected. The attacker then impersonates as target's computer and broadcast a ping packet to all connected nodes. When this ping packet arrives to the nodes, then they will start responding back to the target's computer (even though it did not request for it). The attacker repeats this process unless the victim's computer overwhelms.

9.2.2.2: Distributed Denial of Service (DDoS)

The Denial of Service attack which is launched through multiple points (nodes) is called Distributed Denial of Service (DDOS). In the DDOS attack model, the attacker uses Zombies and Botnet. The Zombie is a computer which is controlled by hacker remotely while the Botnet is the network of Zombies.

9.2.2.3: Unacceptable Web Browsing

The unacceptable web surfing can also cause security breaches. The following actions come under unacceptable web browsing:

Violation of organization Acceptable Use Policy (AUP) Visiting Prohibited Websites Trying to access files/directories that you are not supposed to access.

9.2.2.4 Wiretapping

The attackers can tap the telephone lines and data communication lines both actively and passively (Sniffing) . The active wiretapping can be further classified into two types:

- Between the lines: Active wiretapping, the attacker adds additional information and doesn't modify the original message.
- Piggyback: The attacker completely modifies the message contents.

The most widely used tools for sniffing are Wireshark and Dsniff.

9.2.2.5 Backdoors

Software that includes hidden access methods are called backdoors. For example, Rootkits are the malicious software that opens the backdoor of the target computer to let the back traffic in or can turn off firewall/antivirus.

9.2.3 Additional Security challenges

There are some other security challenges that can also cause security breach:

- Spam: Unwanted emails and mostly the carrier of malware.
- Spim: Unwanted Instant Messages
- Hoax: is some act intended to deceive or trick the receiver.

- Cookies: is a small text file that contains user preferences, user related specific information e.g. User name, password, address, credit card number etc. The web browsers allow the webservers to store a cookie on user's hard drive.

9.3: Types of Active Threats

The following are the types of different active threats that can exploit the vulnerabilities of the computational systems which eventually compromise the security.

9.3.1 **Password Cracking attacks:**

Most of the password cracking attacks are offline, where the attacker steals the hash file of the password and use cracking tools to guess the password. Some of the following methods are widely used in cracking tools

- Birthday attack: The birthday attack is a type of cryptographic attack that exploits the mathematics behind the birthday problem of the probability. The birthday problem concerns the probability in a set of 'n' people having same birthday. The birthday attack model uses the probability of 'n' people having the same password to guess the password.
- Dictionary attacks: Instead of launching brute force (all possible combinations), in this attack model, the attacker does three tasks; create a dictionary of the relevant passwords, calculate the hashes of dictionary and then make a comparison of all computed hashes with stolen hash to guess the password.
- Session Hijacking: The attacker intercepts the communication of server and victim's computer and steals the session token. After having the session token, the attacker takes the control of session and can inject malicious traffic to both the server and the victim's computer.
- Social Engineering attack: The attacker tricks the users to get the confidential information by creating a con, sending phishing email or pharming (Section 3.3.3 discusses the Social Engineering attacks are discussed in detail).

9.3.2 Malicious Software

The short form of Malicious Software is Malware where 'Mal' is take from Malicious and 'ware' is taken from software. Any software which does the following four functions is known as malware;

- Causes the damages
- Bypass the security framework
- Disclose the confidential data
- Modify or delete data

There are many types of malware, some of the common malware types are as follows:

9.3.2.1 Virus

The term computer virus is inspired from its biological counterpart. A biological virus firstly infects one cell then it turns the infected cell into factory of virus and start infecting other cells. Similarly, after entering the computer, the virus attaches itself with a file and starts infecting that file. Then the infected file starts infecting other files and eventually creates obstruction in the normal operation of the computer.

A computer virus can be formally defined as "A small piece of code that migrates through networks and can attach itself with different program files". The virus cannot replicate itself and it requires a human intervention for transportation. The following are the three main virus infection methods:

- Appender Infection : In this infection method, the virus appends itself at the end of the program file instruction at the beginning of the program code. Whenever the user opens the file, the jump instruction redirects the control to the virus code. The Appender infection virus can be easily detected by the antivirus (while scanning the infected file).
- Swiss Cheese Infection: This infection method is similar to the Appender method, where the virus code attaches itself at the end of the program file. However, the virus code is encrypted which makes it hard to detect for anti malware. The decryption keys are randomly placed across the program file and tied together with jump instructions. When the program file is executed the virus code is unveiled and takes control over the session.
- Split Infection : The virus code is broken down into several small pieces and placed at random locations across the program files. The small chunks of the virus code are tied up through a jump instruction and when the infected file is executed, the control is redirected to virus main body

The figure 9.3 describes the three virus infection methods.

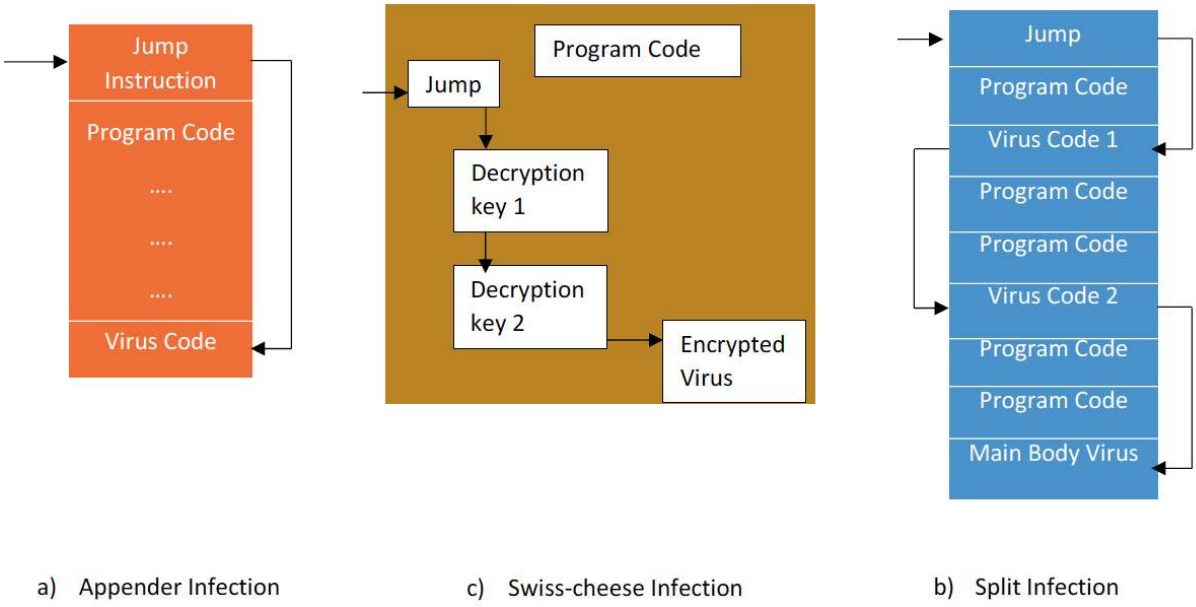


Figure **9.3.1**: Virus Infection Methods ("Information Security" by Umar Khokhar Binh Tran is licensed under CC BY 4.0)

9.3.2.2 Worm

The worm is a self-contained program that replicates itself and propagates across computer and network without human intervention. The main objective of the worm is to exhaust the network bandwidth and create botnets.

9.3.2.3 Torjan Horse

The programs that disguised as something useful with underlying malicious contents and backdoors. Usually, the trojan horse arrives with the free downloadable contents or sometimes just by visiting malicious websites. The trojan horse collects and sends the sensitive information of the victim's computers (which includes web browser history and cookies etc.) to the attackers. Also, trojans open the backdoors (open ports, turn off AVS etc.) to let the bad traffic in, on the victim's computer.

9.3.2.4 Rootkits

The rootkits hide themselves in Operating System files and get triggered each time whenever the victim restarts (reboot) the computer. The rootkit allows the remote user (attacker) to install the rogue files, delete the files, create backdoor and also rootkits hide the existing malware from being detected as well.

9.3.2.5 Adware

The Advertisement Software (Adware) usually designed using JavaScript and are embedded on the malicious websites. When, the victim visits the malicious website the script automatically runs and installs itself on the victim's computer. The adware collects the web browser history and then create an unsolicited targeted advertisement and popup messages. The adware can also pull the session and persistent cookies which are serious threat to privacy and security of the individual.

9.3.2.6 Spyware

The spyware collects and forwards the victim's activities and classified information which includes keystrokes, passwords, web browser history and cookies to the attacker. The keystroke logger is one of the most common type of spyware which records all the keystrokes of the users and sends the recorded data to the attacker.

9.3.3 Social Engineering attacks

The Social Engineering is a process that utilizes the knowledge of the human nature to get information from people which can be further used for destructive purposes. The Social Engineering techniques involves some kind of deception and trick the innocent

users to get their classified information (such as passwords, Social security numbers or Financial details). The main idea of the Social Engineering is “Rather than cracking the password why not ask them their password”. The following are some types of the Social Engineering techniques:

- Authority: Use of power/position to get classified information of the subordinates.
- Dumpster Diving: Collection of information from Un-shredded papers.
- Hoax: Creating a con that involves some kind of deception to get the confidential information of people.
- Phishing: Tricking the people over email (Malware can also be attached with emails).
- Vishing: Tricking the people over phone (Impersonation).
- Whaling: Targeting the top-level managers (Executives) of an organization.
- Pharming: The attackers craft a real looking fake website and then try to redirects the users to the fraudulent website to get their confidential information.

9.4: Wireless Networks and Web Application attacks

In this section, an overview of wireless networks and web application attacks has been presented. The detailed description of these attacks is discussed in in another section.

9.4.1 Wireless Network Attacks

Some of the wireless network attacks are described as follows:

Bluesnarfing: allows the attackers to establish a connection with the victim's Bluetooth enabled device and provides an unauthorized access to its internal data. The attacker can copy the contacts, emails, messages and even call logs without the owner's consent.

Rogue Access Point : An unauthorized Access Point (AP) installed within the legitimate LAN and without proper security configurations is called Rogue Access Point. The Rogue Access Point allows the attackers to bypass the security framework/authentication of the LAN.

Evil Twin : An AP installed by an attacker (outside the legitimate LAN) which uses the same SSID (Service Set Identifier) as of legitimate one is called Evil Twin.

Packet Sniffing : The attackers use IP Packet capturing software such as Wireshark and Dnsiff etc. and can sniff the on-going communication (Packets) of the LAN.

Replay Attacks: The attacker captures the packets/messages of a genuine session and then replays them in a later session with the legitimate parties to gain unauthorize access or desynchronize the legitimate parties.

War Driving: The attacker uses the software such as Vistumbler, Arachni etc. and then drives down the street to look for the free/open Access points. The searching for the open access point is called War Driving.

War Chalking: After War Driving, the attackers publish the information of the open Access Points with Geolocation map (Coverage area) on blogging sites which is called War Chalking.

9.4.2 Web Application Attacks

Since, the tradition network security devices (Firewalls, IPS and IDS) ignore the HTTP contents, so to ensure security of web applications is much more difficult and different as compare to securing a typical network. The detailed description of the web application security concepts is discussed in Chapter 8. The following are some of the web application attacks.

Buffer Overflow Attack: In the Buffer overflow attack, the attackers find the bugs/mistakes in the coding of an application and then exploit it to gain unauthorize access to the system. The attackers push more data beyond the capacity of the buffer and make the application to store the additional data to adjacent memory buffer. It can crash the system and also create a backdoor which lets the bad traffic in.

Cross site scripting: In the Cross-Site Scripting (XSS) attacks, the attackers injects malicious scripts on the vulnerable websites and usually target the clients of the websites. When the users visits the contaminated website then these scripts automatically run and can steal the cookies and web browser history of the victim's computer.

SQL injection attack: In the SQL injection attack, the attacker first finds whether the webserver is vulnerable to SQL injection attack or not. If the webserver is vulnerable to SQL injection attack, then the attacker injects the SQL commands and obtain the secret information (stored on Database) of the individuals.

XML injection attack : In XML injection attack, the attackers manipulate the XML logic of the application and inserts the malicious contents into the resulting outputs. In XML injection attack, the attackers can login as Administrators and can have full control over the server and databases.

9.5: Recommendations for Avoidance

These cyberattacks are becoming very common and inevitable in this modern era where digitization encompasses almost all the aspects of the life. However, many of these attacks can be avoided if the companies/individuals follow the following recommendations:

9.5.1 Multi-Factor Authentication (MFA)

The authentication is a process which ensures whether the individual is who he/she claims to be not an imposter. The typical way to perform authentication is knowledge-based authentication where the legitimate individuals are provided with the username and password and they will be authenticated using the provided credentials if they want to access resources. However, with the integration of Artificial Intelligence (AI), the password cracking tools have become much more powerful than before and also new sophisticated phishing attack models can lead to disclosure of the credentials. So, beside using Knowledge- based authentication, some other factors such as biometrics, IP address, tokens/security codes or actions can also be assimilated with the existing single factor authentication to avoid password cracking attacks.

9.5.2 Security Analysis/Penetration testing

The penetration testing is an authorized (legal) cyberattack to test the organization's computer networks/systems robustness against real-world cyberattacks. While doing the Penetration Testing, the security analyst first finds the vulnerabilities (pitfalls) of the networks and web applications then creates an exploit (venom) to demonstrate how these vulnerabilities can compromise the organization's assets. Finally, most of the security analysts provides recommendations as well to avoid the highlighted attacks. The security audit and Penetration testing can avoid many of the forthcoming threats to the organization.

9.5.3 Educate Users

The Users/people are the weakest link of any organization. The organizations should offer basic security trainings to educate their employee about the recent developments in security fields and familiarize them regarding Social Engineering techniques. The security trainings should involve following topics:

- Phishing and Pharming
- Ransomware attacks
- Basic Ethics of using Computational systems
- Password Management Software
- Organizational Security Policies and AUPs

9.5.4 Anti-malware

As discussed in section 9.3.2, there are different types of malware and some of them can arrive at victim's computer only by visiting the malicious website or just by downloading applications (with underlying malware). The surfing over internet without having an updated anti-malware could be dangerous and can turn your computer into a Zombie computer. Therefore, an updated anti-malware must be installed on individual's computer and organizational systems to avoid most of the pre-existing malware.

9.5.5 Firewall and Network Security Devices

The firewall inspects all incoming and outgoing traffic and then allows/denies packets based on the defined rules. In addition to anti-malware, the firewall also plays an important role to prevent the adversaries from gaining unauthorized access and stealing data from the individual(s) and organizational computers. The firewall can be software (e.g. the one which comes with windows computer) or it can be hardware (e.g. Palo Alto and Cisco NGFW etc.). To ensure the optimal security, an organization should include some other network security devices/software e.g. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in their security fleet. Beside the runtime security, these network security systems provide enormous data for security analysis which is eventually helpful to combat against zero day attacks.

CHAPTER OVERVIEW

10: Social Engineering

10.1: What is Social Engineering

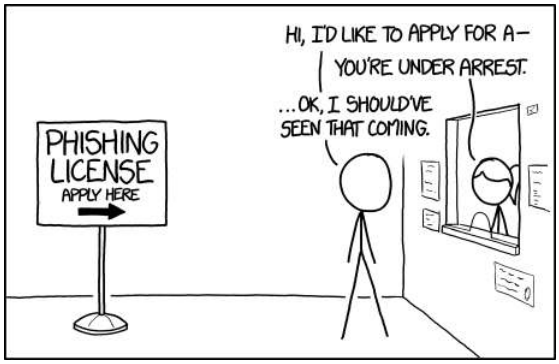


Figure **10.1.1**: A comic from XKCD, a popular techy-nerdy comic strip. (CC-BY-NC)

Social engineering is leveraging social contracts and manipulating people to divulge information or behave in a certain way. Social engineering is hacking humans. Social engineering is conning people.

One of the best known social engineering artists is Kevin Mitnick. Kevin spent five years in jail for a number of computer related crimes. Most of his imprisonment and charges were highly controversial, and Mitnick was seen as an idol in the hacking community. Since his release, he has written four books. His first, The Art of Deception, is the bible of social engineering (you should totally read the book!).

He owns Mitnick Security Consulting, LLC and is also the Chief Hacking Officer and part owner of the security awareness training company KnowBe4[1]. One of the KnowBe4 tools includes sending fake emails to employees at companies to see if they fall for the bait (they also offer cybersecurity training). If you'd like to know more, you can read chapter 3 from the 2012 book The Path of Least Resistance for free.

You should be intimately aware of phishing by now - and phishing falls under the umbrella of social engineering. Consider these real-life cases:

"You gotta send that money NOW!" CEO says

Though his identity remains anonymous (and you'll see why in a minute), in 2019 the CEO of an unnamed UK energy firm received a phone call from the Chief Executive of the parent company - a person he knew well. He transferred about $240,000 to the account of a Hungarian supplier[2]. Business as usual. Sure, there was a bit of urgency to the request, but he knew the person requesting the transfer so it didn't raise any flags. The catch? The CEO of the parent company never made the request and the transferred money was immediately moved to another account (and was lost for good). The culprit? The voice of the CEO was mimicked by artificial intelligence[3].

