Cyber Security

Course material written

By

DR. Bhagirathi Nayak
Ph.D (Computer Science)
Professor and Head (IT & Systems)
Sri Sri University, Cuttack. Odisha

20 Years Experience from IIT Kharagpur.

Contents

Chapter I

Networking Fundamentals

Chapter II

Networking Advanced

Networking Fundamentals

Introduction Networking Concepts

Contact Network

Anyone who has looked for a job knows that one of the best ways to find a job is to network. That is, create a list of friends and associates who will help you find the perfect job. The more people you meet and get to know, the better your chances of obtaining work. As you develop and nurture your career, this contact network will serve you best because your role in it will change as you gain more experience. Soon, you may be able to help the people who helped you. And as your personal and professional networks grow, so do your opportunities.

These examples of human networks should help you understand that networking is common between people and is not just an activity restricted to computers. However, it will focus on computer networks—connecting computers and having them communicate with each other.

Example of Contact Network

Computer Networks

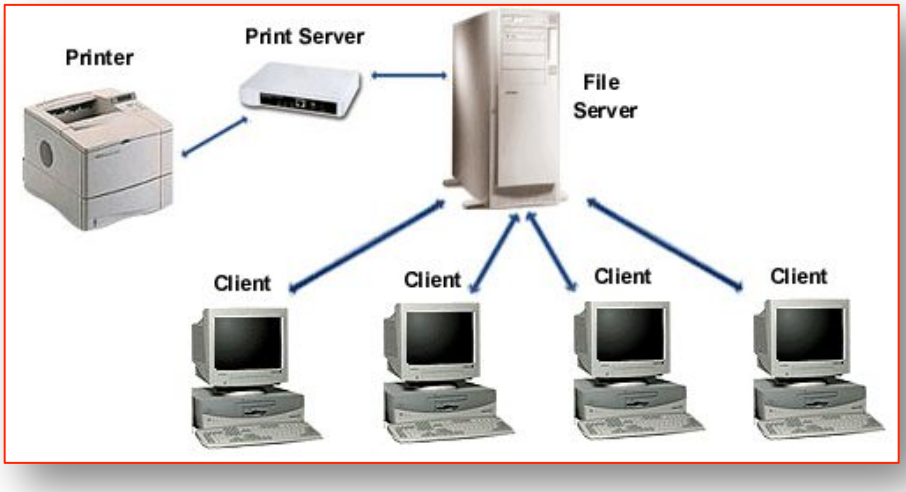
A **computer network** consists of two or more computing devices that are connected in order to share the components of your network (its resources) and the information you store there. The most basic computer network (which consists of just two connected computers) can expand and become more usable when additional computers join and add their resources to those being shared.

The first computer, yours, is commonly referred to as your **local computer**. It is more likely to be used as a location where you do work, a **workstation**, than as a storage or controlling location, a server. As more and more computers are connected to a network and share their resources, the net-

work becomes a more powerful tool, because employees using a network with more information and more capability are able to accomplish more through those added computers or additional resources.

The real power of networking computers becomes apparent if you envision your own network growing and then connecting it with other distinct networks, enabling communication and resource sharing across both networks. That is, one network can be connected to another network and become a more powerful tool because of the greater resources.

Example of Computer Network

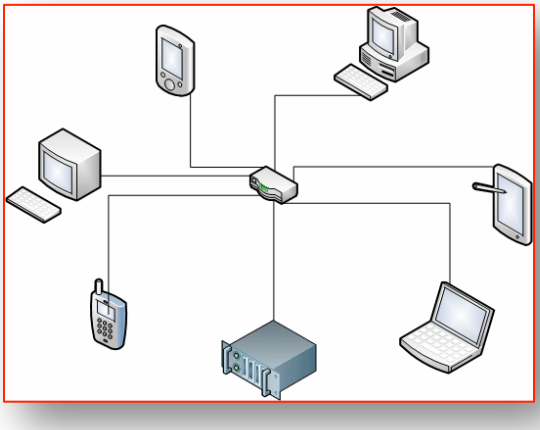


Network Distribution

Networking hardware may also be known as network equipment or computer networking devices. Units, which are the last receiver or generate data, are called hosts or data terminal equipment. All these terms refer to devices facilitating the use of a computer network.

Introduction

Building a network consists partly of connecting the computers



Classifying Networks

Networks are frequently classified according to the geographical boundaries the network spans. Two basic geographical designations for networks—Local Area Network (LAN) and Wide Area Network (WAN)—are the most common. A third designation, Metropolitan Area Network (MAN), is also used, although its use has become clouded (because it might not be a clear-cut classification anymore) as networks continue connecting to the Internet.

Network Hardware

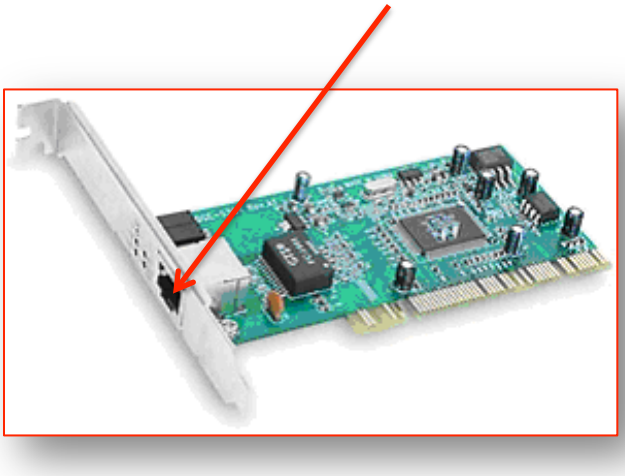
Network Cables

Cable is used to connect computers. Although we may use wireless networking, you should always have cables with you. The most commonly used cable is referred to as Category 6 cable RJ-45. The ends of the cable appear as follows

Category 6 Cable RJ-45 Connector

Wired Network Adapter: Internal

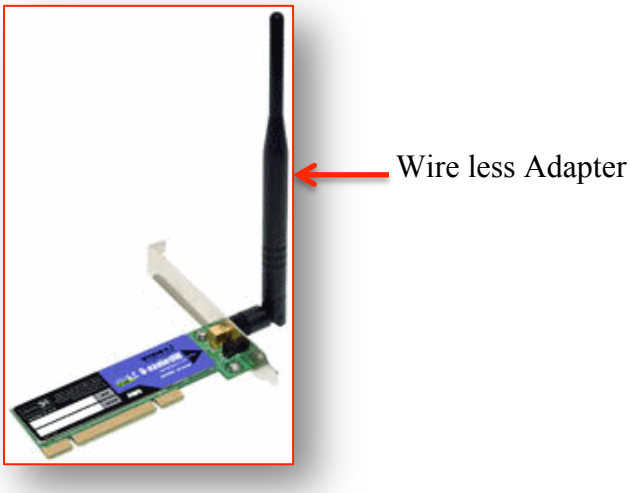
In order to connect to a network, a computer must be equipped with a device called a network card. A network card, or a network adapter, also called a network interface card, or NIC, allows a computer to connect to the exterior. Network Port.



Wireless Network Adapter

Depending on network budget or customers, instead of using wired network cards, it can use wireless ones. Most laptops already have a wireless card built-in so it may not have to acquire one. Many new desktop computers now have built-in wireless capability.

A wireless NIC appears as its wired counterpart. Here is the example.

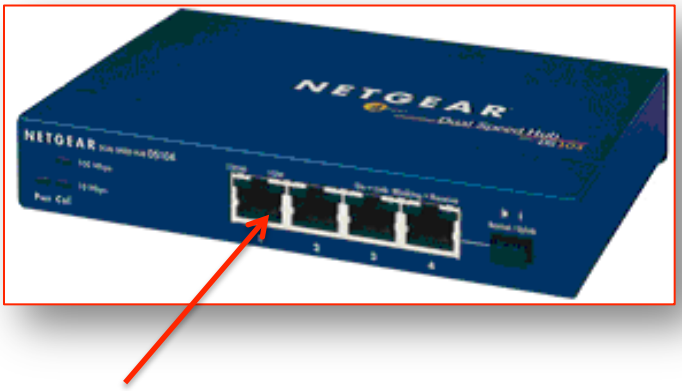


USB Network Adapter

Besides the wireless network cards that can be installed inside the computer, it can use external cards. These are installed using a USB port. Here is an example of a USB adapter:

Hub

A hub is rectangular box that is used as the central object on which computers and other devices are connected. To make this possible, a hub is equipped with small holes called ports. Here is an example of a hub. It can be equipped with 4, 8, 12, 16, 32 ports.



Network Port

Routers: Wired or Wireless

Like a hub, a router is another type of device that acts as the central point among computers and other devices that are part of a network. Here is an example of a wired router.

Network Port

Information Security Concepts

Three basic security concepts important to information on the Internet are confidentiality, integrity, and availability. Concepts relating to the people who use that information are authentication, authorization, and nonrepudiation. Information security (infosec) is the set of business processes that protects information assets regardless of how the information is formatted or whether it is being processed, is in transit or is being stored. This is not a single technology; rather it a strategy comprised of the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Processes and policies typically involve both physical and digital security measures to protect data from unauthorized access, use, replication or destruction. Infosec management can include everything from mantraps to encryption key management and malware detection.

Security Threats and Vulnerable

In computer security a threat is a possible danger that might exploit vulnerability to breach security and thus cause possible harm. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire, or a tornado) or otherwise a circumstance, capability, action, or event.

Computer security threats are relentlessly inventive. Masters of disguise and manipulation, these threats constantly evolve to find new ways to annoy, steal and harm. Arm yourself with information and resources to safeguard against complex and growing computer security threats and stay safe online.

Computer Virus Threats

Perhaps the most well known computer security threat, a computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to computer in the process. Learn how to combat computer virus threats and stay safe online.

Spyware Threats

A serious computer security threat, spyware is any program that monitors online activities or installs programs without consent for profit or to capture personal information. We've amassed a wealth of knowledge that will help you combat spyware threats and stay safe online.

Hackers & Predators

People, not computers, create computer security threats and malware. Hackers and predators are programmers who victimize others for their own gain by breaking into computer systems to steal, change or destroy information as a form of cyber-terrorism. What scams are they using lately? Learn how to combat dangerous malware and stay safe online.

Phishing Threats

Masquerading as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. How can you tell the difference between a legitimate message and a phishing scam? Educate yourself on the latest tricks and scams.

Vulnerabilities

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

Types of Security Vulnerabilities

Most software security vulnerabilities fall into one of a small set of categories.

- Buffer overflows
- Unvalidated input
- Race conditions
- Access-control problems
- Weaknesses in authentication, authorization, or cryptographic practices

Cryptography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

1. **Confidentiality** (the information cannot be understood by anyone for whom it was unintended)

2. **Integrity** (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

3. **Non-repudiation** (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

4. **Authentication** (the sender and receiver can confirm each others identity and the origin/destination of the information)

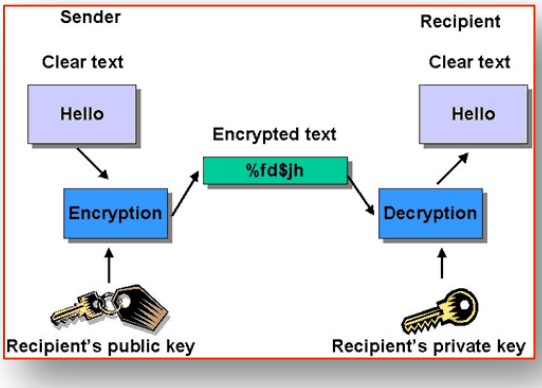
Example: Symmetric Cryptography

Encryption

Encryption is the conversion of electronic data into another form, called cipher text, which cannot be easily understood by anyone except authorized parties. The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the Internet or other computer networks. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications as they can provide not only confidentiality, but also the following key elements of security

- **Authentication:** the origin of a message can be verified.
- **Integrity:** proof that the contents of a message have not been changed since it was sent.
- **Non-repudiation:** the sender of a message cannot deny sending the message.

Example: Encrypted email



Types of Attacks

Cyber-attacks have become commonplace. It is Costly cyber-attacks have become so frequent across industries that cyber-security is top of mind among executives and customers worldwide.

There are several types of attacks is possible, but here it discussed about mostly nine types of cyber attacks accounted for 92% of the incidents that occurred in the past decade:

Crimeware: The public sector, utilities, manufacturing, and information industries are particularly at risk of malware that compromises systems such as servers and desktops. To make it harder for crimeware to get in, patch anti-virus programmes and browsers, avoid Java browser plugins as much as possible, use two-factor identification, and implement configuration-change monitoring.

Insider and privilege misuse: Misuse of computer access privileges is widespread among industries and within companies. To better protect your data, find out who has access to every aspect of it, review user accounts, set up controls to watch for data transfers out of the organisation, and publish anonymised results of audits.

Physical theft and loss: The public and health-care sectors are threatened by the loss or theft of laptops, USB drives, or printed documents. To prevent theft or loss, encrypt devices, back up data regularly, lock down IT equipment to immovable fixtures, and store sensitive documents in secure areas.

Web app attacks: Utilities and companies in the information, manufacturing, and retail sectors face risks from web application attacks. To prevent misuse of stolen credentials or exploitation of vulnerabilities, use two-factor authentication, consider switching to a static content-management system, lock accounts after repeated failed login attempts, and monitor outbound connections.

Denial-of-service attacks: The finance and retail sectors are particularly at risk of being attacked by botnets and powerful servers trying to grind business operations of systems and applications to a halt. To fortify against malicious traffic attacks, ensure that servers are patched promptly, buy a small backup circuit and segregate key servers, test your anti-DoS service, and make sure key operations teams know what to do in case of an attack.

Cyber-espionage: Professional services, transportation, manufacturing, mining, and the public sector are popular targets. To protect against breaches, patch software vulnerabilities, update anti-virus software, train users to recognise and report danger signs, and keep good logs of system, network, and application activity.

POS intrusions: Retail and the hospitality sector are particularly at risk. To reduce the risk, limit remote access to POS systems by third-party companies; enforce strong password policies; do not allow staff to use POS systems to browse the web, check email, or play games; and use two-factor authentication.

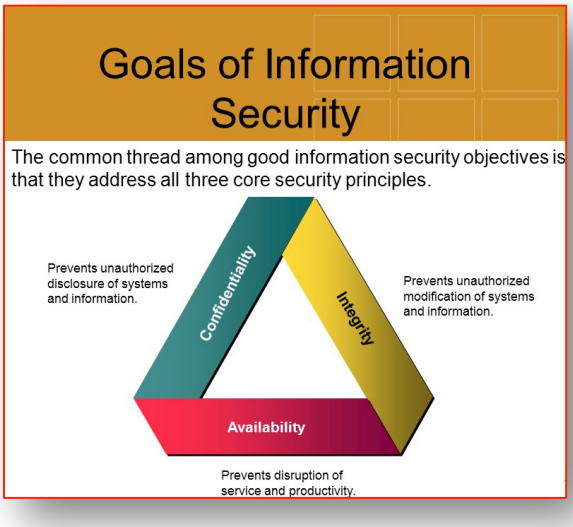
Payment card skimmers: Banks, retailers, and hospitality companies are particularly at risk of skimmers' reading payment cards as customers pay. To prevent the installation of skimmers on, for example, petrol pumps or ATMs, use tamper-resistant terminals, train employees to spot skimmers and recognise suspicious behaviour, and use tamper-evident controls, such as seals over gas pump doors or automated video monitoring.

Miscellaneous errors: Industries that deal in information dissemination are threatened by security mistakes such as accidentally sending private data to a public site, sending information to the wrong recipients, or failing to dispose of documents or assets securely. To minimise such mistakes, implement data-loss prevention software, strengthen controls on publishing, and train staff on asset disposal.

Goals for Security

Overview of goals of security: Confidentiality, Integrity, and Availability. The CIA (Confidentiality, Integrity and Availability) is a security model that is designed to act as a guide for information security policies within the premises of an organization or company. The CIA criteria is one that most of the organizations and companies use in instances where they have installed a new application, creates a database or when guaranteeing access to some data. For data to be completely secured, all of these security goals must come to effect. These are security policies that all work together and therefore it can be wrong to overlook one policy.

The Three Security Goals are Confidentiality, Integrity, Availability, and Safety. All information security measures try to address at least one of three goals: Protect the confidentiality of data. Preserve the integrity of data.



Confidentiality: The confidentiality aspect refers to limiting the disclosure and access of information to only the people who are authorized and preventing those not authorized from accessing it. Through this method, a company or organization is able to prevent highly sensitive and vital information from getting into the hand of the wrong people while still making it accessible to the right people.

- Keep data and communication secret
- Privacy of personal financial/health records, etc.
- Military and commercial relevance

Integrity: Integrity is another security concept that entails maintaining data in a consistent, accurate and trustworthy manner over the period in which it will be existent. In this case, one has to ensure that data is not changed in the course of a certain period. In addition, the right procedures have to be taken to ensure that unauthorized people do not alter the data.

- Protect reliability of data against tampering
- Be sure of the source and content of information?

Availability: The concept of availability refers to the up time maintenance of all resources and hardware. This means that all the hardware and resources one have are functional all the time. It can also involve carrying out of regular hardware repairs.

- Data/resources should be accessible when needed
- Protection against denial of service attacks

Safety: Safety is also a very important aspect not only in an organization but also some other environments such as at home. For optimal assurance of safety, there has to be some properly set strategies that are to be followed if proper safety is to be effective. Safety does not only entail being away from danger but also having the capability to prevent unauthorized access of a particular resource or facility. Safety should also include proper monitoring of all the activities happening in a particular area or vicinity.

E-Commerce Security

What is e-commerce security?

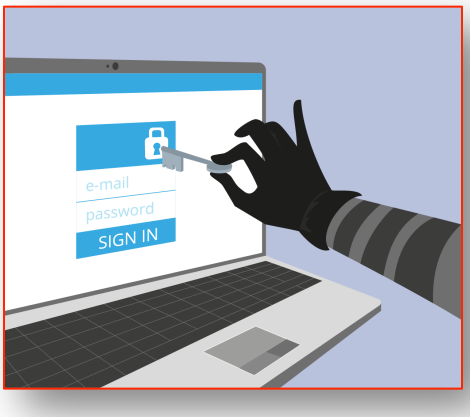
E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.

Six dimensions of e-commerce security

1. **Integrity:** prevention against unauthorized data modification
2. **Nonrepudiation:** prevention against any one party from reneging on an agreement after the fact
3. **Authenticity:** authentication of data source
4. **Confidentiality:** protection against unauthorized data disclosure
5. **Privacy:** provision of data control and disclosure
6. **Availability:** prevention against data delays or removal

E-commerce threats

Threats: anyone with the capability, technology, opportunity, and intent to do harm. Potential threats can be foreign or domestic, internal or external, state-sponsored or a single rogue element. Terrorists, insiders, disgruntled employees, and hackers are included in this profile (President's Commission on Critical Infrastructure Protection)



Common threats

- The base for the website is ultimately their servers and the computer which are their Client through this service. Mainly the threats, which are running against the security of online media is Trojan horse, Active contents, Viruses. Along the sides on server's common threats is Privilege setting, Server Side Include (SSI), Common Gateway Interface (CGI), and File transfer, spamming.