Help the police

In 2021, a 90-year-old woman in Hong Kong was contacted by law enforcement in mainland China. It seemed that someone had been using her identity for criminal activities. The law enforcement agency sent over an officer to deliver a cell phone for direct communication with them. Happily, she was able to rectify the mistaken identity by giving the authorities roughly $32 million dollars… Or did she? Turns out the phone calls and the officer were both part of a scam[4].

Out of order

Back in the 1960s it was common for businesses to drop bags of money off at banks after hours; they would deposit the money in a one-way vault at the bank. On one particular night, around thirty people from various companies arrived at the bank to see a sign that said, "NIGHT DEPOSIT VAULT OUT OF ORDER. PLEASE MAKE DEPOSITS WITH SECURITY OFFICER." Each of the thirty employees did as instructed and received a hand-written receipt from the bank's security guard. Turns out the security guard was not employed by the bank; he had just obtained a uniform and fabricated the sign.[5] Perhaps you've heard of the imposter - Frank Abagnale (whose adventures were chronicled in the 2002 movie Catch Me if You Can.

Yes, the name of my company is legit

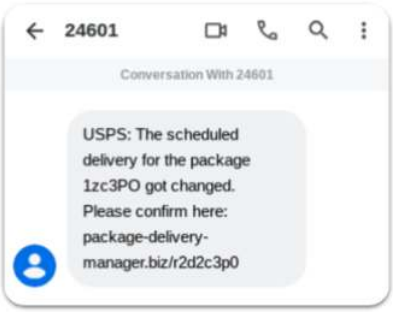
In 2019 the Department of Justice finally caught up with Evaldas Rimasauskas (a Lithuanian citizen). He discovered the name of a company in Asia that sold products to big tech companies like Facebook and Google and then incorporated a company with the same name in Latvia. After creating a few corporate bank accounts with the same name in Latvia and Cyprus, he started sending invoices to the big tech companies. Over the course of three years, he stole over $100 million![6]

Department of Labor invites you to bid on work

In 2022 the Department of Labor sent emails to vendors inviting them to submit bids for upcoming projects. The professional emails had PDFs attached with instructions on how to submit a bid. The PDF had a link to the bidding site, and the site had DoL branding. One of the steps for bidding included a Microsoft Office 365 login (you probably see where this is going). Turns out that the URL for submitting the bids (and the email address) were not genuine DoL addresses. Instead, they were derivatives (like doi-bids.us, for instance).[7]

Who doesn't love packages?

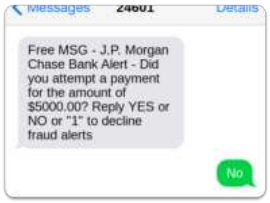
In April 2021, people across the country started receiving texts from the United States Postal Service about packages in transit that had been rerouted. All you had to do was click on the link to track the package and see the updates. As you've probably guessed, the link led to malware with the intention of stealing some of your data.



Of course, an astute person would recognize that the link looks wonky, but that didn't stop people from clicking on it.[8]

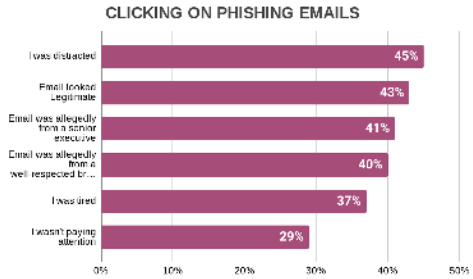
Texts and calls

Later that year, attackers ramped up their methods. A man's daughter received a text from J.P. Morgan inquiring about a $5000 transaction. She replied "NO" and immediately received a phone call from the bank confirming that the transaction attempt was fraudulent. The catch is that she was asked to verify some account details to make sure she was who she claimed she was. This story has a happy ending; she was savvy enough to tell the caller that she would call the bank herself - using the official phone number. She avoided a potentially catastrophic attack.[9]



Social engineering is a serious threat to organizations. In 2021, over 80% of organizations surveyed by Proofpoint reported a successful email phishing attempt (that was up from 46% in 2020!). Proofpoint attributes three factors - "Pandemic Fatigue" (employees are more likely to make an error in their inbox attentiveness), shifting infrastructures (cloud computing and personal devices have been adopted without sufficient training and configuration), and seductive lures in emails (namely Squid Game, Justin Bieber World Tour, and economic issues such as unemployment and relief[10]).

A report from Stanford found that 47% of respondents have admitted to clicking on links in phishing emails. While this data is insightful, there is concern that it is underreported. Based on other factors in the survey, Stanford suggests that some respondents were *unaware that they had* engaged with phishing emails. They also hypothesized that people under report for fear of their job.[11]



Phishing attempts typically result in either compromised data or ransomware victimization. According to Sophos, the average bill for rectifying a ransomware attack in 2021 was $1.85 million.[12] Perhaps you remember the Colonial Pipeline ransomware attack - that cost about $5 million (though the FBI was able to recover about half of that after the fact).[13] But the trophy for the biggest payout of 2021 (and a new World Record!) goes to CNA Financial Corporation. A payout of $40 million in March of 2021 to a Russian Cybergang.[14]

---

1. Kevin Mitnick [Wikipedia]
2. A Voice Deepfake Was Used To Scam A CEO Out Of $243,000
3. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case
4. 90-year-old Hong Kong woman loses $32 million in phone scam
5. Catch Me If You Can: The True Story of a Real Fake
6. Lithuanian Man Pleads Guilty To Wire Fraud For Theft Of Over $100 Million In Fraudulent Business Email Compromise Scheme
7. Office 365 phishing attack impersonates the US Department of Labor
8. Don't click the link: USPS scam texts draw attention to 'smishing'
9. SMS About Bank Fraud as a Pretext for Voice Phishing
10. 2022 State of the Phish
11. Understand the mistakes that compromise your company's security
12. The State of Ransomware 2021 [Sophos]
13. U.S. recovers $2.3 million in bitcoin paid in the Colonial Pipeline ransom
14. CNA Financial Paid $40 Million in Ransom After March Cyberattack

---

10.2: Techniques of Social Engineering

In the vignettes above, did you notice that all but one of the examples required the attacker to get the target to install malicious software? One of the things that is so scary about social engineering is that you don't necessarily need technical prowess; you just need to be good at getting people to trust you.

That is not to say that social engineering does not rely on technical skills - indeed many attacks do. But social engineering is certainly a good way to start an attack. I have an affinity for social engineering because it is a bit of a cerebral attack. Any script kiddie can download software and launch an attack. But it takes a refined, sophisticated, clever mind to successfully perpetrate a social engineering attack.

OSINT

Typically an attacker will start with **OSINT** (open source intelligence). OSINT is information that is openly available. For instance, an attacker might electronically "case the joint" as their first step. Let's say they want to compromise the CEO of a company. Well, a good first step would be to visit the CEO's LinkedIn profile. Who are some of the employees at the company? Who else outside of the organization does the CEO communicate with? Next the attacker might look for an Instagram feed. Unlike Facebook (where you need to be *friends*), Instagram allows attackers to get a lot of information on the target. Does the victim go on vacation at the same time every year? Is there information in the photos that indicates where the victim spends time? What hobbies does the victim enjoy (hobbies are an easy way to artificially engage in conversation)? Check out Network Chuck's quick demo on Osintgram!

OSINT is not just social media. Most towns have public tax rolls that list home addresses and property tax information. Perhaps the target is on a board of directors or the school board - their name (and ideas) will appear in published minutes from meetings. Maybe the victim has been in the local newspaper. Maybe the victim has a criminal record. Maybe the victim hasn't changed the default settings on some of the apps they use so things like their Venmo transactions, Strava runs, or Amazon Wish Lists are visible. Heck, there is even a book entitled "You Can Find Anybody!" by Joseph Culligan (licensed PI) that contains hundreds of resources where you can find information on people (an aggregation of thousands of public databases). There are plenty of OSINT tools that social engineers can use (like Maltego, Creepy, theHarvester, SpiderFoot, metagoofil, and TinEye) and we'll be using Sherlock and Social Engineering Toolkit in this chapter. There are also some really neat OSINT Search Bookmarklets you can put into your browser.

Techniques

After gathering information on a target, there are plenty of techniques a social engineer can use to trick the target.

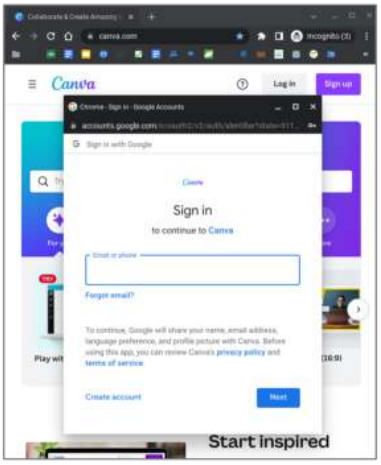
Authority	Attackers assume an authoritative position. This could be as simple as wearing an outfit (like when a thief stole an ATM disguised as a repairman) or appearing important, knowledgeable, and trustworthy.
Baiting	Luring marks into compromising situations. This can be done with USB drives (that's how Stuxnet was brought into Iranian centrifuges) or clicking on malicious links.
Dual reality	A technique where two (or more) parties are experiencing the same thing but how they internalize the event is different.
Dumpster diving	Going through the trash of a person or organization in an effort to gain inside information. A social engineering firm went dumpster diving in the trash of a company they wanted to infiltrate - they were able to find the names of the tech support team for the company and used that to craft a successful infiltration.
Phishing	An attempt to lure a victim into a trap via a fraudulent email crafted to look like a legitimate opportunity. In 2016, $78 million was stolen from Crelan Bank in Belgium because of a phishing email.
Pretexting	This is a stage of social engineering that takes place before the attack; it lays the foundation by creating a plausible situation where the attacker earns the trust of the mark. For instance, in the iconic movie Home Alone, Harry and Marv convince everyone in the neighborhood that they are police officers and will keep an eye on all the houses as families travel for the holiday season.
Quid pro quo	Giving something to someone in return for something else. Brian Brushwood talks about the Coke study, but this technique is used as a vector of attack (for instance, Office Depot offered a PC Health Check, but would inform the customer that their computer was broken and charge them $180).
Scareware	"Your computer may be infected!" - you've probably seen this before. It's a scare tactic intended to drive users to pay for software to protect their computer (though there is no actual issue). In 2021 reports of the Cryxos trojan increased; the software scares users with pop-ups declaring that a virus has been found - but you can remove it by calling a number and paying for tech support!
Shoulder surfing	Looking over the shoulder of a victim as they enter their keycode into a keypad on a door or their PIN number at an ATM.
Smishing	Phishing via SMS (texting). Texts that evoke urgency, texts that suggest you've won a prize, and texts that suggest unusual account activity that needs corrective actions are all suspect. The "Zelle Fraud Scam" is a great example of creating urgency and lending authority - and it tricks the victim into surrendering their six digit 2FA number!
Spear phishing	Pointed phishing that usually requires reconnaissance on the target. One step of the reconnaissance is OSINT (open-source intelligence).
Tailgating	Unauthorized access into a facility perpetrated by following authorized people. Wearing a uniform (delivery, for instance) can help sell the tailgating endeavor. Standing outside a building and smoking/vaping where everyone else in the building goes to smoke is a good way to tailgate.
Urgency	A method of social engineering where the attacker pressures the victim by time-boxing them ("This offer is only good for 19 more minutes!" or "This is your bank and you need to confirm your personal information immediately!").
Vishing	Phishing via voice. Recently a UK energy company was scammed out of $243,000 because of a vishing scheme (it happened to use a deep fake voice), but urgency was a key ingredient.
Whaling	Whaling is spear phishing high-profile or high-ranking personnel (like the CEO of a company).

New attack methods

Bad actors are constantly developing new tools to attack our systems. Not surprisingly, social engineering is always at the forefront of innovation because of two things - it's cheap and it's effective. Oftentimes emerging social engineering trends are low fidelity and easy to implement.

Browser in the browser

One of the more clever forms of social engineering and phishing has just emerged. Known as ***browser in the browser*** attack, the website uses Javascript to craft a **Single Sign On (SSO)** modal window that looks just like a bonafide SSO window). The



catch is that the window that pops up will harvest your credentials if you enter them. This is almost impossible to detect, and most people are used to single sign-on which might increase victimization.

Consider this image - can you determine if the single sign-on modal is legitimate or an imposter?

The easiest way to determine the validity of this modal is to test to see if it is in fact a *standalone browser window* - which it should be or a Javascript-created box. Try minimizing the browser tab (in this case, Canva). If the SSO box is still visible, then it is a window and it is not a BitB attack. However, if the SSO box vanishes when you minimize the browser, then it is likely fake and you should be cautious.

QR Codes

Some might argue that QR codes are not a social engineering scam but they do fit squarely into the social engineering space. People trust them (authority), they pray on our need for immediacy (urgency bias and convenience), and they are easy to distribute. However, unlike robbing a cryptovault, there typically needs to be boots on the ground to implement.

QR codes were introduced in 1994 but didn't gain widespread adoption until 2011. During the pandemic, QR codes gained even more momentum as they were used as a mechanism to provide contactless services (such as downloading a menu at a restaurant). Evidence of the popularity of QR codes was given during the Superbowl in 2022 when cryptocurrency company Coinbase aired a sixty second ad that was nothing but a QR code. More than 20 million people used their phone to scan the code, breaking the Coinbase app! The scary thing is that 20 million people pointed their phones at a QR code not caring about the risks.

In January 2022, the FBI warned that QR codes are the "perfect example of people exploiting a daily exercise." The FBI released a public service announcement the same month:

> Malicious QR codes may also contain embedded malware, allowing a criminal to gain access to the victim's mobile device and steal the victim's location as well as personal and financial information. The cybercriminal can leverage the stolen financial information to withdraw funds from victim accounts.

They also suggested a list of tips to protect yourself.

- Once you scan a QR code, check the URL to make sure it is the intended site and looks authentic. A malicious domain name may be similar to the intended URL but with typos or a misplaced letter.
- Practice caution when entering login, personal, or financial information from a site navigated to from a QR code.

- If scanning a physical QR code, ensure the code has not been tampered with, such as with a sticker placed on top of the original code.
- Do not download an app from a QR code. Use your phone's app store for a safer download.
- If you receive an email stating a payment failed from a company you recently made a purchase with and the company states you can only complete the payment through a QR code, call the company to verify. Locate the company's phone number through a trusted site rather than a number provided in the email.
- Do not download a QR code scanner app. This increases your risk of downloading malware onto your device. Most phones have a built-in scanner through the camera app.
- If you receive a QR code that you believe to be from someone you know, reach out to them through a known number or address to verify that the code is from them.
- Avoid making payments through a site navigated to from a QR code. Instead, manually enter a known and trusted URL to complete the payment.

Even without malware, failing to be vigilant with QR codes can be disastrous. In some cities in Texas, parking meters have a QR code and instructions to pay with your phone. In February 2022, someone printed their own QR code stickers and slapped them over the existing one. When patrons scanned it with their phone, they were directed to a fake website that looked *just like* the real parking website. Patrons were instructed to enter their credit card information and then assured that the meter fare was paid.

Not surprisingly, the credit card information was abused *and* many people probably wound up with parking tickets!

In an even more flummoxing case, QR codes have started showing up in phishing emails and online ads. One rationale might be that QR codes can probably sneak through spam filters easily. But the reality that people who are in front of a computer will take out their phone and snap a QR code is troubling - that's one critical reason why it's important to train people about the hazards.

Old and New Social Engineering

CSO Online published an article laying out five old social engineering attacks that are still popular today - as well as four emerging trends.

Five popular social engineering attacks

- Official-looking email
- "Here's a free USB stick"
- The office gift card scam
- "You have a voicemail" email
- "There's a problem with your package delivery"

Four new social engineering attacks

- "Here are your legal documents from DocuSIgn"
- The "aging accounts report" scam
  - Someone from accounting gets an email from (allegedly) a company executive curious about outstanding balances from customers. Once the attacker has this information, they craft emails to their targets with specific information on how much is owed and where to send it. Spoiler alert - they are not sending the money they owe to the company they owe it to.
- "There's a problem with your bank account. Click here to resolve the issue"
- Phishing by phone

10.3: Social Engineering in Action

Some of the best ways to learn about social engineering is to learn some of the tactics that social engineers use. The following three videos are TOTALLY worth your time to watch:

 YouTube Video	Penetration tester David Kennedy is hired by companies to test their security. In an interview for the CNN, Kennedy shows off his skills. In under three minutes he manages to convince a tech support specialist at a company to click on a malicious link. David Kennedy is the founder of TrustedSec and authored the Social Engineering Toolkit utility.
 YouTube Video	A brilliant demonstration of social engineering from a hacker at DefCon. Note how in this video the hacker creates a sense of urgency and confusion by using exasperation, a crying baby, and wonderful social engineering techniques. Jessica Clark demonstrates in under three minutes how easy it is to get personal information from a phone company - this is how SIM swapping happens!
 YouTube Video	Brian Brushwood is an entertainer, juggler, magician, and author who has a long running YouTube channel called Scam Nation. He also co-hosts the Modern Rogue YouTube shows as well. In this YouTube video, you'll see Brian give a great TEDx talk about social engineering. It is roughly 16 minutes, but you'll walk away with some foundational understanding of the psychology behind social engineering. If you like this video, check out his podcast, The World's Greatest Con.

10.4: Social Engineering in Hollywood

The following video clips are from movies. I've done my best to curate a small, digestible, binge-worthy list of clips from movies you may not have seen. Two thoughts:

1. You should watch all of these movies, *especially Sneakers*
2. I've provided commentary to contextualize the clips.

Matchstick Men

Matchstick Men is a 2003 movie about con men. Starring Nicolas Cage (Roy), Sam Rockwell (Frank), and Alison Lohman (Angela), the movie chronicles the scamming tricks of the trio. Things start to heat up as the movie unfurls in unsuspecting ways.

There are two clips worth looking at. In this one, Frank sets his mark up by guaranteeing that they have won a high-end prize (a new car, a trip, etc.). Once he establishes rapport--note that he gets to know how many grandchildren the mark has), he pulls his AUTHORITY card; he tells them that they are on the hook for the sales tax. The AUTHORITY is fortified by Roy posing as a Frank's boss:

https://www.youtube.com/watch?v=GwQdBsTpmOM

In this second clip, Angela is learning how to scam. In the previous scene, she accompanies Roy's character into a convenience store. They buy a lotto ticket for *today*, but select four of the five numbers from *yesterday's* winning numbers. Then they distress the ticket by rubbing it on surfaces so it looks like it's been through the wash. They take special care to rub off the date of the ticket. Angela comes into a laundromat and subtly suggests to a patron that a found lottery ticket might be a winner. Note that this scam relies on a few things - AUTHORITY of a (fake) winning lotto ticket, RAPPORT of a young, polite, innocent girl, a HUNGRY MARK (the con men bank on patrons of a laundromat to have lotto dreams), and INCEPTION of the idea (the mark is the one who advances the plan -- of her own volition).

https://www.youtube.com/watch?v=TOrEE5NeZ9w

Sneakers

Sneakers is a 1992 movie about penetration testers that totally stands the test of time. In this scene, the team is attempting to break into a rather secure building. One of the plants, River Phoenix (Carl) has arrived before the infiltration occurs. His AUTHORITY is asserted because of his costume and his delivery of Drano. Carl is arguing with the front desk guard who is not expecting the delivery. Quickly we see Robert Redford (Martin) establish IDENTITY and PRETEXT in his first contact. He has a LEGITIMATE REASON for being in the building; there is a party on the fourth floor and he is expecting the cake to be delivered. Luckly, Martin sees the delivery and vanishes from the front desk. He arrives a few seconds later with a cake so big he can't reach his ID card (which clearly he doesn't have anyhow). Tension is rising as the security guard's argument with Carl escalates. There is CONFUSION and URGENCY (remember, the cake is late!) as Martin tries to get the guard to buzz him in. Only the first 40 seconds are relevant to the conversation of social engineering:

https://www.youtube.com/watch?v=oG5vsPJ5Tos

Wolf of Wall Street

The 2013 movie Wolf of Wall Street is a true story of Jordan Belfort (played by Leonardo DiCaprio), a huckster who made a fortune selling "penny stocks" or "pink sheet stock". His rise to crime and corruption is a fascinating story.

In this scene, Belfort, coming off a job at a big brokerage firm, brings his guile to a small outfit that specializes in cheap stocks. Belfort brings URGENCY into his conversations with his marks, AUTHORITY because of his knowledge, and leverages EXPLOIT (the "pink sheets" are not really regulated like blue chip stocks are).

This clip has some vulgar language and may not be appropriate for some audiences; watching this clip is optional!

https://youtu.be/nJzo5TDfamk?t=166

In this second clip, we see Belfort training his new employees how to scam marks. There are a number of tactics here that work out well for the crew. They establish URGENCY by saying that these stocks are going to go up immediately, and waiting until then will be too late. They established PEDIGREE with a firm name that is completely made up -- Stratton Oakmont. Even their logo inspires pride, tradition, knowledge, and trust. The crew establishes AUTHORITY by reciting stocks of big, well-known companies in an effort to sell "penny stocks".

This clip has some vulgar language and may not be appropriate for some audiences; watching this clip is optional!

https://www.youtube.com/watch?v=sxRStrx8xtc

Hackers

In the 1995 movie Hackers, Johnny Lee Miller plays Dade, a talented hacker. In this scene, Dade calls a local TV station and using CONFUSION and KNOWLEDGE successfully convinces an unsuspecting employee to reveal the phone number for the modem to the station. This lets him change the TV programming schedule so the station broadcasts an episode of The Outer Limits.

https://www.youtube.com/watch?v=_G3NT91AWUE

Catch Me if You Can

The true story of Frank Abagnale is captured in the 2002 film Catch Me If You Can. Frank Abagnale was a true con artist -- most notable for faking (convincingly) as a pilot, doctor, and lawyer. The following clip shows how Frank (Leonardo DiCaprio) realized how effective AUTHORITY is. He shows up to his first day at a public high school after spending his childhood in a public school. He's wearing a suit jacket and is mistaken for the substitute teacher. Note the DUAL REALITY that he employs (the students believe he is assigned to the class for the first time, meanwhile the actual substitute teacher is convinced that he is always the substitute for Roberta):

https://www.youtube.com/watch?v=KAeAqaA0Llg

Though not portrayed in the film, there was another stunt Frank orchestrated that relied on the AUTHORITY of a uniform. He brought a chair to a bank one night and sat outside the nighttime deposit box. He also rented a security guard outfit. He fashioned a

sign that read, “Deposit broken. Please leave money with the Guard.” Between the outfit and the SOCIAL CONTRACT of the patrons (they certainly did not want to be embarrassed by not trusting the guard!), it was enough to convince patrons that their money was safe.

In another scene of Catch Me If You Can, Frank is caught by FBI agent Carl Hanratty (Tom Hanks) who has been pursuing Frank for a while now. Frank emerges from the bathroom of the apartment he is renting only to find Agent Hanratty with his gun drawn. Frank quickly realizes that Agent Hanratty does not know what he looks like, so he convinces Hanratty that he is a Secret Service agent who is also hot on the trail of Abagnale, too. By using AUTHORITY, INSIDER KNOWLEDGE (about how the Secret Service works) and DUAL REALITY (he convinces Hanratty that his neighbor, Murphy, has already caught Abagnale while Murphy has no idea what is going on - Frank even covers any confused response Murphy may have had with a cough):

https://www.youtube.com/watch?v=CiXTwfipyqk

10.5 Preventing Social Engineering

- Most imitated brands in phishing emails in first quarter of 2021: report
- 10 Common Social Engineering Attacks & How to Prevent Them
- Social engineering: A cheat sheet for business professionals
- Verify End-Users at the Helpdesk to Prevent Social Engineering Cyber Attack
- Get ready for Zoom-based deepfake phishing attacks, expert warns
- Scammers imitate Windows logo with HTML tables to slip through email gateways
- Why cybercriminals looking to steal personal info are using text messages as bait

Further Investigation

If you are interested in learning more about social engineering, you might want to check out these links:

Dual reality and magic

Social engineers and magicians have overlapping skill sets. The concept of dual reality has been around in magic for centuries. Penn & Teller perform a trick that demonstrates dual reality very clearly. In this case, the participant experiences something completely different than the audience. Typically in magic, neither the audience or the participant will actually experience the secret. But this is Penn & Teller.

This video shows David Blaine performing a trick called “Invisible Touch”, which is a good example of dual reality (though this performance doesn’t really highlight the concept). The revelation of this trick is similar to a longer routine performed here.

A really good explanation of how magicians leverage dual reality is described by O’Brien Magic here (watch from 4:35 to 7:00).

Presentation on social engineering

Jen Fox (DefCon Capture-the-Flag black badge!) talks about -- and demos -- social engineering in her talk at the SANS Security Awareness Summit (2018)

A cool study about the word “because”

https://www.psychologytoday.com/us/blog/brain-wise/201310/the-power-the-word-because-get-people-do-stuff

Open-Source Intelligence (OSINT) in 5 Hours - Full Course - Learn OSINT!

CHAPTER OVERVIEW

11: Secure Software Design

11.1: Introduction to Software Security

Figure **11.1.1**: A comic from XKCD, a popular techy-nerdy comic strip. (CC-BY-NC)

Imagine this common scenario: you are in the airport, about to board your plane when you decide to take a selfie of yourself getting on the plane - boarding pass in hand and posting it to social media.

It is not unreasonable to take and post photos of that nature; in fact you probably have seen many images similar to that in the past.

The reality is that you may have announced to the world some very personal details. This exact scenario happened to Tony Abbott, a former prime minister of Australia. In this case, multiple security flaws existed which allowed anyone to see the photo to get Tony Abbott's passport number and phone number.

The Reality

Writing software is easy. Writing good software is hard. Writing secure software is extremely hard. This chapter will examine security concerns as they relate to software design, implementation and deployment.

Fortunately, organizations exist to identify, define, classify and provide documentation around security "best practices". One such organization, Open Web Application Security Project (or OWASP) exists with a particular emphasis on web applications. Although the OWASP Top 10 has an emphasis on web applications, many core concepts remain outside of the web application world. However, organizations like OWASP are vitally important as more and more software is deployed through web applications.

11.2: Using Other Software as Building Blocks

Software today is often quite complex. So complex that it is nearly impossible for one organization to write all the code. Frequently developers will use smaller pieces of code as building blocks. For example, imagine a developer making an application similar to Spotify. There could be a fair amount of custom code such as user account management, storing and retrieving playlists or songs, etc... The code to take an audio file and convert it to sound is fairly low level and would have to support edge cases such as older file formats (.WAV files), support digital rights management and decompress the audio. In this case, the developer may choose to use a "library" or "package" which manages these tasks. Such a library would handle the mundane tasks such as converting the file to audio, obtaining track metadata such as title and artist from the file and similar functions.

Using these libraries has some benefits including:

- Libraries are often used by multiple software and are generally tested more robustly than standalone code
- Libraries preclude developers from having to deal with edge cases or areas of concern which reside outside the comfort of the developer
- Popular libraries tend to have a good community following, so help is often easy to come by

Be aware that libraries can have some downsides as well.

Supply Chain Attacks

A "supply chain attack" occurs when someone knowingly supplies something with malintent in an effort to disrupt, observe or destroy a consumer upstream.

The Restaurant

Consider the case where a head chef, Addison, is expecting a food critic (Blair) at Addison's new restaurant. Sous Chef (Charlie) is jealous of Addison and knows that a bad review might end Addison's career. Charlie devises a plan: when Addison asks for sugar to make candied sauce for the vegetables, Charlie will hand Addison the salt instead.

This is a "supply chain attack" because Charlie knowingly supplies the wrong ingredient to Addison. Addison may not even realize this because the salt *looks* and *feels* like sugar. When the critic tastes the candied vegetables and realizes that they taste terrible instead of sweet, Addison will get a bad review.

In software, particularly web applications, this attack can be devastating. Most web applications these days rely on tens, hundreds or thousands of small libraries. The "NPM" packages (NPM stands for Node Package Manager) libraries - often implemented in JavaScript - are suitable both for front-end applications as well as back-end logic.

The Case of "left-pad"

In 2016, a developer removed a very small piece of code from NPM[2]. The code was called "left-pad" and was less than 12 lines long. The package merely added spaces to the left part of a string in order to make the string a specific length. For example, this code:

leftpad("hello", 10)

Would return the string " hello" (note that the string is now 10 characters long). While this code is not complicated, it is quite useful (often used for aligning text). As such, it was used by thousands of packages. And those packages, in turn, were used by thousands more packages. All of a sudden, hundreds of thousands developers noticed that their code would not compile because left-pad was no longer found.

The developer who removed the code likely did not anticipate the scope of the problem; in response, NPM published the package again and also removed the ability for developers to delete a package under normal circumstances.

While the removal of left-pad was not intended to cause problems around the globe, it was a high profile example of just how fragile library supply chains can be.

Protestware

The Russian incursion of Ukraine in March 2022 has led to the emergence of protestware - that is, intentional poisoning of a supply chain. The first known occurrence happened in mid-March. An NPM package called node-ipc was updated to remove files from the user's machine and replace them with an emoji of a heart (assuming the computer was geolocated in Russia or Belarus)[3].

Crypto-Miners

Crime can pay! In 2021, a security research firm identified several NPM packages which secretly installed crypto mining[4] software on developers machines.

This example is more common; that is, packages which intend to be malicious. Sometimes malware may be included in packages in order to steal credentials, compromise developers computers or initiate a ransomware campaign.

Video Players

In January 2022 Palo Alto Networks Unit 42 discovered a dangerous (and admirable!) supply-chain attack on cloud-based, customizable JavaScript video players mostly used on real estate sites. The attackers were able to access the upstream JavaScript file and include malicious skimming code. "On the next player update, the video player began

serving the malicious script to all sites that already had the player embedded[5]". The attackers were able to abscond with names, addresses, phone numbers, and credit card information.

Okta Attack

You may never have heard of Okta before, but they are an authentication firm with 15,000 clients (including FedEx and CloudFlare) so there is a good chance you use some of their services in some capacity. In January 2022, an account take over (ATO) at one of Okta's service providers led to downstream effects including affects for 366 of Okta's clients[6]. This is an especially interesting case of a supply chain attack in that Okta itself is a supply chain target but *their* reliance on Sitel as a third-party provider resulted in the attack. It was a supply chain attack on a supply chain provider.

Whereas a supply chain attack might be characterized as "getting the keys to the kingdom", attacking Okta and other similar providers is more like "getting keys to the factory where the keys to multiple kingdoms are made".

Combating Supply Chain Attacks

Supply chain attacks happen all the time (MailChimp in 2022[7], Microsoft Exchange Server in 2021[8], SolarWinds in 2020[9], British Airways in 2018[10]) but there are ways to mitigate them. While some might argue that building systems from scratch instead of relying on code reuse is the solution, the adage "Given enough eyeballs all bugs are shallow[11]" is a potent reminder of the durability of well-vetted open-source software. One particular weakness of a home-grown solution is that the code is private and cannot be audited. For a recent example look no further than Samsung's proprietary implementation of Android's Trusted Execution Environment that led to vulnerabilities in 100 million smartphones[12]. Or consider a (as of this writing) *still persistent* mishandling of account logins at Coinbase - bad actors can gain intelligence on email accounts linked to a Coinbase account, easing phishing campaigns. The issue is that a bad actor can divine email addresses with a Coinbase account and then target them. This isn't the first time Coinbase suffered from a vulnerable design. In 2019 a data exposure revealed 3,500 plaintext passwords[13] and in 2021 over 6,000 accounts had cryptocurrency stolen because of a flaw in the SMS account recover scheme[14]. While there is no evidence to support the claim that the email confirmation/denial issue is a byproduct of homegrown code, that type of mistake is indicative of amateur programming.

We have started to see attempts at securing supply chain attacks. In May 2021, Executive Order 14028 Improving the nation's cybersecurity was given. In response, in July 2021 the National Institute of Standards and Technology (NIST), along with the Cybersecurity & Infrastructure Security Agency (CISA) and the Office of Management and Budget (OMB) released two key publications[15] that are stage three of a seven stop program:

- Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028
- Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security

Outside of governmental involvement there are a few different private endeavors that are being rolled out. Described in more detail in the next section, GitHub's Dependabot helps by alerting developers of supply chain threats[16]. Additionally, Google is creating tools and methodology to help developers verify "build provenance". In other words, developers can be equipped with tools that will help verify that source files are not malicious or that malicious artifacts have not been injected into code. The framework that improves the integrity of development is known as Supply-chain Levels for Software Artifacts (SLSA)[17]. As supply chain attacks increase, tools to help combat them will also increase in efficacy and adoption.

TechRadar ran a piece in March 2022 suggesting that developers accept that fact that code reuse is inevitable so proper mechanisms to verify the code in development and distribution is a proactive way to mitigate supply chain attacks[18].