- The prone area where the effect of attack is visible is shopping software cart. The routines, which are applicable here, are online purchasing updates, tracking customer's details and accounts and bunch of other services. It is all tied up in software. It is basically an operating system. The next point where there is need for security is online payment transaction. The whole system works around with accepting credit cards details through a gateway, which is purely online.

- Other such threats are cracking; spoofing, eavesdropping, root kits. The trends also show us threats like System unavailability and denial of service, power interruptions.

Intellectual property threats: Use existing materials found on the Internet without the owner's permission, e.g., music downloading, domain name (cybersquatting), software pirating.

Client computer threats

- Trojan horse
- Active contents
- Viruses

Communication channel threats

- Sniffer program
- Backdoor
- Spoofing
- Denial-of-service

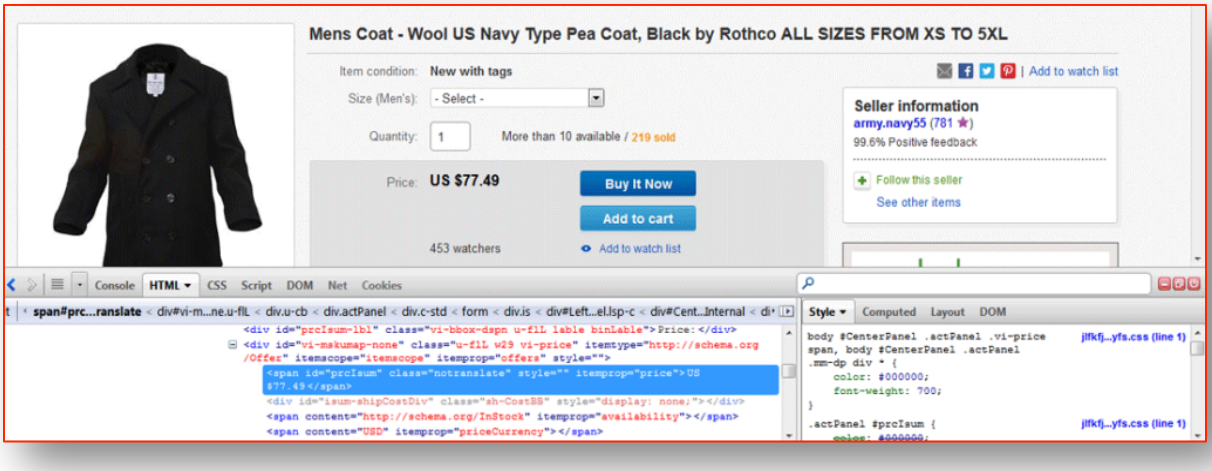
Server threats

- Privilege setting
- Server Side Include (SSI), Common Gateway Interface (CGI)
- File transfer
- Spamming

Common vulnerabilities:

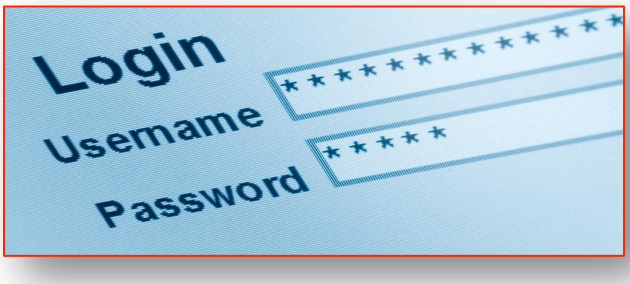
- **SQL Injection:** SQL injection is a phenomenon with which malware author inserts SQL characters in field of user input. Through this it make such that queries are executed at the back-end of database. IF say the e-commerce website is vulnerable to such attacks, they have the power to attack even the restricted areas of website. Depending upon the knowledge of the attacker, they may steal sensitive data viz. credit card numbers, transaction details, etc. The tendencies of getting such an attack via log in page are common.

- **Price Manipulation:** This is vulnerability where the total payable price of the goods purchased is stored over a hidden HTML field, which is dynamically generated by web page. With use of some tools, the modification of payable amount is changed.



- **Cross-site scripting:** It is because of lack of proper input/output validation by the web application that such circumstances are faced by the websites driving commerce. The forms which are present on such website which are basically for feedback or suggestion about the products, here the malware author can induce his own content and make a whole new script running on the victim's system. This way they steal sensitive information and session ID's. It leads to stealing credential of users again.

- **Weak Authentication and Authorization:** The Authentication mechanisms are simple criteria to breach into the target system by malware authors. Some of system which does not limit the failed log ins often gets to face the circumstances of stealing away the credentials of users or even sometimes leading to fake online purchase being some other person. This way there is huge risk to authentic user's credentials.



Computer Forensics

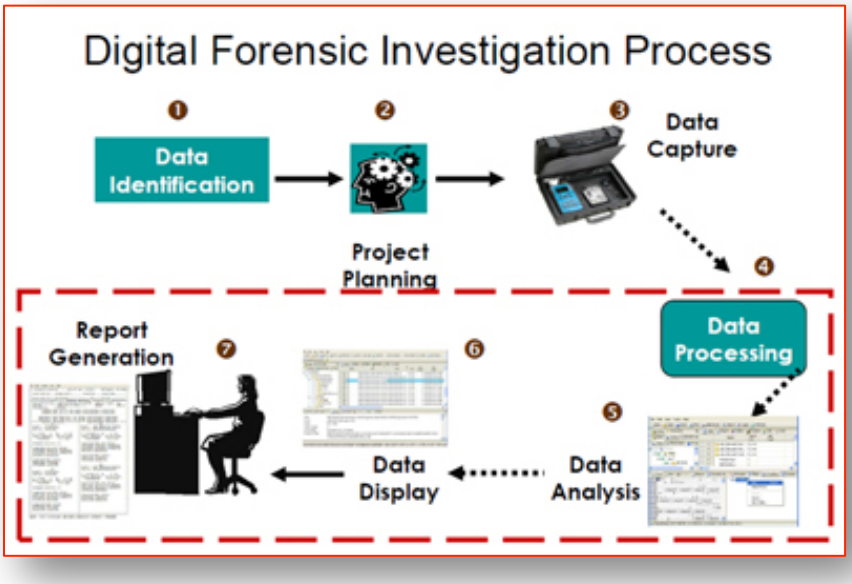
Computer forensics is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally.

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Forensic investigators typically follow a standard set of procedures: After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.

Example: Digital Investigation Process



Uses of computer forensics

There are few areas of crime or dispute where computer forensics cannot be applied. Law enforcement agencies have been among the earliest and heaviest users of computer forensics and consequently have often been at the forefront of developments in the field.

Computers may constitute a 'scene of a crime', for example with hacking or denial of service attacks or they may hold evidence in the form of emails, internet history, documents or other files relevant to crimes such as murder, kidnap, fraud and drug trafficking.

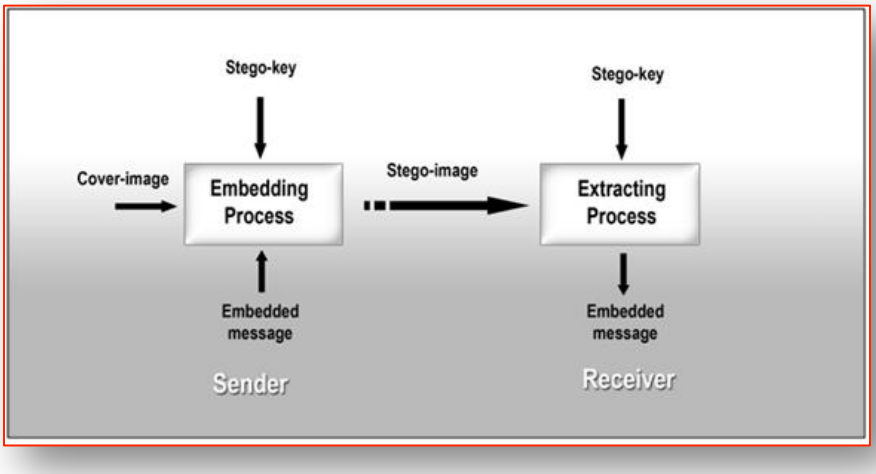
It is not just the content of emails, documents and other files, which may be of interest to investigators, but also the 'metadata' associated with those files. A computer forensic examination may reveal when a document first appeared on a computer, when it was last edited, when it was last saved or printed and which user carried out these actions.

More recently, commercial organizations have used computer forensics to their benefit in a variety of cases such as:

* Intellectual Property theft
* Industrial espionage
* Employment disputes
* Fraud investigations
* Forgeries
* Bankruptcy investigations
* Inappropriate email and Internet use in the work place
* Regulatory compliance

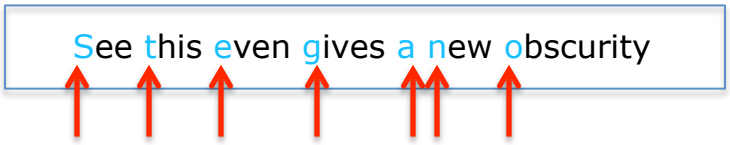
Steganography

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.



This technique is commonly used to conceal information inside files that appear to be normal, the most common being inside images. This can start off very simple such as having a plain coloured background for an image, then changing the colour slightly and trying a message into the image (look out for this here!) or go as advanced as using programs to encrypt the message and embed it into the image. This however is very hard to un-encrypt without know the encryption used.

It can also be used to hide messages inside a paragraph, for example:



Taking the first letter of each word, or simply

Sound Stegano

It is also very easy to hide messages in a sound (such as an mp3) file. The most commonly used method is a method knows as **backmasking** in which the message is reversed and added to the sound file. Also speeding up the message by a large amount so that it just sounds like some static is also effective. This can be classed as subliminal messaging though and can get in trouble if the listener doesn't know it contains a hidden message.