Vulnerable and Outdated Components

Using libraries, packages or components from third parties can introduce security concerns. OWASP lists this as number 6 on their top 10 list[19]. Generally this refers to software libraries which either contain security vulnerabilities (inadvertently) or become outdated.

log4j

Just in time for Christmas in 2021, the very popular library log4j was discovered to have a remote code execution vulnerability[20]. The vulnerability had existed for years and affected several versions of the software. When news of this vulnerability surfaced, companies around the world had to fix or update their code in order to ensure that they were not vulnerable.

openssl

The openssl library might be considered the de-facto standard for open source encryption. Providing services such as encryption, decryptions and certificate validation, it is important in nearly all manners of encryption. While it is expected that vulnerabilities exist in all software, some particularly nasty bug were found in 2003 which led to the ability to trick servers into disclosing the server's private key[21].

The way to mitigate such an attack is to keep libraries up to date. This can be an automated process. For example, GitHub provides the use of "dependabot[22]", which was originally released in 2020 as a way to automate dependencies with security issues[23], the most recent version released in April 2022 notifies software authors when libraries are available which address vulnerabilities[24]. The dependabot can also offer to patch software with the latest version.

WinRAR

Even software as innocuous as compression software can be problematic. In 2019, researchers found an error with WinRAR that let attackers gain full control over a user's computer[25]! Issues like this can be especially insidious because users have an implicit belief that popular utilities should be relatively safe (and for 19 years, WinRAR was safe). But the most pernicious part of this story is that WinRAR does not have an automatic update feature - so unless everyday users get their daily news from cybersecurity outlets, there is a good chance people are unaware of the issue (or that the issue can be fixed with a simple update).

Routers

We see the no-automatic-updates problem often in home routers as well. Though the latest trend in home routers do a much better job of updating automatically, for a long time that was not the case. And the percentage of average users that ventured into their router to manually check for updates and install any updates that exist is probably very low. This problem is even worse when companies are aware that their products are susceptible to attacks and won't even release updates. This happened in late 2021 when Cisco informed users of remote attack that gave unauthenticated attackers the ability to execute arbitrary code on the target device[26].

Dependency Confusion

Another fascinating attack was discovered by ethical hacker Alex Birsan in February 2021 (he reportedly made roughly $130,00 in bug bounties for this discovery). Dubbed dependency confusion, the hack was simple. In fact, it did not even require malicious injections; rather his hack leveraged poor design for software development processes. The oversimplified explanation is simple[27]:

- Companies have private code repositories that other code relies on

- Birsan found those repository names in code that was published
- Birsan then publicly published his own code with the same repository name
- Companies' development tools defaulted to the public repository when given the option
- Birsan pwned many companies including Apply, Microsoft, and Shopify

As a reminder to cybersecurity professionals - when a vulnerability is published, fix any liabilities in your organization. In the wake of Birsan's post, copycats of his attack targeted several companies (including Amazon, Slack, Zillow, and Lyft) by poisoning public repos that were relied on[28].

But this isn't the only threat based on a model of developing using repositories. A similar attack, repo jacking, requires more malicious energy. If an attacker knows what GitHub repositories a company relies on, that hacker can monitor the dependent repositories. If the owner of the repository changes their username, the hacker can swoop in, create an account with that username, and then publish their own code[29].

2. How one programmer broke the internet by deleting a tiny piece of code
3. Sabotage: Code added to popular NPM package wiped files in Russia and Belarus
4. Popular npm Project Used by Millions Hijacked in Supply-Chain Attack
5. Hackers use video player to steal credit cards from over 100 sites
6. Okta Says It Goofed in Handling the Lapsus$ Attack
7. Mailchimp hacked to launch 'exceptional' supply chain attack
8. China's and Russia's spying sprees will take years to unpack
9. What You Need to Know About the SolarWinds Supply-Chain Attack
10. British Airways breach: How did hackers get in?
11. Linus's law [Wikipedia]
12. 100 million Samsung phones affected by encryption weakness
13. Coinbase Hack Attributed to a Multi-factor Authentication Flaw That Allowed Scammers To Steal Cryptocurrency
14. Coinbase says hackers stole cryptocurrency from at least 6,000 customers
15. NIST Delivers Two Key Publications to Enhance Software Supply Chain Security Called for by Executive Order
16. Secure your software supply chain
17. Improving software supply chain security with tamper-proof builds
18. How to finally secure the software supply chain
19. A06:2021 – Vulnerable and Outdated Components
20. Log4j Vulnerability FAQs
21. Debian Security Advisory
22. GitHub dependabot
23. Keep all your packages up to date with Dependabot
24. Prevent the introduction of known vulnerabilities into your code
25. Extracting a 19 Year Old Code Execution from WinRAR
26. Cisco Small Business routers vulnerable to remote attacks, won't get a patch
27. Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies
28. Malicious NPM packages target Amazon, Slack with new dependency attacks
29. Repo Jacking: Exploiting the Dependency Supply Chain

11.3 Privacy

Software developers need to be concerned with privacy as well as vulnerabilities. Privacy can be a tricky line for software, particularly as it relates to social media. For example, some people can make a case to have all social media posts viewable by anyone - after all, one point of social media is to reach a larger audience. Contrast that with a medical record provider who must keep as much information private as possible. There is a line to balance somewhere in the middle, but that line is not always clear and certainly depends on the users expectations and preferences as well as any laws governing data availability.

Application Default Settings

Most software allows tweaking of settings, from preferred language to background color to security considerations. Software developers try hard to make the default settings reasonable. Keep in mind that it may be challenging or impossible to devise default settings which are in the best interest of all users.

Strava

Strava can be a great social application to share workouts with like-minded people and find new places to run or cycle. In 2018, Strava generated heat maps from users such that all users could find common places to run simply by looking at a map. While specific user data was protected, aggregate data was still available. In this case, heat maps were used to identify military bases[30].

As well, when running routes are available for anyone to see, it generally becomes trivial to identify where someone lives as their runs often start and stop where they live.

Venmo

Default security settings in Venmo caused some concern. In 2021, Venmo announced that it would be removing the global transaction feed. Until that was released, strangers' transactions would be available for all to see. Indeed this is an invasion of privacy at the least but arguably a security concern. In addition to that, users' friends lists were publicly available, as well, representing a huge security violation.

Broken Access Control

The number one spot in the OWASP Top 10 is "Broken Access Control". This vulnerability, when expressed, can lead to " unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits[31]"

Remember Tony Abbott?

Recall that in the opening story in this chapter, Tony Abbot had his passport information and his phone number exposed. One reason that this happened is because sensitive information was sent to an unauthorized actor. In particular, anyone with the last name and boarding pass number (which was included in the social media photo that Mr. Abbott shared).

An eerily similar (but more widespread) issue happened in Missouri. A website that lists names of teachers in the state and their certifications was flawed in that it also included the social security numbers of the educators (albeit the social security number was not displayed on the screen but was present in the HTML for the site). A reporter named Josh Renaud responsibly disclosed his findings to the organization responsible but then reported on it when the issue wasn't fixed. While this is not necessarily poor design (when people can right-click and choose "View Source" to reveal private information is never a good idea), politicians made it much worse. Governor Mike Parson accused Renaud of hacking private information. Captain John Hotz from the state police said they were "investigating the potential unauthorized access to Department of Elementary and Secondary Education data."

The New York Times reporting of the incident highlights the government's absurd misunderstanding of the law[32]:

Mr. Parson, a Republican, said that it was "unlawful to access encoded data and systems in order to examine other people's personal information."

He cited a state law that said a hacker was anyone who gained unauthorized access to information or content. He said the reporter had no authorization to "convert or decode" the information on the website.

"This was clearly a hack," Mr. Parson said, adding that the state would investigate the flaws that were uncovered in the system.

Legal observers said they were perplexed by Mr. Parson's interpretation of what constituted a hack.

Frank Bowman, a professor of law at the University of Missouri School of Law, said that it was difficult to imagine the prosecution of a reporter who alerted state officials to information he discovered by examining a publicly available website.

The chances of prosecutors going after Mr. Renaud, the reporter, "are between zero and zero," Professor Bowman said. "They're not going to embarrass themselves like this."

Clearly, legislatures are failing to keep up with technology and it is challenging democracy.

30. Strava tweaks map settings that inadvertently displayed military sites
31. A01:2021 – Broken Access Control
32. Governor Accuses Reporter of Hacking After Flaws in State Website Are Revealed

---

11.4 Software Design

CVE's

Common Vulnerabilities and Exposures

Managed by the MITRE corporation,the canonical list of CVE's is comprised of a list of publicly disclosed security flaws[33].

Because CISA (overseen by the Department of Homeland Security) funds the CVE program, perhaps one of the clearest places to find a directory of recent CVE's is at the Known Exploited Vulnerabilities Catalog (hosted at CISA).

Of course, a searchable database may be easier to use when looking up CVE's by number.

Design Considerations

Authentication

Authentication is perhaps one of the most commonly used security functions. Nearly all apps and websites use some form of authentication in order to assert that a user is who they claim to be. Authentication often appears in the form of a username and password. More recently multiple factor authentication has risen in popularity.

Before we even go into the more technical issues with authentication, check out this innovative scam that requires little technical understanding. Gmail accounts have a “dots don’t matter” feature. That means that the address thisisnotanactualaddress@gmail.com is the same as this.is.not.an.actual.address@gmail.com as far as logging in and receiving email is concerned. However, many user accounts at other websites would consider these as two different accounts. Netflix is one of these accounts. And you don’t need to verify your email account to start watching videos on Netflix.

Someone who had a Netflix account with the email thisisnotanactualaddress@gmail.com is insecure. I could create an account at Netflix with a very similar email address - this.is.not.an.actual.address@gmail.com - and when it came time to enter payment information, Netflix would email the account holder at this.is.not.an.actual.address@gmail.com asking for payment information. But that email would actually go to thisisnotanactualaddress@gmail.com. Since the email would actually come from Netflix and would seem legitimate, the Gmail user with the email thisisnotanactualaddress@gmail.com might inadvertently enter payment information for my account[34]!

Now let’s look at some of the more technical issues. Implementing security, particularly

authentication, has been shown historically to be hard to accomplish. In fact, at least 3 of the OWASP Top 10 are related to authentication.

A02:2021 – Cryptographic Failures[35]

While not specific to authentication, "Cryptographic Failures" does have a place within authentication. In particular, consider these points

- Using weak or compromised algorithms for encrypting persisted data can make is easier for intruders to obtain sensitive data such as passwords or personal information
- Prefer storing derivable sensitive information over encrypted (or plain-text) values; for example, storing a salted and hashed password (which is derivable) instead of the plain-text password should be preferred

A04:2021 – Insecure Design[36]

Again, this tenet is not specific to authentication but does play a large role. Have you seen these poor security practices implemented?

- Ability to reset a lost password merely by answering questions?
  - Such questions are often obvious or easy to guess or otherwise find the answer to
- Are file uploads available?

- A web server may be vulnerable if uploaded files are not restricted or validated. For example, uploading a malicious PHP file instead of a profile photo could put the server at risk because subsequent calls to the uploaded PHP file may result in arbitrary code running in an escalated environment.

- Do default passwords exist?
  - It is common today to find devices with default usernames and passwords; for most consumers this is evident on home routers, though newer routers have started shipping with either unique credentials OR the requirement that users define credentials before the device can be used

A07:2021 – Identification and Authentication Failures[37]

The name alone indicates the relationship with authentication. This risk pertains to poorly implemented authentication. There are several ways to implement poor authentication, including some of the more common failures:

- Allowing brute force attacks; throttling or limiting the number of login attempts can go a long way to mitigating this failure
- Permitting weak or common passwords; doing so reduces security by allowing brute force attacks to become more successful. While not called out by OWASP specifically, limiting password length or valid characters also can be problematic for users
- Not allowing multi factor authentication; the industry is moving to a multi factor authentication model because such a solution can offer greater security and (in some cases) more convenience
- Providing clues about account information; invalid login attempts which specify "invalid user" or "invalid password" can be leveraged by hackers in an attempt to identify valid user names. Instead, consider a generic message along the lines of "invalid username or password", which does not provide any information about the existence of a username.

- A03:2021 – Injection[38]

  Injection does not refer solely to SQL injection, though SQL inject is perhaps the best-known type of injection attack.

  An injection attack most frequently occurs when software uses user input without first validating that the user input is safe to use. The process of making sure that user input is safe is called "sanitizing" and is language-specific, meaning that sanitizing Java code is performed in a different manner than C#, for example.

  Injection attacks can lead to leaking sensitive or confidential data, running arbitrary code or even causing a DOS (denial-of-service) attack on an affected machine.

  There is no specific remediation for injection attacks, but it helpful to remember these key points when coding against such attacks:

- Use an API or library to sanitize user data
- **NEVER TRUST USER DATA - injection attacks occur largely because of bad data supplied by the user (explicitly or otherwise)**

- A08:2021 – Software and Data Integrity Failures[39]

  Just as user authentication is critical to software, so is validating data. This topic demonstrates the need for software to validate related software artifacts such as firmware updates, plugins and third party code (see section 9.2 for a detailed analysis of third party code).

  Consider a router which has updateable firmware (most routers support updateable firmware and it is common for the user to perform the firmware update). If the firmware is not cryptographically signed by the manufacturer AND also validated on the router before an upgrade, then bad actors may be able to distribute malicious firmware to unwitting users.

  Before looking at the next section - updating software - let's look at one more common blunder in the wild with authentication. While Steve Gibson talked about this on the March 22, 2022 episode of Security Now, reports of this issue surfaced all the way back in 2018.

Duo is a third-party multi-factor authentication software owned by Cisco and has some default configurations that are… problematic. Specifically, two default configurations led to a catastrophic breach:

- Allow for re-enrollment of a new device for dormant accounts
- ***Fail-open*** (we'll take a peek at that in just a minute)

At this point in this book, you are equipped with a robust understanding of hacks and vulnerabilities. This one is a wonderful example of chaining exploits together. Buckle your seatbelt[40].

Hackers use brute force to log in to a network using simple, predictable, or popular passwords. Some of these accounts are dormant but still exist.

Here's where the first default configuration issue comes into play. Duo's MFA is disabled since the account is old and not used. But since Duo's default configuration allows dormant accounts to enroll new devices, the bad actors are able to add a device to the MFA scheme.

This rudimentary network access isn't sufficient, so the bad actors introduce an privilege escalation vulnerability known as PrintNightmare (this is an especially nasty bug that Windows tried fixing a few times and, well, could just not get it right[41]).

Once the bad actors were able to gain administrator access, they went in and *modified the hosts file!* Yes. You read that right. DNS poisoning at the source! They altered the IP address for Duo's authentication servers to be localhost.

This move prevented authentication validation (since the computer couldn't access Duo) and exploited the second default configuration - fail-open. When systems fail-closed that means it shuts down. From a security standpoint, that's great. But from a convenience standpoint, it is annoying. Oddly Duo's MFA default configuration is to fail-open - that means "the system remains 'open' and operations continue as if the system were not even in place[42]". With this as the behavior for the device when connecting to VPN, the bad actors were able to connect to the Windows Domain Controller with Remote Desktop Protocol.

Game over.

Note that Duo *does* allow users to fix this issue. At the time of installation, these configurations can be changed. However, once the installation happens, the only way to change these settings is to change the key in the registry[43] (which requires administrator privilege and specialized knowledge).

33. What is a CVE?
34. Gmail "dots don"t matter" feature exposes Netflix users to phishing attacks
35. A02:2021 – Cryptographic Failures
36. A04:2021 – Insecure Design
37. A07:2021 – Identification and Authentication Failures
38. A03:2021 – Injection
39. A08:2021 – Software and Data Integrity Failures
40. FBI Warns that Hackers Gain Network Access by Exploiting MFA and "PrintNightmare" Vulnerability
41. Microsoft adds second CVE for PrintNightmare remote code execution
42. Fail Closed, Fail Open, Fail Safe and Failover: ABCs of Network Visibility
43. Duo Authentication for Windows Logon and RDP - FAQ

11.5 Updating Software

Software is constantly evolving. This has always held true; new features are added, bugs are fixed and security vulnerabilities are patched. Today it is quite common for software to update automatically. To wit, major operating systems such as Windows and MacOS will suggest updates but can ultimately force updates. The same holds true for most mobile phones, as well. This was not always the case! Older software did not have the means to auto-update as the infrastructure required includes a network (the Internet in most cases) and one or more servers to host the updated files. The Internet was terribly pervasive at the turn of the century and auto-updating software was only starting to enter the mainstream.

It Is On You!

It is on you, as a user, to be sure that you have everything up to date. This includes firmware for your hardware, operating systems and any installed applications. This can be a heavy lift for anyone involved in IT but even more so for someone who is not an IT expert. Perhaps this is one of the reasons that auto-updating software has become so popular.

WinRAR

WinRar has been one of the most popular archiving programs for nearly 20 years, weighing in at over one billion downloads.

Steve Gibson talks about a vulnerability in WinRAR back in 2019. Mr. Gibson correctly points out that the vulnerability permits attackers both *persistence* as well as *code execution* - and refers to the combination as the "the two golden things you want[44]".

Compounding the issue is that there is no auto-update functionality, meaning that only users who actively update their install of WinRAR will receive the security patch.

44. Security Now! Transcript of Episode #708

11.6 Deployed Applications and Web Applications

Subtopic

Software security does not stop at the time the software is shipped! Particularly in cases where the software is a web application and the software is used constantly by users all over the world. Additionally, web applications are accessible from nearly anyone in the world, making them a target for attacks.

This chapter focuses on software as it is being designed and developed, but a quick look into the last 3 of the OWASP Top 10 rounds out the chapter.

A05:2021-Security Misconfiguration

Misconfigured software happens frequently; most of the time the consequences are not large but sometimes sensitive data may be leaked.

Stack Traces

A "stack trace" describes where in the code an error occurred. So called "stack traces" are helpful when developing code and debugging failures. However, stack trace data can sometimes contain sensitive or proprietary information. As such, a stack trace should never be displayed to a user. The image below indicates an actual stack trace from a web application.

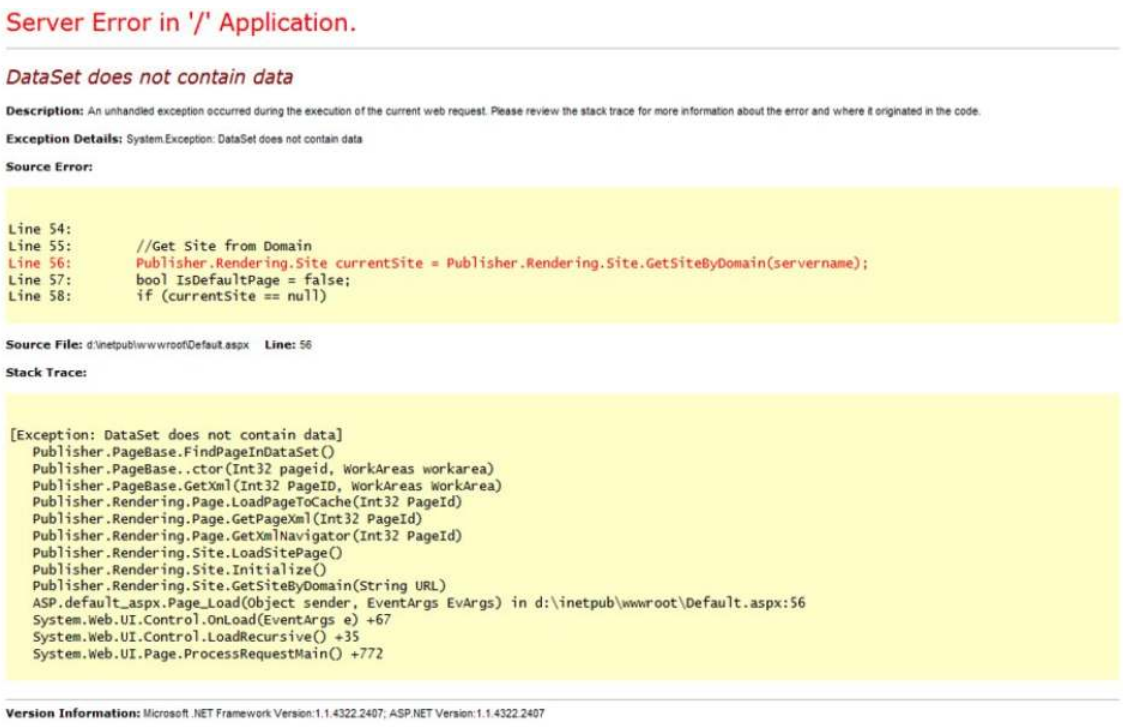


Figure 1: Server Error in web application (CC-BY-SA)

Note that the stack trace suggests some very useful information for a hacker. In particular, consider:

- A fully qualified directory name exists - this might be useful for a path traversal attack
- The "GetSiteByDomain(servername)" function suggests that perhaps other sites use this software; maybe an nslookup or whois would lead to other sites which can be compromised

Be sure to look at the OWASP45 page for more details.

A09:2021–Security Logging and Monitoring Failures

This refers to two separate but related concepts:

- Security Logging - persisting an audit trail such that details of how a breach occurred are available after the fact in order to provide evidence
- Monitoring - observing user behavior, often by referencing logs and audit trails, in real time or close to real time

Security logging is useful in order to keep a record of what is happening at any point in time within the system. Logging alone will not prevent an attack, but it will make it easier to figure out what happened.

Conversely, monitoring the system (and often the security logs) is a way to identify attacks in real time or discover that an attack occurred after the fact. With the rise of artificial intelligence or machine learning, coupled with the sharp rise in cyber attacks and ransomware attacks, real time monitoring is becoming a big market for software vendors.

Be sure to look at the OWASP page[46] for more details.

A10:2021–Server-Side Request Forgery (SSRF)

Rounding out the OWASP Top 10 is server side request forgery[47]. As web browsers become more advanced and security aware, SSRF attacks are not as commonplace as they once were.

Bank Example

To better understand this scenario, follow this example:

1. A user logs into their online bank using a web browser
2. The user does not log out, but navigates to a malicious page
3. The malicious page can, behind the scenes, send a request to the users bank in order to transfer money from the users account into the attackers bank account

This happens because the attacker is able to take advantage of the way web browsers work. In particular, any cookie associated with a website is sent with each request to that site. Additionally, session information is often stored in a cookie. That means that any request from a web browser to a specific web site will result in the cookie being sent, regardless of who told the browser to send the request. All the attacker needs to do is:

1. Hope that a user is logged into a bank website (https://www.myinsecurebank.com)
2. Convince the user to visit the a malicious site (https://www.mymaliciouswebsite.com)
3. The malicious site can use JavaScript in order to send a request *from the user's browser* to the user's bank website (https://www.myinsecurebank.com) in order to transfer funds

From the bank website's perspective, nothing is amiss as the user has valid cookies and valid session information. From the user's perspective, there is no visual indicator that any attack happened and the attack will go unnoticed until the user checks their balance at some point later.

Server-Side Request Forgery is a collection of techniques to prevent attacks of this nature. Mitigation tactics can be found on the OWASP page[48] for this vulnerability.

---

45. A05:2021 – Security Misconfiguration
46. A09:2021 – Security Logging and Monitoring Failures
47. A10:2021 – Server-Side Request Forgery (SSRF)
48. A10:2021 – Server-Side Request Forgery (SSRF)

11.7 Common Programming Errors

The following issues are common in programming (but are out of scope for this class). Be on the lookout for the following:

- Race Conditions>
- Type Errors
- Use After Free
- Cross-Origin Resource Sharing

CHAPTER OVERVIEW

12: Malware, Viruses & Other Threats

12.1 Introduction to Malware

"Viruses have no morality, no sense of good and evil, the deserving or the undeserving...."
Chris Crutcher, King of the Mild Frontier: An Ill-Advised Autobiography

Figure 1: A comic from XKCD, a popular techy-nerdy comic strip. (CC BY-NC 2.5)

After studying this section you should be able to do the following:

1. Identify the history of viruses
2. Educate others on how to protect themselves from malware

What is Malware?

Malware is an umbrella of malicious software designed to disrupt the user or damage the user's files. Malware has been around for almost as long as networks. Generally speaking, there are three main categories of malware: viruses, worms, and trojans (we will look at some other flavors of malware later in this chapter).

One of the more popular malware threats today is ransomware (malware that will find files on a victim's computer and encrypt them--the only way to rescue the files is to pay money to the attackers). Ransomware is a growing threat that has catapulted in popularity in the past few years.

On May 12 of 2017, a ransomware worm named WannaCry was taking over computers--literally thousands every minute. Two researchers in the UK (working for a cybersecurity firm in Los Angeles) stumbled across an odd feature in WannaCry; it looked like they had found a kill switch. Maybe. They didn't know. But they probably couldn't make the WannaCry pandemic worse. So they tried.

After reverse engineering the code, it appeared that WannaCry would look at a particular domain name and if it wasn't registered, WannaCry would infect. And spread. And infect. In a frenzied effort, one of the researchers (Marcus Hutchins, aka @MalwareTech) bought the domain name and registered it as his own.

Surprisingly, this stopped WannaCry dead in it's tracks. But the fight was just beginning. The architects of WannaCry (who had actually based it on code stolen from the NSA--DoublePulsar and EternalBlue) then launched a botnet attack, Mirai, on Hutchins.

The story is spectacular, and you can read about it in a wonderful article at TechCrunch. More recently, Wired magazine wrote a phenomenal piece about Marcus.

There are a few lessons to be learned (and questions that still haven't been answered) that first surfaced in the years since. Why did it infect 200,000 machines in the blink of an eye? Microsoft had released the vulnerability patch that would have prevented WannaCry from infecting a computer two months prior. It turns out that many systems did not update their patches. That's a hard lesson for users (although at the time, the price to decrypt your files was a paltry $300; as of August 2019, the average price is $13,000). Why did the worm stop when Hutchins registered the domain name? No one knows for sure, but a theory is that the authors of the malware thought that if they put in a random domain name in the code, and security analysts pinged the domain, that

would be a signal to the worm that it was being investigated--probably in a sandbox--so it should go dormant to avoid detection. Unwittingly, Hutchins may have made the entire world into a sandbox! Two years later, Hutchins has reported that *in* June of 2019 alone, his kill switch has prevented 60 million ransomware detonations!

Figure 1: For further investigation, you should check out Episode 44 of the Darknet Diaries podcast. Host Jack Rhysider talks to some people behind the curtain in the shadowy ransomware world. (Copyright 2022; Jack Rhysider)

The First Virus

Before the internet, the ARPANET (a creation from the Defense Department) ruled communication between clients. As an experiment, a simple program replicated itself across hosts on the network and displayed the message:

I'm the creeper, catch me if you can!

This minor inconvenience was given the name *Creeper* and was the first documented virus. Happily the first anti-virus, *Reaper*, was designed to seek out Creeper and destroy it. But it's not always that simple (in fact, most of the time, viruses require much more complex intervention).

Since then, viruses have evolved to be remarkably more sophisticated and diabolically more damaging. But not everyone hates viruses--there is actually a Malware Museum online (it's actually worth a visit to see what was happening in the sector of cybersecurity in the 1980s and 1990s). Additionally, in May of 2019, a computer was sold for $1.3 million dollars. The catch? The computer was sold as an art installation that represented digital threats. It actually had six pieces of malware carefully curated on it (including WannaCry!).

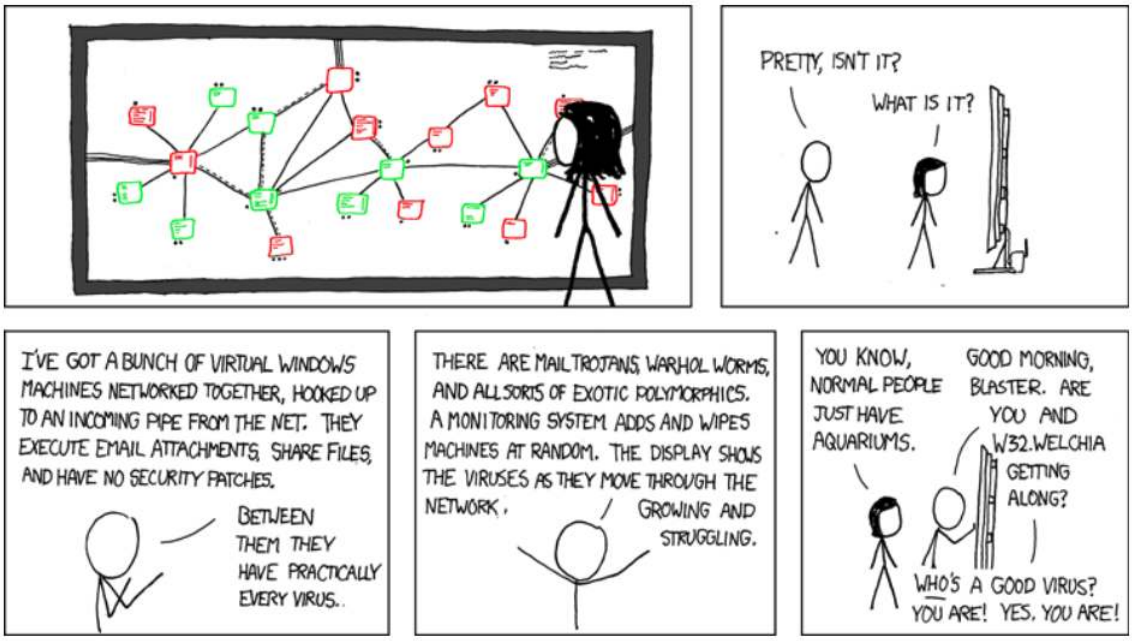


Figure 1: A comic from XKCD, a popular techy-nerdy comic strip. (CC-BY-NC-2.5)

12.2 Viruses and Threats

After studying this section you should be able to do the following:

1. Identify core characteristics of the three major types of malware

Virus

Definition

A computer virus is a piece of code, generally malicious in nature, that is intended to “infect” a computer. Once it has infected a host machine, it may potentially spread itself. The term virus is often used generically, as a reference to any manner of malicious code that may impact (albeit unknowingly) a user’s experience. They can remain hidden, pose minor inconveniences (such as repeated pop-ups), or even replicate to the point of making a computer unbootable.

Examples

One great example is the ILOVEYOU virus from 2000. Once a user has clicked on an infected attachment (using social engineering as a love confession scam), the virus then automatically sends itself as an attachment to other users. After that, the virus then replicates itself to overwrite other files on the host machine eventually making the machine unable to boot. It was estimated to reach 45 million people in a single day, and caused upwards of $15 billion in damages.

Another good example, and of a virus incredibly hard to kill off, is Conficker, also known as Downad. Even 10 years after its debut, it still routinely infects millions of computers worldwide. The primary reason it remains such a threat is because so many machines are still running on out of date software/patching. It spreads itself using methods and protocols that have since been patched and fixed, but as long as people continue to let their systems stay out of date, Conficker will continue to be a prevalent threat. Even though it was not created to generate revenue for criminals (such as with ransomware), it still aims to infect as many machines as it can simply for notoriety. There is nothing to say that its methods couldn’t also be used to deliver other more malicious payloads as well.

How to Protect Yourself

There are many things one can do to help protect their devices from being infected by a virus. The only guaranteed way of preventing a virus is to completely isolate the machine from the rest of the world (no access to the Internet, other computers, flash drives, or any other source of a virus - also called **air gapped**). In today’s world, this practically defeats the purpose of having a computer, but the trick is to reduce the likelihood of being exposed.

- Install Anti-virus software. Windows 10 comes with Windows Defender for free,
- which recent studies have shown to be very effective - even more so than some of the paid products.
- Keep operating systems, web browsers, and other applications up to date with the latest patches.
- Never plug in unknown media from an unknown source, this includes things like flash drives and DVDs.
- Never click on ads, *ever.* If you see an ad for something you are interested in, do a web search in a trusted search engine or go directly to the retailer’s website. This would include things known as “clickbait” where a headline for a web link may be written in such a way to tempt you to visit in order to read more.
- Don’t download software you aren’t explicitly sure is safe, or from sources that aren’t trustworthy. Be especially wary of Peer-to-Peer (P2P) sites that allow downloading of pirated software through methods such as BitTorrent. Even legal software through these methods may be infected. To mitigate your risk, you should also verify the hash of software.
- Practice good email habits - don’t click on attachments that you aren’t 100% sure of the source and intention.
- Keep important files backed up to another location that is isolated, such as an external hard drive dedicated to backups that is not kept connected when not in use.
- Be wary of anything that wants to transact in digital currency such as BitCoin. It’s often a clue that an entity wants to cover their tracks, and usually for no good reason.

Odds are incredibly high that every person will have to deal with a virus at least once, if not numerous times. When that happens, it is a good idea to run a scan using your anti-virus software. There are also some free tools from reputable anti-virus companies that can be used to scan if you do not have an anti-virus application installed. In worst case scenarios, the best thing that can be done is to wipe the device clean with a fresh install of the factory image or operating system. This provides the highest likelihood of completely eliminating the virus.

Trojans

Definition

Trojans are malicious malware that attempt to disguise themselves as a safe or familiar program, software, or file. This is to deceive the user from the true intent of the malware which could be almost anything. They are named Trojans based on the Greek Trojan Horse story where the army hid in a horse in order to deceive the town as a peace offering or gift, then proceed to gain entrance into the city undetected.

Examples

Trojan horse malware comes in many different types based on the task it is needed for. One common Trojan horse malware is the Backdoor Trojan that when used by a hacker and successfully placed and masked on a computer, grants access and control of the computer to the hacker. The worst part is that this Trojan or other malware can be downloaded by a different type of Trojan. The Downloader Trojan targets affected computers then proceeds to download new versions of the Trojan or more malware, adware, and trojans. These are only the tipping point of a vast sea of Trojan horse malwares equipped for any purpose and want.