Video

There are hiding messages in videos; this is very easy to do because of the high frame rate videos use. For example cartoons usually use on average 10 frames a second, meaning if one of those frames is altered slightly chances are no one will notice. Words could be added to one of the frames or the frame could be changed completely to display something else entirely.

Security Threats

General methods of security threats fall under two categories:

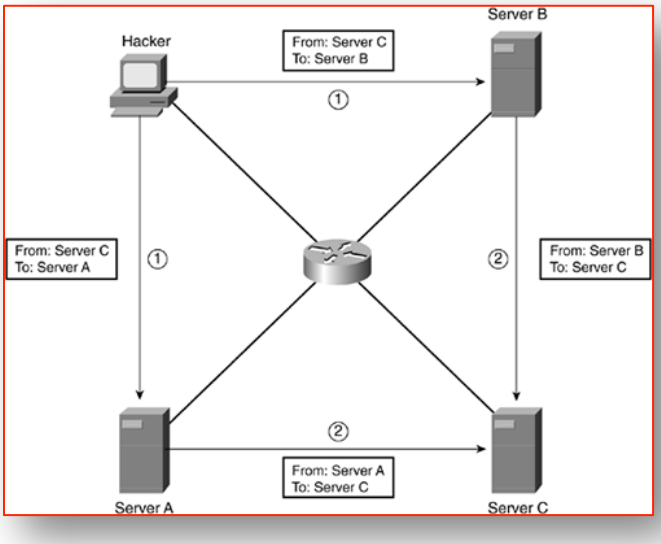
- Unstructured threats
- Structured threats

Unstructured Threats: An unstructured security threat is one created by an inexperienced person who is trying to gain access to your network? a wannabe hacker. A good security solution easily should thwart this kind of attack. Many tools available to anyone on the Internet can be used to discover weaknesses in a company's network. These include port-scanning tools, address-sweeping tools, and many others. Most of these kinds of probes are done more out of curiosity than with a malicious intent in mind. This is especially true of internal users who are interested in what kinds of devices exist in their own network.

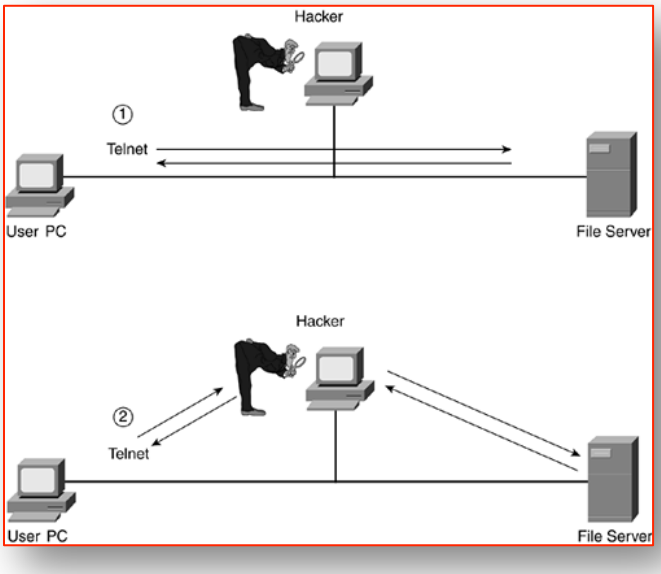
Structured threats: A structured security threat, on the other hand, is implemented by a technically skilled person who is trying to gain access to your network. This hacker creates or uses some very sophisticated tools to break into your network or to disrupt the services running in your network. A good example of a structured attack is a distributed ICMP flood. A person with very little hacking skill probably would send a flood of pings from the same source machine, making it fairly easy to track down the culprit. A sophisticated hacker, on the other hand, will try to hide the source of the ICMP packets by changing the source address inside the packets (called spoofing), as well as executing the attack from several different sources. Tracking down the culprit of this kind of attack takes a lot of work and patience.

This shows a simple example of a sophisticated spoofing attack. In this example, the hacker changes the source address in ICMP packets to those of Server C, which is the device that the hacker is attacking. He sends these packets to both Server A and Server B. These servers respond to the ICMP messages to the destination listed as the source in the packets, Server C. In this example, with the hacker flooding packets to both Server A and Server B, which, in turn, hit Server C twice as hard, it becomes more difficult, from Server C's perspective, to figure out who the real culprit of the attack is: the hacker.

Sophisticated Spoofing Attack



Session-Hijacking Attack



Password Cracking

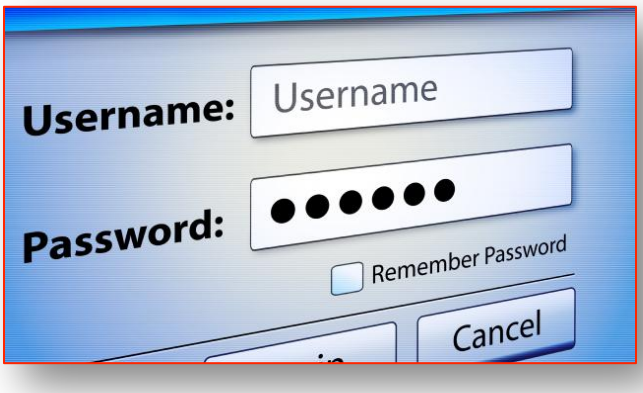
A password cracker is an application program that is used to identify an unknown or forgotten password to a computer or network resources. It can also be used to help a human cracker obtain unauthorized access to resources.

Password crackers use two primary methods to identify correct passwords: brute-force and dictionary searches. When a password cracker uses brute-force, it runs through combinations of characters within a predetermined length until it finds the combination accepted by the computer system. When conducting a dictionary search, a password cracker searches each word in the dictionary for the correct password. Password dictionaries exist for a variety of topics and combinations of topics, including politics, movies, and music groups.

Some password cracker programs search for hybrids of dictionary entries and numbers. For example, a password cracker may search for ants01; ants02; ants03, etc. This can be helpful where users have been advised to include a number in their password.

A password cracker may also be able to identify encrypted passwords. After retrieving the password from the computer's memory, the program may be able to decrypt it. Or, by using the same algorithm as the system program, the password cracker creates an encrypted version of the password that matches the original.

Top ten password cracking techniques



Here are the ten most common password-cracking techniques in use:

1. Dictionary attack

This uses a simple file containing words that can, surprise surprise, be found in a dictionary. In other words, if you will excuse the pun, this attack uses exactly the kind of words that many people use as their password. Cleverly grouping words together such as ‘letmein’ or ‘superadministratorguy’ will not prevent your password from being cracked this way - well, not for more than a few extra seconds.

2. Brute force attack

This method is similar to the dictionary attack but with the added bonus, for the hacker, of being able to detect non-dictionary words by working through all possible alpha-numeric combinations from aaa1 to zzz10.

It's not quick, provided your password is over a handful of characters long, but it will uncover your password eventually. Brute force attacks can be shortened by throwing additional computing horsepower, in terms of both processing power - including harnessing the power of your video card GPU - and machine numbers, such as using distributed computing models and zombie botnets.

3. Rainbow table attack

A rainbow table is a list of pre-computed hashes - the numerical value of an encrypted password, used by most systems today - and that's the hashes of all possible password combinations for any given hashing algorithm mind. The time it takes to crack a password using a rainbow table is reduced to the time it takes to look it up in the list.

4. Phishing

There's an easy way to hack: ask the user for his or her password. A phishing email leads the unsuspecting reader to a faked online banking, payment or other site in order to login and put right some terrible problem with their security. Why bother going to the trouble of cracking the password when the user will happily give it you anyway?

5. Social engineering

Social engineering takes the whole 'ask the user' concept outside of the inbox that phishing tends to stick with and into the real world. A favourite of the social engineer is to telephone an office posing as an IT security tech guy and simply ask for the network access password. You'd be amazed how often this works. Some even have the necessary gonads to don a suit and name badge before walking into a business to ask the receptionist the same question face to face.

6. Malware

A key logger or screen scraper can be installed by malware which records everything you type or takes screen shots during a login process, and then forwards a copy of this file to hacker central. Some malware will look for the existence of a web browser client password file and copy this, which unless properly encrypted, will contain easily accessible saved passwords from the user's browsing history.

7. Offline cracking

It's easy to imagine that passwords are safe when the systems they protect lock out users after three or four wrong guesses, blocking automated guessing applications. Well, that would be true if it were not for the fact that most password hacking takes place offline, using a set of hashes in a password file that has been 'obtained' from a compromised system.

Often the target in question has been compromised via an hack on a third party, which then provides access to the system servers and those all-important user password hash files. The password cracker can then take as long as they need to try and crack the code without alerting the target system or individual user.

8. Shoulder surfing

The most confident of hackers will take the guise of a parcel courier, aircon service technician or anything else that gets them access to an office building. Once they are in, the service personnel 'uniform' provides a kind of free pass to wander around unhindered, and make note of passwords being entered by genuine members of staff. It also provides an excellent opportunity to eyeball all those post-it notes stuck to the front of LCD screens with logins scribbled upon them.

9. Spidering

Savvy hackers have realised that many corporate passwords are made up of words that are connected to the business itself. Studying corporate literature, website sales material and even the websites of competitors and listed customers can provide the ammunition to build a custom word list to use in a brute force attack. Really savvy hackers have automated the process and let a spidering application, similar to those employed by leading search engines to identify keywords, collect and collate the lists for them.

10. Guess

The password crackers best friend, of course, is the predictability of the user. Unless a truly random password has been created using software dedicated to the task, a user generated 'random' password is unlikely to be anything of the sort. Instead, thanks to our brains' emotional attachment to things we like, the chances are those random passwords are based upon our interests, hobbies, pets, family and so on. In fact, passwords tend to be based on all the things we like to chat about on social networks and even include in our profiles. Password crackers are very likely to look at this information and make few-often-correct educated guesses when attempting to crack a consumer-level password without resorting to dictionary or brute force attacks.

Insecure Network connections

Internet Explorer won't open a website because of an insecure connection to the site's server. This happens when Internet Explorer encounters a security protocol that is insecure or no longer supported. This type of a connection will make your PC vulnerable to attacks by allowing data sent between you and the website to be intercepted. Internet Explorer 11 now blocks insecure connections to help protect your PC and personal data.

Loading a WordPress/Shopp website over HTTPS with a valid SSL certificate results in "insecure content", "non-secure content", "partially encrypted" or "mixed content" warnings in different browsers.

Errors

Chrome

Error displays when hovering over the crossed out https in the location bar.

> The connection to website.com is encrypted with 256-bit encryption. However, this page includes other resources, which are not secure. These resources can be viewed by others while in transit, and can be modified by an attacker to change the behavior of the page.

Safari

No secure lock icon appears in the top right of the browser window title bar. The error message only appears in the error console.

> The page at https://website.com/ displayed insecure content from http://website.com/images/image.jpg.

Firefox

Clicking the website icon shown on the left side of the location bar will display the error.

> Your connection to this site is only partially encrypted, and does not prevent eavesdropping.

Clicking the **More Information** button of the connection details popup shows the following **Technical Details**

> Connection Partially Encrypted
>
> Parts of the page you are viewing were not encrypted before being transmitted over the Internet. Information sent over the Internet without encryption can be seen by other people while it is in transit.

Internet Explorer

Internet Explorer 9 displays a popup dialog at the bottom of the page.

> Only secure content is displayed.

Internet Explorer 8 displayed a popup alert.

Security Warning

Do you want to view only the webpage content that was delivered securely?

This webpage contains content that will not be delivered using a secure HTTPS connection, which could compromise the security of the entire webpage.

Opera

Clicking the **Page Information** icon button show to the left of the location bar displays a popup with the error.

Insecure Connection

Clicking the **More Details** button shows a new window with in-depth **Security Information**.

Site not secure

The connection to website.com is not secure. Do not use it to submit sensitive information.

The server attempted to apply security measures, but failed.

Open your Internet Explorer browser then go to **Internet Options**.

- Click on **Security** tab.
- Click on **Trusted sites**, and then click the **Sites** button.
- On the "**Add this website to the zone:**" URL bar, type the complete URL address.
- Click on **Add** button.
- Once you already added all URL addresses, click the **Close** button.
- Click on **Apply** or **OK** button then close your Internet Explorer browser.

A wireless **network** is "**unsecured**" if you can access the Internet using the **network** without entering a password or **network** key. For example, a "hotspot" is a wireless **network** that is open and available for the public to use.

Insecure Network Services

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence UNCOMMON	Detectability AVERAGE	Impact MODERATE	Application / Business Specific
Consider anyone who has access to the device via a network connection, including external and internal users.	Attacker uses vulnerable network services to attack the device itself or bounce attacks off the device. Attack could come from external or internal users.	Insecure network services may be susceptible to buffer overflow attacks or attacks that create a denial of service condition leaving the device inaccessible to the user. Denial of service attacks against other users may also be facilitated when insecure network services are available. Insecure network services can often be detected by automated tools such as port scanners and fuzzers.		Insecure network services can result in data loss or corruption, denial of service or facilitation of attacks on other devices.	Consider the business impact of devices, which have been rendered useless from a denial of service attack, or the device is used to facilitate attacks against other devices and networks. Could your customers or other users be harmed?

Malicious Code

Malicious code is the term used to describe any **code** in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. **Malicious code** is an application security threat that cannot be efficiently controlled by conventional antivirus software alone.

Malicious code refers to a broad category of programs that can cause damage or undesirable effects to computers or networks. Potential damage can include modifying, destroying or stealing data, gaining or allowing unauthorised access to a system, bringing up unwanted screens, and executing functions that a user never intended.

Examples of malicious code include computer viruses, worms, trojan horses, logic bombs, spyware, adware and backdoor programs. Because they pose a serious threat to software and information processing facilities, users and administrators must take precautions to detect and prevent malicious code outbreaks.

Risk

The risks posed by malicious code are on the rise, due to fundamental changes in the threats and purposes that malicious code is put to. Instead of just causing a nuisance and being destructive, malicious code attacks are becoming more motivated by financial gain. Attackers are increasingly sophisticated and organised, adopting methods that are similar to traditional software development and business practices.

It has been shown that the amount of time between the discovery of software vulnerability and attempts to exploit that vulnerability via attacks from new computer viruses/worms is continuously decreasing. In addition, it takes time for anti-virus vendors to develop virus and malicious code definitions, so there is always a chance that your anti-virus software cannot detect newly discovered malicious code in time. Thus, your computer is still vulnerable to virus attack if other security best practices are not put in place.

Computer system could be infected if:

- A user is lured into installing or opening a malicious attachment / program / plug-in from an un-trusted source or from a spam email
- A user is lured into visiting a malicious website
- The computer is not properly patched, so attackers take advantage and exploit a vulnerability
- The computer is not properly configured, so attackers take advantage and exploit a vulnerability

Examples of **malicious code** include computer viruses, worms, trojan horses, logic bombs, spyware, adware and backdoor programs.

Bugs in Programming

Webster's Collegiate Dictionary includes the following definition of **bug**: "an unexpected defect, fault, flaw, or imperfections." In programming jargon, “errors” are known as “bugs”. There are many apocryphal stories about the origin of this term and how it got applied to programming. In the most popular story, Grace Murray Hopper discovered that the Harvard Mark II computer was producing incorrect answers. When she examined the machine more closely, trying to locate the problem, she found a squashed moth, which was caught between the contacts of an electromechanical relay, preventing the relay from fully closing; ergo, the first computer bug. In fact, she extracted the moth with a pair of tweezers and taped it into the operator's logbook with the comment “First actual bug found” -implying that the term was already in use at that time. Other stories about the first use of “bug” abound, so perhaps we shall never know the true entomology of this word.

The term bug became popular in programming to save the egos of programmers who could not admit that their programs were full of errors. Instead, they preferred to say that their programs had bugs in them. Actually, the metaphor is apt: programming bugs are hard to find; and although a located bug is frequently easy to fix, it is difficult to ensure that all the bugs have been removed from a program.
Debugging is the name that programmers give to the activity of locating and removing errors from programs (once the errors are known to exist, from **testing** the program). A programmer who is

testing a program is often looking for new bugs to correct.

Classifying Bugs

This section classifies bugs into five broad categories, each illustrated via an analogy that should help clarify its nature. Knowing the names of our enemies is the first step toward defeating them.

- **Token error**
- **Syntax error**
- **Syntax constraint error**
- **Execution error**
- **Intent error**.

Token error

A token error occurs whenever our program contains a word or symbol that is not in Java's vocabulary. As an analogy, suppose that one day we are standing on a street in San Francisco, and are asked by a lost motorist, "How can I get to Portland, Oregon?" If we say, "Just keep gngoi for ihegt hundred semil," we would have committed multiple token errors. The motorist is unable to follow our instructions, because he is unable to decipher some of the words from which the instructions are composed. Similarly, the Java compiler must recognize each token (identifier, symbol, literal, and comment) in our programs.

Syntax error

Even though the Java compiler may recognize every token in a program, the program still may contain a syntax error. This type of error occurs whenever we use incorrect grammar or punctuation (according to the syntax rules of the Java programming language). Going back to our lost motorist, we might reply, "For keep hundred miles going eight just." Here, each word/token is individually recognizable as correct English, but we have combined them in a senseless and convoluted manner: the parts of speech are not in their correct positions for English grammar.

Syntax constraint error

These errors occur when the Java compiler cannot determine the meaning of a program. Sometimes a sentence might seem syntactically correct but, meaningless; for example, "Colorless green ideas sleep furiously." Suppose that we told the motorist, "Keep going for eight hundred just miles." Technically, this sentence is syntactically correct: we can use the word "just" an adjective meaning *righteous* —as in the sentence, "He is a just man." But while the phrase "just man" is meaningful, the phrase "just miles" is meaningless. So once again, the motorist would not be able to understand fully what we told him.

If a program contains any token, syntactic, or syntax constraint errors, the Java compiler will discover them. In all three cases, the Java compiler has no idea of what we meant to say, so it will not try to correct the error; it will simply report the problem (as best as it can) in the Errors & Warnings window and be unable to finish compiling the program.
All these errors are called **compile-time** errors, because the Java compiler detects them while

compiling our programs. We can link and run only programs that contain no compile-time errors. Errors that occur when the program is running (or executing) are called **run-time** errors. Since the compiler points out compile-time errors, they are much easier to fix.

Execution error

Execution errors occur when the Java runtime system is executing a program and discover that it can't legally carry out one of our instructions (for example, dividing by 0). If it recognizes such a case, it terminates execution of the program (again, supplying some information about the error). Returning to our motorist trying to get from San Francisco to Portland, we might tell him to, "Just keep going for eight hundred miles". But, if he happens to be facing west at the time, and interprets our instructions literally, he could travel only a few miles before reaching the Pacific Ocean. At this point he would stop (we hope) and realize that he could not complete our instructions as given. This illustrates an execution error.

Execution errors are often called run-time errors, because the Java runtime system can detect them only when it tries to execute or run a program.

Intent error

The final error class is the most insidious, because neither the Java compiler or runtime system can detect this type of error when it occurs. An intent error occurs whenever Java successfully completes execution of a program, but the program doesn't compute the correct answer. Coming back to our motorist who is trying to reach Portland from San Francisco; we could again tell him, "Just keep going for eight hundred miles." But if this time he happened to be facing south, he could successfully carry out our instructions to completion, but he would end up in Tijuana, Mexico not Portland, Oregon.