The plethora of Trojans makes circulation of malware easy and with the boom of coin-mining one particular Trojan would gain traction and attention. The Rakhni Trojan is a malware that has been around since 2013 and is used to take a computer and use it as a means of mining. This Trojan as people may feel their computer slow down but not realize that it is the innocent looking app that is using the computer to generate wealth.

How to Protect Yourself

With the serious nature of these trojans, it makes sense to take the best course of action in protecting one’s device from suffering from a Trojan. First, you should make sure all security software is up to date, then make sure you have and are using a firewall and antivirus service with a good reputation. Even if they have a good reputation, this still does not mean you should go clicking on every link in an email, or go to every ad popup and website. You should also make sure your passwords are hard to crack.

Worms

Definition

Worms are malware that are self replicating, which helps it remain active on devices that has already infected while using that network to infect more devices. Each copy can also make copies of itself, which causes these infections to spread quickly from device to device. Since worms are self-replicating they don’t need human interaction in order to spread, this is another reason why they’re considered more aggressive and contagious than a regular virus. Keep an eye on hard drive space, performance and if there are any missing or new files, Worms will eat up hard drive space and slow down your device. They also delete or replace files.

Examples

MyDoom, a computer worm that affected Windows computers, first sighted in January 26 , 2004. It’s an email worm that was the fastest spreading worm that had exceeded Sobig worm and ILOVEYOU. The email that contain MyDoom had a typical error message and if the recipient were to click on the attachment then the worm would then resend itself to the addresses in the user’s address book of their email. Although the author of the virus is unknown, some researchers believe that it originated in Russia. The original worm had two triggers, one was to begin a DDoS attack on Feb. 1 and the second was for it to stop on

Feb. 12. However the backdoors that it created in the operating system would remain open. The second attack a year later started a DDoS attack on certain search engines. There was also a MyDoomB that blocked Microsoft websites and antivirus sites by modifying host files, this blocked removal tools from antivirus sites.

MyLife is another email based worm that affected Microsoft Outlook in the same manner as MyDoom. By replicating and sending itself to users in the address book. MyLife would download itself into a system file, later varients it would display an image as it did this. The worm will go in to check the time and if it's greater than :45 then it will start deleting system files. These files included: .sys and .com files in the C:\ root folder, all .com, .sys, .ini, and .exe in the Windows folder and .sys, .vxd, .exe, and .dll files in the System folder.

How to Protect Yourself

Updating the devices' latest updates for operating systems and applications since worms take advantage of software vulnerabilities.

Phishing is also a way that worms can infect a computer by downloading or clicking links that come from untrustworthy sources. Always check links and downloads before clicking.

Anti-virus software that includes phishing protection along with protection against other online threat is also recommended.

If your device happens to get infected by a worm, disconnect from the internet to prevent the spread of the worm and damage. Scan your computer to see if your antivirus software can remove the worm if it can't remove the problem then you might have to reinstall your operating system. Reinstalling the operating system removes all the files and any additional software you may have on your computer. Once reinstalling your operating system it's best to go through and install any patches to fix the vulnerabilities that the worm used to get onto your device in the first place.

12.3 Other Malware

Learning Objectives

After studying this section you should be able to do the following:

1. Describe different types of malware
2. Provide examples of different types of malware
3. Explain how to protect users from malware

Adware

Definition

Programs that are installed without the users knowledge that display unsolicited ads.

Examples

One type of adware that is commonly encountered is in the form of a "**browser hijacker**". These are cleverly hidden into a bundle of free software that the user decides to download. Before the user even knows what happened their browser is injected with countless ads that impede the ability to surf the web seamlessly.

Another example is Gator which was a form of adware that was prevalent years ago that is no longer active today. This malware also had it's claws into the ads that the user would see when browsing. What Gator did was replace ads that were on websites already with their own ads. This was even more deceptive since it didn't seem like you were getting bombarded with ads, they just knew how to hide in plain sight.

How to Protect Yourself

The easiest way to protect yourself is to get antivirus software. Anything that gives your machine a better hand when dealing with malicious software. Having the knowledge on what you might be downloading is also key. Low effort attempts to gain access to your PC can often be spotted just by looking at it. Taking the time to understand how they are trying to put malware on your computer is the best advice one can give - along with giving the names of some trusted antivirus software.

Backdoors

Definition

Write the definition, in your own words, here.

Examples

Provide at least two examples here. Paint a picture. Give a nice story. This can be technical, but really you're telling a story here. Help future readers get in to what you are talking about.

How to Protect Yourself

What are some strategies that people can do to protect themselves? What are things people can do if they've already been infected?

Bots & Botnets

(Julia Struble)

Definition

A botnet is a network of remotely controlled internet devices, utilized to accomplish some goal of the attacker. A bot is an individual device that is being controlled. The devices are typically brought under the control of the attacker via malware, and are then used for tasks that require a large number of devices, such as a DDoS attack, or Bitcoin mining.

Examples

A botnet is kind of like a horde of zombie computers, under the control of the head necromancer. Above is a *very realistic* depiction of a botnet that I drew.

The first botnet to gain notoriety was a spammer from the year 2000. Mr. Khan Smith used a botnet to send 1.25 **million** emails in about one year. These e-mails were all phishing scams. Phishing scams like these use the logic that if they send enough emails, odds are somebody will fall for it (i.e. law of large numbers).

Another example was the 2007 "Storm". This botnet was notable because it was one of the first to be controlled by several different servers. This network ranged from 250,000 to one million infected computers. This network was available for rent on the dark web, for anyone to use for whatever reason.

How to Protect Yourself

Botnets work by infecting a large number of devices, and then carrying out their tasks in the background, unbeknownst to the user. A large number of computers are already infected with botnet malware, often via a trojan horse. Therefore, the steps you need to take to protect yourself from becoming an infected botnet computer are the same steps you take to avoid viruses and malware in general. Run regular anti-virus scans, avoid suspicious email attachments, and keep your software updated.

Keylogger

Definition

Usually software, but sometimes hardware, a keylogger records a user's direct input into their keyboard for later retrieval or transmission. Keyloggers easily go undetected and the software itself is legal, even if it can be used for malicious purposes.

Example

It's time to pay your credit card bill for the month. You open your web browser and input the URL for your credit card company. You login, pay your bill, logout, and go about your day.

Next month when you go to pay your bill, you notice a lot of activity that you don't recognize. You haven't lost your card? So what happened?

Well you hadn't renewed your security software subscription, so when you torrented the nominations for Best Picture you unwittingly downloaded a keylogger. When you typed your username and password (right after typing the website of a major credit card company) you left the door to the vault wide open, and rolled out the red carpet.

That doesn't worry you?

Well you also let your friend Kyle check his Facebook on your computer, which meant that you had to sign back in.

You just got an email with some screenshots of a very embarrassing conversation with a coworker (Kyle no less) containing some language that may threaten your continued employment. Now the keylogger has been leveraged to access information that can be used to extort ransom.

How to Protect Yourself

Keep your security software up to date! Take this story from 2005:

"In February 2005, Joe Lopez, a businessman from Florida, filed a suit against Bank of America after unknown hackers stole $90,000 from his Bank of America account. The money had been transferred to Latvia.

An investigation showed that Mr. Lopez's computer was infected with a malicious program, Backdoor.Coreflood, which records every keystroke and sends this information to malicious users via the Internet. This is how the hackers got hold of Joe Lopez's user name and password, since Mr. Lopez often used the Internet to manage his Bank of America account.

However the court did not rule in favor of the plaintiff, saying that Mr. Lopez had neglected to take basic precautions when managing his bank account on the Internet: a signature for the malicious code that was found on his system had been added to nearly all antivirus product databases back in 2003."

Using a token generator or two-factor-verification when signing in to sensitive accounts are other good options to limit your risk of falling victim to a maliciously deployed keylogger.

Logic Bombs

Definition

A logic bomb is a piece of code injected into existing software and lies dormant until it is executed by a specific programmed event; causing a malicious action to occur on a computer network. There are two types of triggers to cause the payload -- a positive trigger and a negative trigger. A positive trigger is when a preprogrammed event occurs, such as reaching a specific date. The negative trigger runs the malicious code when an action is NOT taken, such as a user failing to input data by a certain time. Like a bomb, this attack usually destroys data by wiping hard drives, deleting files, clearing a database, etc. Logic bombs are commonly used in the context of a company whose attacker an inside worker with knowledge and access to sensitive information. However, logic bombs have become a part of many hacker's toolkits and can be used in a multitude of ways. This could include embedding a logic bomb in a fake program (like a Trojan) to damage a victim's PC or using a logic bomb in a spyware program to run a keylogger when a user visits a certain website to log in.

Examples

One particularly devastating case of a logic-bomb-based attack dates back to March 20 in 2013 when the hard drives and master boot records of bank-owned computers in South Korea were wiped of their data. Once a programmed date and time passed, the bomb used a file called AgentBase.exe to destroy data6. Cyber security experts believe the malicious files were introduced onto the targeted networks via a phishing email loaded with a Trojan6. The outcome took down not only computers but also ATMs thus halting banking operations.

More recently on December 17 in 2016, a logic bomb that infected Ukraine's electric grid via a backdoor turned off power to regions of the country at predetermined times. What is more frightening is when operators attempted to regain access to the grid, the malware would override their actions to continue disabling power while also deleting files on the operator machines. The operators had little choice but to manually operate the power grid due to the damage caused by the logic bomb8. This infrastructure targeted attack is now known as "Industroyer" and, rather than damaging a select company, impacted an entire nation of people.

How to Protect Yourself

Part of the logic bomb's notoriety is the difficulty of detecting one using traditional antivirus7. While antivirus may not be able to detect special logic bomb signatures, they should still be regularly updated since logic bombs are often coupled with other types of malware.

For companies, prevention and damage minimization should focus on inside workers. Employees should only have as many rights/privileges on a system that they need to perform their job. Companies should also make employees aware of phishing emails as they can introduce malware loaded with logic bombs into the system.

Monitoring systems for suspicious, unexpected changes could prevent a logic bomb from going off7. This piece of advice is highly recommended for industrial organizations, such as Ukraine's power grid, who would rarely make changes to their systems. The sooner a system is routinely monitored and/or audited the better in the case of a logic bomb already lying dormant in the system.

For any system, industrial or private, backing up information is an essential process to remain secure. This way, if a logic bomb delivered a damaging payload, the information would still remain intact elsewhere and systems would have a chance at being restored.

RAT

Definition

Short for Remote Access Trojan; a malware program that provides a backdoor into a computer system allowing an intruder or hacker unlimited, anonymous administrative control over the infected computer without the user's knowledge. RATs allow for viewing and modifying user's files and functions in the system, monitoring and recording user activity, and using the victim's system to attack other systems. RATs are manually controlled and can easily hide as ghost entities in the system for years if left undetected.

Examples

RAT infection takes place by directing the user to install an invisible modified file either piggybacked on a user-requested program, such as a video game, or through email attachments, unsafe website popup, accepted cookies, or social engineering attacks using deceivingly look-alike advertisements. Upon execution of the trojan, an intruder is able to secretly access any information the user can. Online banking credentials, application passwords, account passwords, hardware, system structure and any features installed on the targeted system are highly sought after prizes.

The simplest example of an attack that RATs can perform is the ability to activate infected computers webcam and microphone devices anytime the device is on and connected to the internet. Hackers can discreetly view, record or listen to conversations and/or activities occurring within range of the infected computer. A larger scale example would be Intelligence agencies and activist groups use RATs for specific purposes like blackmailing or espionage.

How to Protect Yourself

For basic protection; RATs can easily be avoided by simply enabling Windows Defender Antivirus Software included on Windows 10. For additional protection, Malwarebytes Anti-Malware has an extensive database of well known RATs commonly used by lazy hackers. Always download games, files or software from secure websites. Always use updated browsers which prevent automatic downloads from websites and notify you when a site is unsafe. Most importantly, keep your Operating System up-to-date with security patches and properly shut down your system when not in use.

Rootkit

Definition

A malicious software designed to provide ongoing access to a computer with likely elevated privileges (administrator) in the system.

Examples

Rootkits have many forms, generally speaking these come in many forms. Once a system is infected, in many cases they can be the most difficult forms of malware to remove. Registry rootkits may involve changing the actual registry itself. With personal limited experience and hours of working on a singular rootkit, the program had duplicated itself multiple times and with different names each time. In order to remove the program all processes had to be stopped as well as all instances running.

How to Protect Yourself

The chance of a rootkit infection can be drastically reduced by following basic security advice, keep firmware up to date, do not open emails from unknown sources, keep an updated anti-virus, only obtain programs from legitimate and trustworthy sources.

Phishing

Definition

A crime in which someone posing as a legitimate or credible source tries to steal information or money from unsuspecting individuals, typically by email, fake websites, texts, or phone calls. Phishing scams are usually based on quantity not quality (though spearphishing is based on quality, not quantity).

Examples

This example is so old I don’t even know if it is used anymore but it was a classic back when the internet was pretty new. The classic email scam, that I definitely thought was real at one point, was a Nigerian prince was trying to get his gold or other goods out of the country but didn't have the money to do so. They needed you the unsuspecting fool to send a few thousand dollars to allow them to get the goods out of the country, which they would then not only pay you back with but also reward you handsomely. I recently have heard that this one has been making the rounds again, but it is “military” trying to get gold bars out of the Middle East after raiding one of the many palaces. A poor lady was scammed out of $13,000.

Another one that was very common before things were easier to check on, was when you would get a call from a person that, for example, your son had been arrested and the bail was $5,000 and needed immediately. Before the call they would gather minimal information. Things like you have a 19 year old son named Michael. That was enough. The call would be placed. Then they would

hit you with the fact that you need to send it via Western Union. For whatever reason they were always involved in any request for scam money transfers. I think that funds could basically be sent and received almost anonymously, which is why it was used.

How to Protect Yourself

- Visit websites directly.
- Check welfare of family before sending money.
- Scrutinize things or requests from unsolicited sources.
- Do not open attachments from unknown sources.
- Use an SSL certificate to secure all traffic to and from your website.

Ransomware

Definition

A type of malware which locks down a computer system or access to data until a ransom is paid, usually spread via phishing emails or visiting an infected website, once its infected one system, it becomes exponentially more infectious by infecting all connected systems, until its claimed a large amount of software and hardware.

Examples

Provide at least two examples here. Paint a picture. Give a nice story. This can be technical, but really you're telling a story here. Help future readers get in to what you are talking about.

How to Protect Yourself

What are some strategies that people can do to protect themselves? What are things people can do if they've already been infected?

Spear Phishing

Definition

A targeted attack where the hackers use information they discovered online about a user to prompt them to click an email link or provide more sensitive information about themselves. They do this by posing as trusted companies to trick users into believing the emails are real. These attacks are more dangerous than random phishing attacks because they mask malicious intent behind seemingly real sources.

Examples

Let's say you lost your wallet and posted about it on social media. A hacker who learns about your post could assume that you have paused or locked your bank cards. In this scenario, a spear phishing account could include an email prompt to sign into your online banking account to confirm the lock on your bank card within 24 hours or your account will be closed. These types of attacks always seem to have an urgent motivator attached to them. But when you sign in you're actually giving your login credentials to the hacker.

Another scenario could be an email that seems to be from the company you use for cloud storage. The email lets you know your storage is full and that file management is needed immediately to keep your account open. The email then has a link or a button that you think will lead you to the cloud storage site, but it really takes you to a dangerous site instead.

How to Protect Yourself

It can be really hard to discern verifiable emails from spear phishing attacks. So it is important to do your due diligence before entering any information, clicking links, or permitting access to your accounts.

How to prevent being a victim

- **Verify the information** in the email through the actual web page of the service instead of clicking the link provided.
- **Preview the address** of links before you click on them by hovering over the link. This will allow you to check the address you'll go to before potentially compromising your information.

- **Avoid posting** personal information online! Your followers could potentially use that information against you.

Spyware

(Stephan Bonzo)

Definition

Software that allows the user to covertly get information of another computer's activities by transferring data from their hard drive.

Examples

Let’s look at a couple of examples. Keep in mind that there are more types than the ones I am going to explain.

Info Stealers

In most cases, Info Stealers exploit browser related security deficiencies to steal your data. Sometimes they will even input extra fields into web forms, so that when the user fills out those fields, they will then instead be sent to the hacker instead of the website owner.

Keyloggers

Sometimes referred to as system monitors, these programs aim to record keystrokes of a connected keyboard on the infected device. The goal here is to record the strokes on the keyboard in real time, or take a screenshot every few seconds of the screen. This will allow the Hacker to record passwords, credit card details, emails, and even browsing data.