Remember that Java understands either our programs or what we indended to do with them. It knows only how to compile, link and execute the instructions that we give it. There is no way for Java to know what we intend the program to do, or detect that our program did not accomplish what we intended it to do.

Frequently, intent errors occur early in our programs and then later lead to execution errors. In such cases, the error becomes manifest at a location that is different than the source of the error. Thus, we must carefully hand simulate our programs, either from the beginning, or backward from the execution error or end of the program, to locate the incorrect instructions.

Example of Bug: TYPE - Accidental

```
for (i=0; i<numrows; i++)
  for (j=0; j<numcols; j++);
    pixels++;
```

Commentary: Caused by a stray ";" on line 2. Accidental bugs are often caused by stray characters, etc. While "minor" in their fix, they can be the devil to find!

Cybercrime & Cyber terrorism

"Cyberterrorism is also clearly an emerging threat. Terrorist groups are increasingly computer savvy, and some probably are acquiring the ability to use cyber attacks to inflict isolated and brief disruptions of US infrastructure. Due to the prevalence of publicly available hacker tools, many of these groups probably already have the capability to launch denial-of-service and other nuisance attacks against Internet-connected systems. As terrorists become more computer savvy, their attack options will only increase." (*War on Terrorism*, 2003)

As the global reach of the Internet keeps growing, its effect on all areas of online human endeavour becomes more pervasive. Individuals or groups can exploit the anonymity afforded by cyberspace to engage in illegal or illicit activities that aim to intimidate, harm, threaten or cause fear to citizens, communities, organizations or countries. The virtual and physical distance between the attacker and the victim and the difficulty in tracing back the attack to an individual minimizes the inherent threat of capture to the attacker. But how are such activities defined? What is a Cybercrime and what are its characteristics? How can a Cyberterrorist be identified and what are his or her differences from a Cybercriminal? So far, the definitions for Cybercrime and Cyberterrorism in literature, government documents and everyday use have been highly varied, context-specific and emotionally loaded, which makes discourse on the subject difficult. The FBI alone has published three distinct definitions of Cyberterrorism: "Terrorism that initiates…attack[s] on information" in 1999, to "the use of Cyber tools" in 2000 and "a criminal act perpetrated by the use of computers" in 2004." (Baranetsky, 2009). Cybercrime and Cyberterrorism have been used to describe online acts such as:

- Black-hat hacking / Cracking
- Child sex offences (pornography and grooming)
- Crimes in virtual worlds
- Cyberactivism / Hacktivism
- Virus writing and malware
- Cyberstalking
- Identity theft / Fraud
- Illegal financial transactions / Money laundering
- Copyright infringement
- Serious acts of cyberbullying
- Denial of service attacks
- Rogue bot-nets

Digital signature

A digital signature (not to be confused with a digital certificate) is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

In many countries, including the United States, digital signatures have the same legal significance as the more traditional forms of signed documents. The United States Government Printing Office publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures.

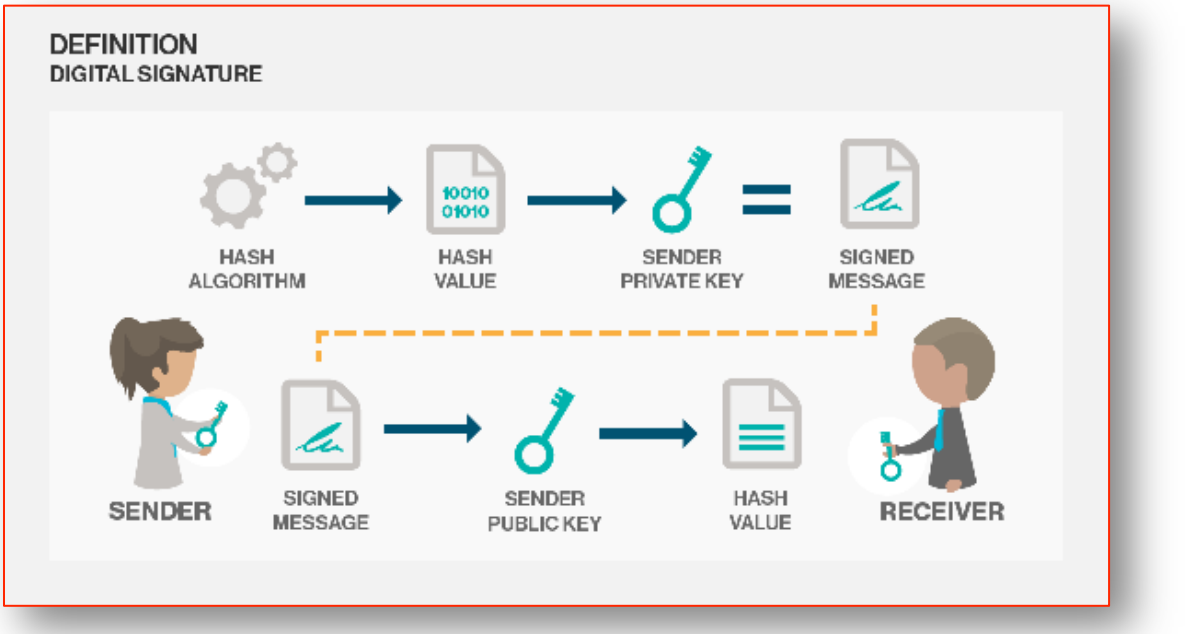
How digital signatures work

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

The value of the hash is unique to the hashed data. Any change in the data, even changing or deleting a single character, results in a different value. This attribute enables others to validate the integrity of the data by using the signer's public key to decrypt the hash. If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. If the two hashes don't match, the data has either been tampered with in some way (integrity) or the signature was created with a private key that doesn't correspond to the public key presented by the signer (authentication).

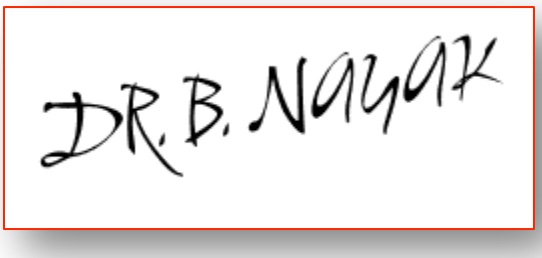
A digital signature can be used with any kind of message -- whether it is encrypted or not -- simply so the receiver can be sure of the sender's identity and that the message arrived intact. Digital signatures make it difficult for the signer to deny having signed something (non-repudiation) -- assuming their private key has not been compromised -- as the digital signature is unique to both the document and the signer, and it binds them together. A digital certificate, an electronic document that contains the digital signature of the certificate-issuing authority, binds together a public key with an identity and can be used to verify a public key belongs to a particular person or entity.

Example of Digital Signature Process



Most modern email programs support the use of digital signatures and digital certificates, making it easy to sign any outgoing emails and validate digitally signed incoming messages. Digital signatures are also used extensively to provide proof of authenticity, data integrity and non-repudiation of communications and transactions conducted over the Internet.

Example of Digital Signature



Public Key Infrastructure

A **public key infrastructure** (**PKI**) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage **public-key** encryption. Without PKI, sensitive information can still be encrypted (ensuring confidentiality) and exchanged, but there would be no assurance of the identity (authentication) of the other party. Any form of sensitive data exchanged over the Internet is reliant on PKI for security.

Elements of PKI

A typical PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates. Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate.

A typical PKI includes the following key elements:

- A trusted party, called a certificate authority (CA), acts as the root of trust and provides services that authenticate the identity of individuals, computers and other entities
- A registration authority, often called a subordinate CA, certified by a root CA to issue certificates for specific uses permitted by the root
- A certificate database, which stores certificate requests and issues and revokes certificates
- A certificate store, which resides on a local computer as a place to store issued certificates and private keys

A CA issues digital certificates to entities and individuals after verifying their identity. It signs these certificates using its private key; its public key is made available to all interested parties in a self-signed CA certificate. CAs used this trusted root certificate to create a "chain of trust" -- many root certificates are embedded in Web browsers so they have built-in trust of those CAs. Web servers, email clients, smartphones and many other types of hardware and software also support PKI and contain trusted root certificates from the major CAs.

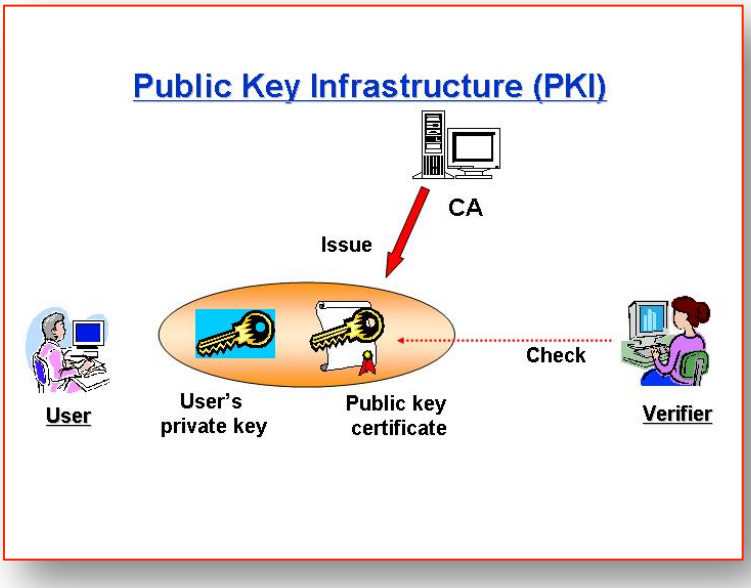
Along with an entity's or individual's public key, digital certificates contain information about the algorithm used to create the signature, the person or entity identified, the digital signature of the CA that verified the subject data and issued the certificate, the purpose of the public key encryption, signature and certificate signing, as well as a date range during which the certificate can be considered valid.

Problems with PKI

PKI provides a chain of trust, so that identities on a network can be verified. However, like any chain, a PKI is only as strong as its weakest link. There are various standards that cover aspects of PKI -- such as the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC2527) -- but there is no predominant governing body enforcing these standards. Although a CA is often referred to as a "trusted third party," shortcomings in the security procedures of various CAs in recent years has jeopardized trust in the entire PKI on which the Internet depends. If one CA is compromised, the security of the entire PKI is at risk.

In the real world, people use ID cards such as a driver's license, passport, or an employee ID badge to prove their identity. A certificate does the same basic thing in the electronic world, but with one big difference. Certificates are not just issued to people (users, administrators, etc.). Certificates can also be issued to computers, software packages, or to just about anything else that you may need to prove the identity.

Example: Public Key Infrastructure



Application of Cryptography

Authentication and digital signatures are a very important application of public-key cryptography. The only requirement is that public keys are associated with their users by a trusted manner, for example a trusted directory.

There are some applications of Cyptography.

Time Stamping

Time stamping is a technique that can certify that a certain electronic document or communication existed or was delivered at a certain time. Time stamping uses an encryption model called a blind signature scheme. Blind signature schemes allow the sender to get a message receipted by another party without revealing any information about the message to the other party.

Time stamping is very similar to sending a registered letter through mail, but provides an additional level of proof. It can prove that a recipient received a specific document. Possible applications include patent applications, copyright archives, and contracts. Time stamping is a critical application that will help make the transition to electronic legal documents possible.

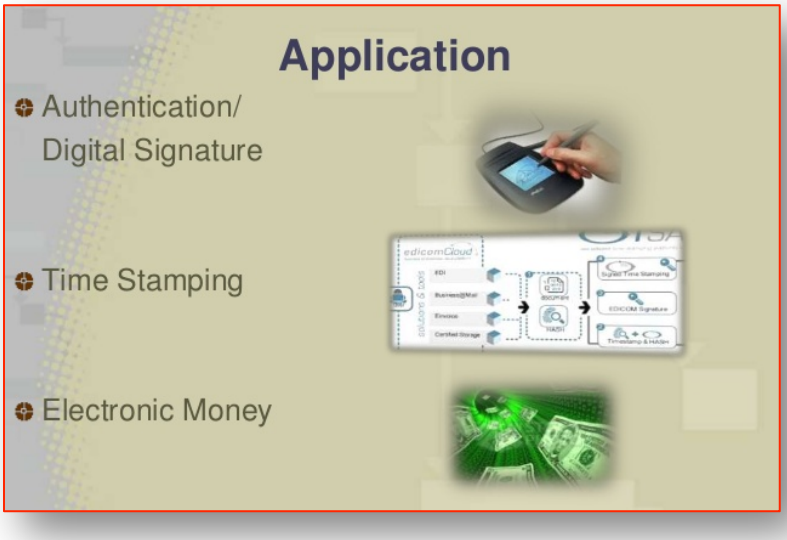
Electronic Money

The definition of electronic money (also called electronic cash or digital cash) is a term that is still evolving. It includes transactions carried out electronically with a net transfer of funds from one party to another, which may be either debit or credit and can be either anonymous or identified. There are both hardware and software implementations.

Anonymous applications do not reveal the identity of the customer and are based on blind signature schemes. (Digicash's Ecash) Identified spending schemes reveal the identity of the customer and are

based on more general forms of signature schemes. Anonymous schemes are the electronic analog of cash, while identified schemes are the electronic analog of a debit or credit card. There are also some hybrid approaches where payments can be anonymous with respect to the merchant but not the bank (CyberCash credit card transactions); or anonymous to everyone, but traceable (a sequence of purchases can be related, but not linked directly to the spender's identity).

Encryption is used in electronic money schemes to protect conventional transaction data like account numbers and transaction amounts, digital signatures can replace handwritten signatures or a credit-card authorizations, and public-key encryption can provide confidentiality. There are several systems that cover this range of applications, from transactions mimicking conventional paper transactions with values of several dollars and up, to various micropayment schemes that batch extremely low cost transactions into amounts that will bear the overhead of encryption and clearing the bank.

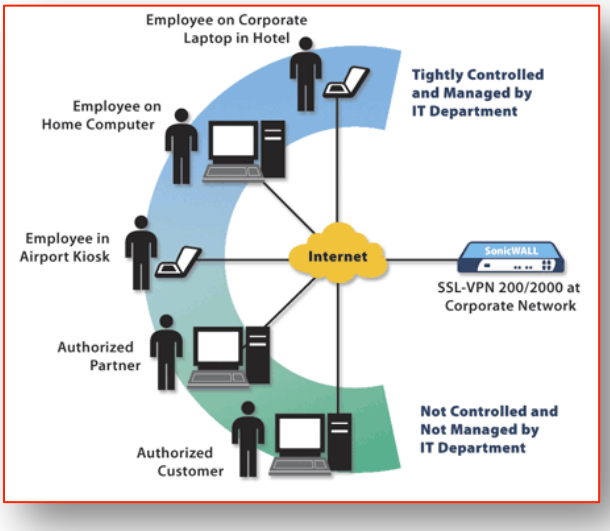


Secure Network Communications

Secure Socket Layer (SSL) Netscape has developed a public-key protocol called Secure Socket Layer (SSL) for providing data security layered between TCP/IP (the foundation of Internet-based communications) and application protocols (such as HTTP, Telnet, NNTP, or FTP). SSL supports data encryption, server authentication, message integrity, and client authentication for TCP/IP connections.

The SSL Handshake Protocol authenticates each end of the connection (server and client), with the second or client authentication being optional. In phase 1, the client requests the server's certificate and its cipher preferences. When the client receives this information, it generates a master key and encrypts it with the server's public key, then sends the encrypted master key to the server. The server decrypts the master key with its private key, then authenticates itself to the client by returning a message encrypted with the master key. Following data is encrypted with keys derived from the master key. Phase 2, client authentication, is optional. The server challenges the client, and the client responds by returning the client's digital signature on the challenge with its public-key certificate.

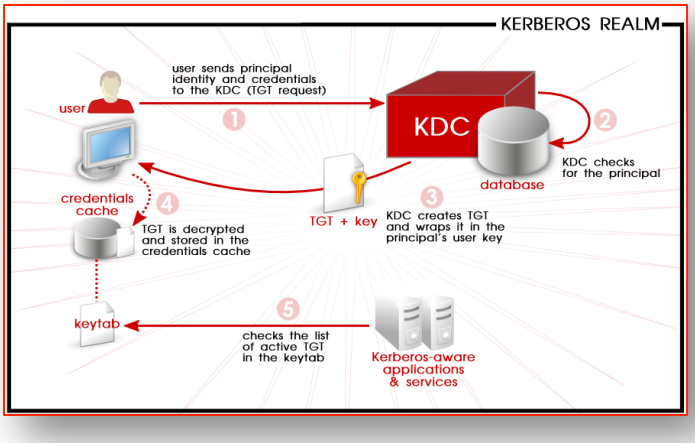
Secure Network Communications



Kerberos

Kerberos is an authentication service developed by MIT which uses secret-key ciphers for encryption and authentication. Kerberos was designed to authenticate requests for network resources and does not authenticate authorship of documents.

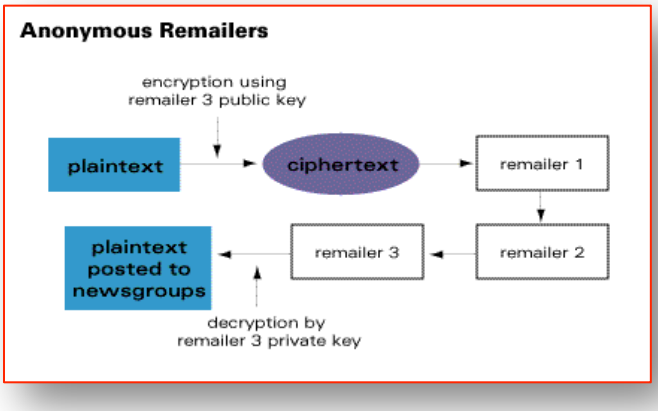
In a Kerberos system, there is a site on the network, called the Kerberos server, to perform centralized key management and administrative functions. The server maintains a key database with the secret keys of all users, authenticates the identities of users, and distributes session keys to users and servers who need to authenticate one another. Kerberos depends on a trusted third party, the Kerberos server, and if the server were compromised, the integrity of the whole system would be lost. Kerberos is generally used within an administrative domain (for example across a companies closed network); across domains (e.g., the Internet), the more robust functions and properties of public-key systems are often preferred.



Anonymous Remailers

A remailer is a free service that strips off the header information from an electronic message and passes along only the content. It's important to note that the remailer may retain your identity, and rather than trusting the operator, many users may relay their message through several anonymous remailers before sending it to its intended recipient. That way only the first remailer has your identity, and from the end point, it's nearly impossible to retrace.

Here's a typical scenario - the sender intends to post a message to a news group via three remailers (remailer 1, remailer 2, remailer 3). He encrypts the message with the last remailer's (remailer 3's) public key. He sends the encrypted message to remailer 1, which strips away his identity, then forwards it to remailer 2, which forwards it to remailer 3. Remailer 3 decrypts the message and then posts it to the intended newsgroup.



Networking Advanced

Network Security

Identification and Authorization

Authentication, authorization is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. As the first process, authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials are at variance, authentication fails and network access is denied.

Following authentication, a user must gain authorization for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.