This is a program that has the ability to scan an infected computer and steal a wide variety of information. Typically this is browsing data, passwords, email, usernames, personal documents, and even media files. Depending on the type of Info Stealer, they will either store the info they collect on a remote server, or keep it local to grab at another time.

Although they are mainly used by hackers, they have managed to also become practical use in normal business practices. This will allow managers to keep tabs on their employees activity while at work. Parents might also install a keylogger on their child's hardware to see what they have been up to.

How to Protect Yourself

The best thing you can do to protect yourself is to not just go ham and click everything you see on the internet. Do a quick bit of research and make sure that everything seems as it is with every site you go to. Don’t click suspicious links, or download suspicious files. If at any time you start noticing things being weird or out of order with your hardware, run some sort of anti-virus to just be safe.

(Jaiden Hernandez)

Definition

Spyware (as the definition implies) is malicious software that is installed on your computer in order to ‘spy’ on the victim. This includes collection of valuable information such as emails, passwords, and even credit card information. Spyware can come in many forms, such as an internet cookie, adware, keyloggers and more. Spyware usually installs itself onto your computer without the user's knowledge.

Examples

Spyware has many examples that can be used, one notable example of spyware is accepting a popup, or allowing cookies on an unfamiliar website. These allow them to be installed without the knowledge of the user. Malware can also come in the form of an unsuspecting download, or ‘trojan’. This trojan has the ability to monitor computer activities in order to see what the user is doing and possibly collect the information to be used maliciously. An example of this software is Zlob , a trojan program in which it uses computer vulnerabilities to track keystrokes and record the browsing history of victims.

How to Protect Yourself

Because of the common occurrence of spyware on the internet it is pretty easy to remove it once it has been located. Modern day antivirus software is equipped with dealing with a plethora of different types of malicious malware, and there are many things to do

to help prevent it. Some things to do to protect yourself is to make sure you never click on any suspicious links, or pop-ups that may enable your browser to get a cookie hidden as spyware. Weekly scheduling of antivirus scans and keeping your computer drivers and software updated is another way to watch out for these vulnerabilities. There are patents even being filed to recover from these attacks.

12.4 Staying Safe

Learning Objectives

After studying this section you should be able to do the following:

1. Articulate ways to protect yourself and others from malware

- ## Staying Safe
- ### Updating Your OS (Operating System)
- (Shawn Newton)
- Operating system updates aren't usually for show, they are patching something that doesn't work or they are sent out in the attempt to protect users from flaws that can be exploited by those who want to get into or affect your system. For example Windows recently urged it's users to update their systems as soon as possible because of the fact that they had a glaring flaw that was exploitable.
- ### MalwareBytes
- Another smart way to protect yourself is by installing MalwareBytes, this program actively protects your computer in real time by pointing out sites you are attempting to visit as security threats before you visit them. Alongside that feature it also takes initiative in finding viruses and malware by using machine learning.
- ### Social Engineering
- Good ways to protect yourself from Social Engineering attacks like Phishing is to be blatantly suspicious of unsolicited communications from sources you are unsure of. Double-check the source of any email you are sent, especially if they are requesting sensitive data. Attempt to call the person back before transferring any information to avoid being the victim of a Spoofing attack.
- **Unknown File Downloads**
- Avoid downloading files you aren't completely sure about, double-check everything!
- **Safe Browsing**
- Other safe Browsing habits include most of what we've gone over alongside, not reusing passwords, keeping your browser up to date and not reusing the same password for everything.
- **Use Complex and Secure Passwords**
- The first step of maintaining a security and preventing from hacker getting into individuals computers is to have a strong, complex, and secure passwords. Hackers have a hard time with complex passwords because if the password consists of at least 8 characters with numbers, upper and lower case letters, and special characters then the chances of them getting into your personal information is extremely slim. There was a study done that showed if a password have 6 character with all lower case letters then it can be broken under 6 minutes.
- **Install Firewall**
- Firewall is a security guard that will protect your computer. "It creates a barrier between the computer and any unauthorized program trying to come in through the Internet."
- **Install Antivirus Software**
- Another way to protect your computer is by installing antivirus software. This software helps protect the computer from unauthorized software that is a threat. Virus, keyloggers, Trojans are some examples of unauthorized software. It also prevents future attacks of viruses too.

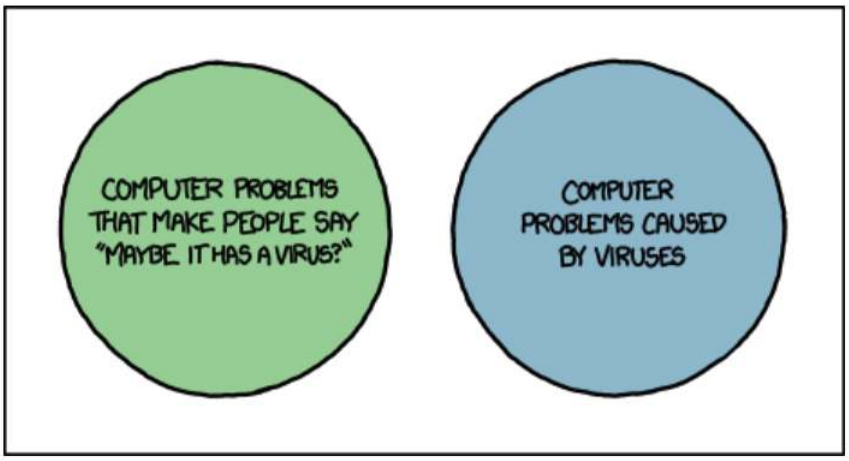


Figure 1: A comic from XKCD, a popular techy-nerdy comic strip. (CC BY-NC 2.5)

CHAPTER OVERVIEW

13: Application Security

CHAPTER OVERVIEW

14: Assessing Security

CHAPTER OVERVIEW

5: Cryptography

5.1: Introduction

Cryptography, or cryptology (from Ancient Greek: κρυπτός, romanized: kryptós "hidden, secret"; and γράφειν graphein, "to write", or -λογία -logia, "study", respectively

Cryptography prior to the modern age was effectively synonymous with encryption, converting readable information (plaintext) to unintelligible nonsense text (ciphertext), which can only be read by reversing the process (decryption). The sender of an encrypted (coded) message shares the decryption (decoding) technique only with intended recipients to preclude access from adversaries. The cryptography literature often uses the names "Alice" (or "A") for the sender, "Bob" (or "B") for the intended recipient, and "Eve" (or "E") for the eavesdropping adversary. Since the development of rotor cipher machines in World War I and the advent of computers in World War II, cryptography methods have become increasingly complex and their applications more varied.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in actual practice by any adversary. While it is theoretically possible to break into a well-designed system, it is infeasible in actual practice to do so. Such schemes, if well designed, are therefore termed "computationally secure"; theoretical advances (e.g., improvements in integer factorization algorithms) and faster computing technology require these designs to be continually reevaluated, and if necessary, adapted. Information-theoretically secure schemes that provably cannot be broken even with unlimited computing power, such as the one-time pad, are much more difficult to use in practice than the best theoretically breakable, but computationally secure, schemes.

The growth of cryptographic technology has raised a number of legal issues in the Information Age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.

Adapted from:

5.2: Terminology

The first use of the term "cryptograph" (as opposed to "cryptogram") dates back to the 19th century—originating from "The Gold-Bug," a story by Edgar Allan Poe.

Until modern times, cryptography referred almost exclusively to "encryption", which is the process of converting ordinary information (called plaintext) into an unintelligible form (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A cipher (or cypher) is a pair of algorithms that carry out the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a "key". The key is a secret (ideally known only to the communicants), usually a string of characters (ideally short so it can be remembered by the user), which is needed to decrypt the ciphertext. In formal mathematical terms, a "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms that correspond to each key. Keys are important both formally and in actual practice, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

There are two main types of cryptosystems: symmetric and asymmetric. In symmetric systems, the only ones known until the 1970s, the same secret key encrypts and decrypts a message. Data manipulation in symmetric systems is significantly faster than in asymmetric systems. Asymmetric systems use a "public key" to encrypt a message and a related "private key" to decrypt it. The advantage of asymmetric systems is that the public key can be freely published, allowing parties to establish secure communication without having a shared secret key. In practice, asymmetric systems are used to first exchange a secret key, and then secure communication proceeds via a more efficient symmetric system using that key. Insecure symmetric algorithms include children's language tangling schemes such as Pig Latin or other cant, and all historical cryptographic schemes, however seriously intended, prior to the invention of the one-time pad early in the 20th century.

In colloquial use, the term "code" is often used to mean any method of encryption or concealment of meaning. However, in cryptography, code has a more specific meaning: the replacement of a unit of plaintext (i.e., a meaningful word or phrase) with a code word (for example, "wallaby" replaces "attack at dawn"). A cypher, in contrast, is a scheme for changing or substituting an element below such a level (a letter, a syllable, or a pair of letters, etc.) in order to produce a cyphertext.

Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key normally required to do so; i.e., it is the study of how to "crack" encryption algorithms or their implementations.

Some use the terms "cryptography" and "cryptology" interchangeably in English, while others (including US military practice generally) use "cryptography" to refer specifically to the use and practice of cryptographic techniques and "cryptology" to refer to the combined study of cryptography and cryptanalysis. English is more flexible than several other languages in which "cryptology" (done by cryptologists) is always used in the second sense above. RFC 2828 advises that steganography is sometimes included in cryptology.

The study of characteristics of languages that have some application in cryptography or cryptology (e.g. frequency data, letter combinations, universal patterns, etc.) is called cryptolinguistics.

5.3: A Bit of History

Before the modern era, cryptography focused on message confidentiality (i.e., encryption)—conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message). Encryption attempted to ensure secrecy in communications, such as those of spies, military leaders, and diplomats. In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs and secure computation, among others.

Classic cryptography

The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message (e.g., 'hello world' becomes 'ehlol owrdl' in a trivially simple rearrangement scheme), and substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters (e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the Latin alphabet). Simple versions of either have never offered much confidentiality from enterprising opponents. An early substitution cipher was the Caesar cipher, in which each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet. Suetonius reports that Julius Caesar used it with a shift of three to communicate with his generals. Atbash is an example of an early Hebrew cipher. The earliest known use of cryptography is some carved ciphertext on stone in Egypt (ca 1900 BCE), but this may have been done for the amusement of literate observers rather than as a way of concealing information.

The Greeks of Classical times are said to have known of ciphers (e.g., the scytale transposition cipher claimed to have been used by the Spartan military). Steganography (i.e., hiding even the existence of a message so as to keep it confidential) was also first developed in ancient times. An early example, from Herodotus, was a message tattooed on a slave's shaved head and concealed under the regrown hair.[14] More modern examples of steganography include the use of invisible ink, microdots, and digital watermarks to conceal information.

In India, the 2000-year-old Kamasutra of Vātsyāyana speaks of two different kinds of ciphers called Kautiliyam and Mulavediya. In the Kautiliyam, the cipher letter substitutions are based on phonetic relations, such as vowels becoming consonants. In the Mulavediya, the cipher alphabet consists of pairing letters and using the reciprocal ones.

In Sassanid Persia, there were two secret scripts, according to the Muslim author Ibn al-Nadim: the šāh-dabīrīya (literally "King's script") which was used for official correspondence, and the rāz-saharīya which was used to communicate secret messages with other countries.

David Kahn notes in The Codebreakers that modern cryptology originated among the Arabs, the first people to systematically document cryptanalytic methods. Al-Khalil (717–786) wrote the Book of Cryptographic Messages, which contains the first use of permutations and combinations to list all possible Arabic words with and without vowels.[25]

Ciphertexts produced by a classical cipher (and some modern ciphers) will reveal statistical information about the plaintext, and that information can often be used to break the cipher. After the discovery of frequency analysis, perhaps by the Arab mathematician and polymath Al-Kindi (also known as Alkindus) in the 9th century, nearly all such ciphers could be broken by an informed attacker. Such classical ciphers still enjoy popularity today, though mostly as puzzles (see cryptogram). Al-Kindi wrote a book on cryptography entitled Risalah fi Istikhraj al-Mu'amma (Manuscript for the Deciphering Cryptographic Messages), which described the first known use of frequency analysis cryptanalysis techniques.[26][27]

Language letter frequencies may offer little help for some extended historical encryption techniques such as homophonic cipher that tend to flatten the frequency distribution. For those ciphers, language letter group (or n-gram) frequencies may provide an attack.

Essentially all ciphers remained vulnerable to cryptanalysis using the frequency analysis technique until the development of the polyalphabetic cipher, most clearly by Leon Battista Alberti around the year 1467, though there is some indication that it was already known to Al-Kindi. Alberti's innovation was to use different ciphers (i.e., substitution alphabets) for various parts of a message (perhaps for each successive plaintext letter at the limit). He also invented what was probably the first automatic cipher device, a wheel which implemented a partial realization of his invention. In the Vigenère cipher, a polyalphabetic cipher,

encryption uses a key word, which controls letter substitution depending on which letter of the key word is used. In the mid-19th century Charles Babbage showed that the Vigenère cipher was vulnerable to Kasiski examination, but this was first published about ten years later by Friedrich Kasiski.

Although frequency analysis can be a powerful and general technique against many ciphers, encryption has still often been effective in practice, as many a would-be cryptanalyst was unaware of the technique. Breaking a message without using frequency analysis essentially required knowledge of the cipher used and perhaps of the key involved, thus making espionage, bribery, burglary, defection, etc., more attractive approaches to the cryptanalytically uninformed. It was finally explicitly recognized in the 19th century that secrecy of a cipher's algorithm is not a sensible nor practical safeguard of message security; in fact, it was further realized that any adequate cryptographic scheme (including ciphers) should remain secure even if the adversary fully understands the cipher algorithm itself. Security of the key used should alone be sufficient for a good cipher to maintain confidentiality under an attack. This fundamental principle was first explicitly stated in 1883 by Auguste Kerckhoffs and is generally called Kerckhoffs's Principle; alternatively and more bluntly, it was restated by Claude Shannon, the inventor of information theory and the fundamentals of theoretical cryptography, as Shannon's Maxim—'the enemy knows the system'.

Different physical devices and aids have been used to assist with ciphers. One of the earliest may have been the scytale of ancient Greece, a rod supposedly used by the Spartans as an aid for a transposition cipher. In medieval times, other aids were invented such as the cipher grille, which was also used for a kind of steganography. With the invention of polyalphabetic ciphers came more sophisticated aids such as Alberti's own cipher disk, Johannes Trithemius' tabula recta scheme, and Thomas Jefferson's wheel cypher (not publicly known, and reinvented independently by Bazeries around 1900). Many mechanical encryption/decryption devices were invented early in the 20th century, and several patented, among them rotor machines—famously including the Enigma machine used by the German government and military from the late 1920s and during World War II. The ciphers implemented by better quality examples of these machine designs brought about a substantial increase in cryptanalytic difficulty after WWI.

Adapted from:

5.4: Computers and Cryptography

Early computer-era cryptography

Cryptanalysis of the new mechanical ciphering devices proved to be both difficult and laborious. In the United Kingdom, cryptanalytic efforts at Bletchley Park during WWII spurred the development of more efficient means for carrying out repetitious tasks, such as military code breaking (decryption). This culminated in the development of the Colossus, the world's first fully electronic, digital, programmable computer, which assisted in the decryption of ciphers generated by the German Army's Lorenz SZ40/42 machine.

Extensive open academic research into cryptography is relatively recent, beginning in the mid-1970s. In the early 1970s IBM personnel designed the Data Encryption Standard (DES) algorithm that became the first federal government cryptography standard in the United States. In 1976 Whitfield Diffie and Martin Hellman published the Diffie–Hellman key exchange algorithm. In 1977 the RSA algorithm was published in Martin Gardner's Scientific American column. Since then, cryptography has become a widely used tool in communications, computer networks, and computer security generally.

Some modern cryptographic techniques can only keep their keys secret if certain mathematical problems are intractable, such as the integer factorization or the discrete logarithm problems, so there are deep connections with abstract mathematics. There are very few cryptosystems that are proven to be unconditionally secure. The one-time pad is one, and was proven to be so by Claude Shannon. There are a few important algorithms that have been proven secure under certain assumptions. For example, the infeasibility of factoring extremely large integers is the basis for believing that RSA is secure, and some other systems, but even so, proof of unbreakability is unavailable since the underlying mathematical problem remains open. In practice, these are widely used, and are believed unbreakable in practice by most competent observers. There are systems similar to RSA, such as one by Michael O. Rabin that are provably secure provided factoring n = pq is impossible; it is quite unusable in practice. The discrete logarithm problem is the basis for believing some other cryptosystems are secure, and again, there are related, less practical systems that are provably secure relative to the solvability or insolvability discrete log problem.

As well as being aware of cryptographic history, cryptographic algorithm and system designers must also sensibly consider probable future developments while working on their designs. For instance, continuous improvements in computer processing power have increased the scope of brute-force attacks, so when specifying key lengths, the required key lengths are similarly advancing. The potential impact of quantum computing are already being considered by some cryptographic system designers developing post-quantum cryptography.[when?] The announced imminence of small implementations of these machines may be making the need for preemptive caution rather more than merely speculative.

Adapted from:
"Cryptography" by Multiple Authors, Wikipedia is licensed under CC BY-SA 3.0

5.5: Modern Cryptography

Symmetric-key cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.

Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs that have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted). Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access. Many other block ciphers have been designed and released, with considerable variation in quality. Many, even some designed by capable practitioners, have been thoroughly broken, such as FEAL.

Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output stream is created based on a hidden internal state that changes as the cipher operates. That internal state is initially set up using the secret key material. RC4 is a widely used stream cipher. Block ciphers can be used as stream ciphers by generating blocks of a keystream (in place of a Pseudorandom number generator) and applying an XOR operation to each bit of the plaintext with each bit of the keystream.

Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key can be used to authenticate the hash value upon receipt; this additional complication blocks an attack scheme against bare digest algorithms, and so has been thought worth the effort. Cryptographic hash functions are a third type of cryptographic algorithm. They take a message of any length as input, and output a short, fixed-length hash, which can be used in (for example) a digital signature. For good hash functions, an attacker cannot find two messages that produce the same hash. MD4 is a long-used hash function that is now broken; MD5, a strengthened variant of MD4, is also widely used but broken in practice. The US National Security Agency developed the Secure Hash Algorithm series of MD5-like hash functions: SHA-0 was a flawed algorithm that the agency withdrew; SHA-1 is widely deployed and more secure than MD5, but cryptanalysts have identified attacks against it; the SHA-2 family improves on SHA-1, but is vulnerable to clashes as of 2011; and the US standards authority thought it "prudent" from a security perspective to develop a new standard to "significantly improve the robustness of NIST's overall hash algorithm toolkit." Thus, a hash function design competition was meant to select a new U.S. national standard, to be called SHA-3, by 2012. The competition ended on October 2, 2012, when the NIST announced that Keccak would be the new SHA-3 hash algorithm. Unlike block and stream ciphers that are invertible, cryptographic hash functions produce a hashed output that cannot be used to retrieve the original input data. Cryptographic hash functions are used to verify the authenticity of data retrieved from an untrusted source or to add a layer of security.

Public-key cryptography

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, although a message or group of messages can have a different key than others. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps for each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all consistent and secret.

In a groundbreaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of public-key (also, more generally, called asymmetric key) cryptography in which two different but mathematically related keys are used—a public key and a private key. A public key system is so constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair. The historian David Kahn described public-key cryptography as "the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance".

In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the public key is used for encryption, while the private or secret key is used for decryption. While Diffie and Hellman could not find such a system, they showed that public-key cryptography was indeed possible by presenting the Diffie–Hellman key exchange protocol, a solution that is now widely used in secure communications to allow two parties to secretly agree on a shared encryption key. The X.509 standard defines the most commonly used format for public key certificates.

Diffie and Hellman's publication sparked widespread academic efforts in finding a practical public-key encryption system. This race was finally won in 1978 by Ronald Rivest, Adi Shamir, and Len Adleman, whose solution has since become known as the RSA algorithm.

The Diffie–Hellman and RSA algorithms, in addition to being the first publicly known examples of high-quality public-key algorithms, have been among the most widely used. Other asymmetric-key algorithms include the Cramer–Shoup cryptosystem, ElGamal encryption, and various elliptic curve techniques.[citation needed]

A document published in 1997 by the Government Communications Headquarters (GCHQ), a British intelligence organization, revealed that cryptographers at GCHQ had anticipated several academic developments. Reportedly, around 1970, James H. Ellis had conceived the principles of asymmetric key cryptography. In 1973, Clifford Cocks invented a solution that was very similar in design rationale to RSA. In 1974, Malcolm J. Williamson is claimed to have developed the Diffie–Hellman key exchange.

Public-key cryptography is also used for implementing digital signature schemes. A digital signature is reminiscent of an ordinary signature; they both have the characteristic of being easy for a user to produce, but difficult for anyone else to forge. Digital signatures can also be permanently tied to the content of the message being signed; they cannot then be 'moved' from one document to another, for any attempt will be detectable. In digital signature schemes, there are two algorithms: one for signing, in which a secret key is used to process the message (or a hash of the message, or both), and one for verification, in which the matching public key is used with the message to check the validity of the signature. RSA and DSA are two of the most popular digital signature schemes. Digital signatures are central to the operation of public key infrastructures and many network security schemes (e.g., SSL/TLS, many VPNs, etc.).

Public-key algorithms are most often based on the computational complexity of "hard" problems, often from number theory. For example, the hardness of RSA is related to the integer factorization problem, while Diffie–Hellman and DSA are related to the discrete logarithm problem. The security of elliptic curve cryptography is based on number theoretic problems involving elliptic curves. Because of the difficulty of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are commonly hybrid cryptosystems, in which a fast high-quality symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent with the message, but encrypted using a public-key algorithm. Similarly, hybrid signature schemes are often used, in which a cryptographic hash function is computed, and only the resulting hash is digitally signed.

Cryptographic Hash Functions

Cryptographic Hash Functions are cryptographic algorithms that are ways to generate and utilize specific keys to encrypt data for either symmetric or asymmetric encryption, and such functions may be viewed as keys themselves. They take a message of any length as input, and output a short, fixed-length hash, which can be used in (for example) a digital signature. For good hash functions, an attacker cannot find two messages that produce the same hash. MD4 is a long-used hash function that is now broken; MD5, a strengthened variant of MD4, is also widely used but broken in practice. The US National Security Agency developed the Secure Hash Algorithm series of MD5-like hash functions: SHA-0 was a flawed algorithm that the agency withdrew; SHA-1 is widely deployed and more secure than MD5, but cryptanalysts have identified attacks against it; the SHA-2 family improves on SHA-1, but is vulnerable to clashes as of 2011; and the US standards authority thought it "prudent" from a security perspective to develop a new standard to "significantly improve the robustness of NIST's overall hash algorithm toolkit." Thus, a hash function design competition was meant to select a new U.S. national standard, to be called SHA-3, by 2012. The competition ended on October 2, 2012, when the NIST announced that Keccak would be the new SHA-3 hash algorithm. Unlike block and stream ciphers that are invertible, cryptographic hash functions produce a hashed output that cannot be used to retrieve the original input data. Cryptographic hash functions are used to verify the authenticity of data retrieved from an untrusted source or to add a layer of

security.

Adapted from:
"Cryptography" by Multiple Authors, Wikipedia is licensed under CC BY-SA 3.0

5.6: Crytography and Legal Rights

Legal issues

Prohibitions

Cryptography has long been of interest to intelligence gathering and law enforcement agencies. Secret communications may be criminal or even treasonous[citation needed]. Because of its facilitation of privacy, and the diminution of privacy attendant on its prohibition, cryptography is also of considerable interest to civil rights supporters. Accordingly, there has been a history of controversial legal issues surrounding cryptography, especially since the advent of inexpensive computers has made widespread access to high-quality cryptography possible.

In some countries, even the domestic use of cryptography is, or has been, restricted. Until 1999, France significantly restricted the use of cryptography domestically, though it has since relaxed many of these rules. In China and Iran, a license is still required to use cryptography. Many countries have tight restrictions on the use of cryptography. Among the more restrictive are laws in Belarus, Kazakhstan, Mongolia, Pakistan, Singapore, Tunisia, and Vietnam.

In the United States, cryptography is legal for domestic use, but there has been much conflict over legal issues related to cryptography. One particularly important issue has been the export of cryptography and cryptographic software and hardware. Probably because of the importance of cryptanalysis in World War II and an expectation that cryptography would continue to be important for national security, many Western governments have, at some point, strictly regulated export of cryptography. After World War II, it was illegal in the US to sell or distribute encryption technology overseas; in fact, encryption was designated as auxiliary military equipment and put on the United States Munitions List. Until the development of the personal computer, asymmetric key algorithms (i.e., public key techniques), and the Internet, this was not especially problematic. However, as the Internet grew and computers became more widely available, high-quality encryption techniques became well known around the globe.

Export Controls

In the 1990s, there were several challenges to US export regulation of cryptography. After the source code for Philip Zimmermann's Pretty Good Privacy (PGP) encryption program found its way onto the Internet in June 1991, a complaint by RSA Security (then called RSA Data Security, Inc.) resulted in a lengthy criminal investigation of Zimmermann by the US Customs Service and the FBI, though no charges were ever filed. Daniel J. Bernstein, then a graduate student at UC Berkeley, brought a lawsuit against the US government challenging some aspects of the restrictions based on free speech grounds. The 1995 case Bernstein v. United States ultimately resulted in a 1999 decision that printed source code for cryptographic algorithms and systems was protected as free speech by the United States Constitution.

In 1996, thirty-nine countries signed the Wassenaar Arrangement, an arms control treaty that deals with the export of arms and "dual-use" technologies such as cryptography. The treaty stipulated that the use of cryptography with short key-lengths (56-bit for symmetric encryption, 512-bit for RSA) would no longer be export-controlled. Cryptography exports from the US became less strictly regulated as a consequence of a major relaxation in 2000; there are no longer very many restrictions on key sizes in US-exported mass-market software. Since this relaxation in US export restrictions, and because most personal computers connected to the Internet include US-sourced web browsers such as Firefox or Internet Explorer, almost every Internet user worldwide has potential access to quality cryptography via their browsers (e.g., via Transport Layer Security). The Mozilla Thunderbird and Microsoft Outlook E-mail client programs similarly can transmit and receive emails via TLS, and can send and receive email encrypted with S/MIME. Many Internet users don't realize that their basic application software contains such extensive cryptosystems. These browsers and email programs are so ubiquitous that even governments whose intent is to regulate civilian use of cryptography generally don't find it practical to do much to control distribution or use of cryptography of this quality, so even when such laws are in force, actual enforcement is often effectively impossible.

NSA Involvement

Another contentious issue connected to cryptography in the United States is the influence of the National Security Agency on cipher development and policy. The NSA was involved with the design of DES during its development at IBM and its consideration by the National Bureau of Standards as a possible Federal Standard for cryptography. DES was designed to be

resistant to differential cryptanalysis, a powerful and general cryptanalytic technique known to the NSA and IBM, that became publicly known only when it was rediscovered in the late 1980s. According to Steven Levy, IBM discovered differential cryptanalysis, but kept the technique secret at the NSA's request. The technique became publicly known only when Biham and Shamir re-discovered and announced it some years later. The entire affair illustrates the difficulty of determining what resources and knowledge an attacker might actually have.

Another instance of the NSA's involvement was the 1993 Clipper chip affair, an encryption microchip intended to be part of the Capstone cryptography-control initiative. Clipper was widely criticized by cryptographers for two reasons. The cipher algorithm (called Skipjack) was then classified (declassified in 1998, long after the Clipper initiative lapsed). The classified cipher caused concerns that the NSA had deliberately made the cipher weak in order to assist its intelligence efforts. The whole initiative was also criticized based on its violation of Kerckhoffs's Principle, as the scheme included a special escrow key held by the government for use by law enforcement (i.e. wiretapping).

Digital Rights Management

Cryptography is central to digital rights management (DRM), a group of techniques for technologically controlling use of copyrighted material, being widely implemented and deployed at the behest of some copyright holders. In 1998, U.S. President Bill Clinton signed the Digital Millennium Copyright Act (DMCA), which criminalized all production, dissemination, and use of certain cryptanalytic techniques and technology (now known or later discovered); specifically, those that could be used to circumvent DRM technological schemes. This had a noticeable impact on the cryptography research community since an argument can be made that any cryptanalytic research violated the DMCA. Similar statutes have since been enacted in several countries and regions, including the implementation in the EU Copyright Directive. Similar restrictions are called for by treaties signed by World Intellectual Property Organization member-states.

The United States Department of Justice and FBI have not enforced the DMCA as rigorously as had been feared by some, but the law, nonetheless, remains a controversial one. Niels Ferguson, a well-respected cryptography researcher, has publicly stated that he will not release some of his research into an Intel security design for fear of prosecution under the DMCA. Cryptologist Bruce Schneier has argued that the DMCA encourages vendor lock-in, while inhibiting actual measures toward cyber-security. Both Alan Cox (longtime Linux kernel developer) and Edward Felten (and some of his students at Princeton) have encountered problems related to the Act. Dmitry Sklyarov was arrested during a visit to the US from Russia, and jailed for five months pending trial for alleged violations of the DMCA arising from work he had done in Russia, where the work was legal. In 2007, the cryptographic keys responsible for Blu-ray and HD DVD content scrambling were discovered and released onto the Internet. In both cases, the Motion Picture Association of America sent out numerous DMCA takedown notices, and there was a massive Internet backlash triggered by the perceived impact of such notices on fair use and free speech.

Forced Disclosure of Encryption Keys

In the United Kingdom, the Regulation of Investigatory Powers Act gives UK police the powers to force suspects to decrypt files or hand over passwords that protect encryption keys. Failure to comply is an offense in its own right, punishable on conviction by a two-year jail sentence or up to five years in cases involving national security. Successful prosecutions have occurred under the Act; the first, in 2009, resulted in a term of 13 months' imprisonment. Similar forced disclosure laws in Australia, Finland, France, and India compel individual suspects under investigation to hand over encryption keys or passwords during a criminal investigation.

In the United States, the federal criminal case of United States v. Fricosu addressed whether a search warrant can compel a person to reveal an encryption passphrase or password. The Electronic Frontier Foundation (EFF) argued that this is a violation of the protection from self-incrimination given by the Fifth Amendment. In 2012, the court ruled that under the All Writs Act, the defendant was required to produce an unencrypted hard drive for the court.

In many jurisdictions, the legal status of forced disclosure remains unclear.

The 2016 FBI–Apple encryption dispute concerns the ability of courts in the United States to compel manufacturers' assistance in unlocking cell phones whose contents are cryptographically protected.

As a potential counter-measure to forced disclosure some cryptographic software supports plausible deniability, where the encrypted data is indistinguishable from unused random data (for example such as that of a drive which has been securely wiped).

Adapted from:
"Cryptography" by Multiple Authors, Wikipedia is licensed under CC BY-SA 3.0

5.7: Cryptography Applications

Uses for Cryptography

General

Cryptography is widely used on the internet to help protect user-data and prevent eavesdropping. To ensure secrecy during transmission, many systems use private key cryptography to protect transmitted information. With public-key systems, one can maintain secrecy without a master key or a large number of keys. But, some algorithms like Bitlocker and Veracrypt are generally not private-public key cryptography. Such as Veracrypt, it uses a password hash to generate the single private key. However, it can be configured to run in public-private key systems. The C++ opensource encryption library OpenSSL provides free and opensource encryption software and tools. The most commonly used encryption cipher suit is AES, as it has hardware acceleration for all x86 based processors that has AES-NI. A close contender is ChaCha20-Poly1305, which is a stream cipher, however it is commonly used for mobile devices as they are ARM based which does not feature AES-NI instruction set extension.

Cybersecurity

Cryptography can be used to secure communications by encrypting them. Websites use encryption via HTTPS. "End-to-end" encryption, where only sender and receiver can read messages, is implemented for email in Pretty Good Privacy and for secure messaging in general in WhatsApp, Signal and Telegram.

Operating systems use encryption to keep passwords secret, conceal parts of the system, and ensure that software updates are truly from the system maker. Instead of storing plaintext passwords, computer systems store hashes thereof; then, when a user logs in, the system passes the given password through a cryptographic hash function and compares it to the hashed value on file. In this manner, neither the system nor an attacker has at any point access to the password in plaintext.

Encryption is sometimes used to encrypt one's entire drive. For example, University College London has implemented BitLocker (a program by Microsoft) to render drive data opaque without users logging in.

Cryptocurrencies and Cryptoeconomics

Cryptographic techniques enable cryptocurrency technologies, such as distributed ledger technologies (e.g., blockchains), which finance cryptoeconomics applications such as decentralized finance (DeFi). Key cryptographic techniques that enable cryptocurrencies and cryptoeconomics include, but are not limited to: cryptographic keys, cryptographic hash functions, asymmetric (public key) encryption, Multi-Factor Authentication (MFA), End-to-End Encryption (E2EE), and Zero Knowledge Proofs (ZKP)

Adapted from:
"Cryptography" by Multiple Authors, Wikipedia is licensed under CC BY-SA 3.0

Index

D

Glossary

Sample Word 1 | Sample Definition 1

Detailed Licensing

Overview

Title: Information Security

Webpages: 114

Applicable Restrictions: Noncommercial

All licenses found:

- CC BY-SA 4.0: 57% (65 pages)
- Undeclared: 36% (41 pages)
- CC BY-NC-SA 4.0: 6.1% (7 pages)
- CC BY 4.0: 0.9% (1 page)

By Page