The final plank in the framework is accounting, which measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

Example: Identification and Authorization

Intrusion Detection Systems

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways

Intrusion Detection
Systems

Secure your organization's assets and inventory

This is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses *vulnerability assessment* (sometimes refered to as *scanning*), which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming ever more sophisticated; at the same time, less technical ability is required for the novice attacker, because proven past methods are easily accessed through the Web.

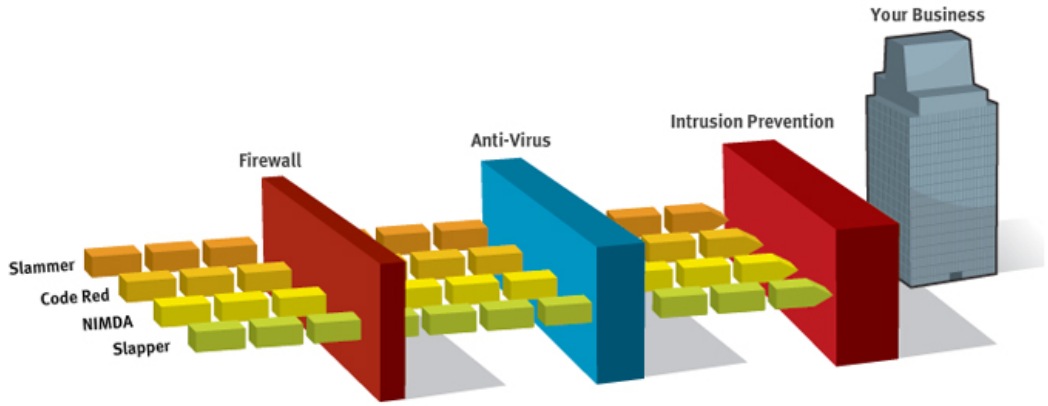
Typically, an ID system follows a two-step process. The first procedures are host-based and are considered the *passive* component, these include: inspection of the system's configuration files to detect inadvisable settings; inspection of the password files to detect inadvisable passwords; and inspection of other system areas to detect policy violations. The second procedures are network-based and are considered the *active* component: mechanisms are set in place to reenact known methods of attack and to record system responses.

Intrusion Prevention Systems

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. Intrusion prevention is a preemptive approach to network security used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) monitors network traffic. However, because an exploit may be carried out very quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the network administrator. For example, an IPS might drop a packet that it determines to be malicious and block all further traffic from that IP address or port. Legitimate traffic, meanwhile, should be forwarded to the recipient with no apparent disruption or delay of service.

According to Michael Reed of Top Layer Networks, an effective intrusion prevention system should also perform more complex monitoring and analysis, such as watching and responding to traffic patterns as well as individual packets. "Detection mechanisms can include address matching, HTTP string and substring matching, generic pattern matching, TCP connection analysis, packet anomaly detection, traffic anomaly detection and TCP/UDP port matching."

Broadly speaking, an intrusion prevention system can be said to include any product or practice used to keep attackers from gaining access to your network, such as firewalls and anti-virus software.



Intrusion prevention system

Server Management and Firewalls

User Management

The User Management service enables to create and manage login credentials for each user. It can also limit the merchant accounts that each user can access, together with the available functionality. Only one username and password is required to access all applications that are available to the user. It can control.

Example

- The applications a user can access
- Whether access is read-only
- If a user can update information
- The features a user can access within the Merchant Interface, if applicable
- The merchant codes that each user can access, if it have multiple accounts

User Management

- Contributes to the overall security of your business
- Makes it easier for your users to access the pages they need
- Simplifies deployment of our services within your organisation

For example, accounting staff need access to the parts of the Merchant Interface that are used to manage payments, while system administrators want to configure the way in which the payment services work.

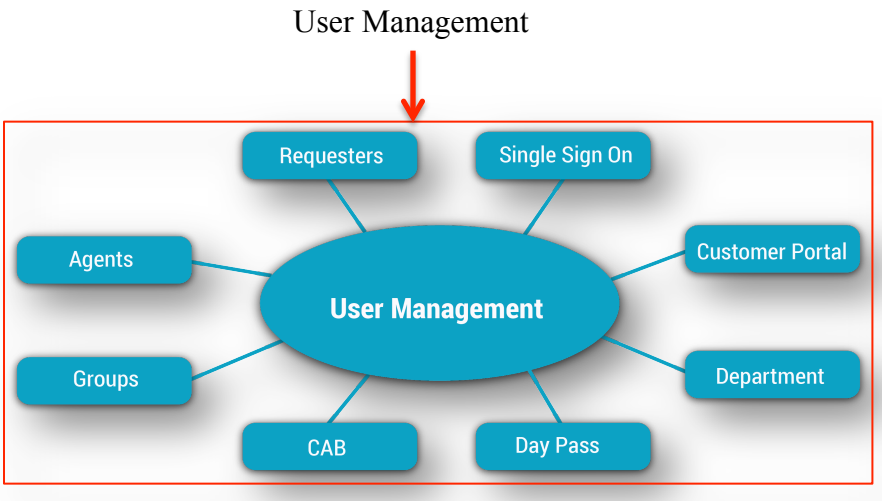
Users and the User Profile

The details about each user of the Merchant Interface (MAI) are stored in a user-profile which is created initially either by the Administrator or by a user the Administrator has created and assigned the user management role.

The user profile contains:

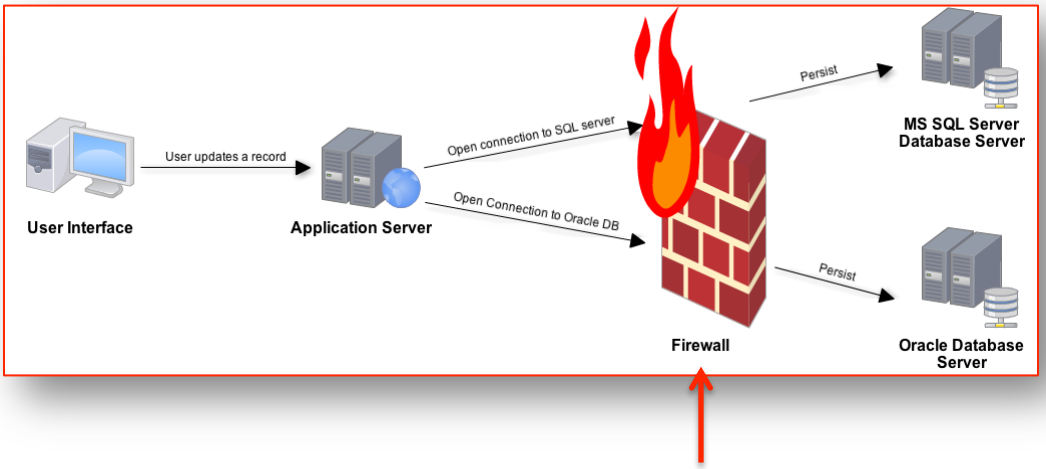
- Login credentials - the user-name and password that enable a user to login to the MAI
- Assigned roles - a list of the roles assigned to them and the roles not assigned to them
- Assigned merchant codes - a list of the merchant codes (accounts) to which they have access and those they do not identity data - the user's email address and a challenge question and associated response, both used to help manage their user profile and help validate the identity of the user when they change their user-name or password.

All of the details in the user profile can be updated by the user, which will created it and all of the details, except for the assigning of roles and accounts, can be updated by the user for whom it was created. This means that a user can change the user-name and password issued to them, for example, to make them easier to remember, without having to refer to the person that created their profile.



Overview of Firewall

A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules. Acting as a barrier between a trusted network and other untrusted networks, such as the Internet or less trusted networks, and such as a retail merchant's network outside of a cardholder data environment. A firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network defined in the firewall policy is all other traffic is denied.



History and types of firewalls

Computer security borrowed the term firewall from firefighting and fire prevention, where a firewall is a barrier established to prevent the spread of fire. When organizations began moving from mainframe computers and dumb clients to the client-server model, the ability to control access to the server became a priority. Before firewalls emerged in the late 1980s, the only real form of network security was performed by access control lists (ACLs) residing on routers. ACLs determined which IP addresses were granted or denied access to the network.

The growth of the Internet and the resulting increased connectivity of networks meant that this type of filtering was no longer enough to keep out malicious traffic as only basic information about network traffic is contained in the packet headers. Digital Equipment Corp. shipped the first commercial firewall, DEC SEAL, in 1992, and firewall technology has since evolved to combat the increasing sophistication of cyber attacks.

Packet firewalls

The earliest firewalls functioned as packet filters, inspecting the packets that are transferred between computers on the Internet. When a packet passes through a packet-filter firewall, its source and destination address, protocol, and destination port number are checked against the firewall's rule set. Any packets that aren't specifically allowed onto the network are dropped (i.e., not forwarded to their destination). For example, if a firewall is configured with a rule to block Telnet access, then the firewall will drop packets destined for TCP port number 23, the port where a Telnet server application would be listening.
Packet-filter firewalls work mainly on the first three layers of the OSI reference model (physical, data-link and network), although the transport layer is used to obtain the source and destination port numbers. While generally fast and efficient, they have no ability to tell whether a packet is part of an existing stream of traffic. Because they treat each packet in isolation, this makes them vulnerable to spoofing attacks and also limits their ability to make more complex decisions based on what stage communications between hosts are at.

Stateful firewalls

In order to recognize a packet's connection state, a firewall needs to record all connections passing through it to ensure it has enough information to assess whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection. This is what's called "stateful packet inspection." Stateful inspection was first introduced in 1994 by Check Point Software in its FireWall-1 software firewall, and by the late 1990s. It was a common firewall product feature.

This additional information can be used to grant or reject access based on the packet's history in the state table, and to speed up packet processing; that way, packets that are part of an existing connection based on the firewall's state table can be allowed through without further analysis. If a packet does not match an existing connection, it's evaluated according to the rule set for new connections.

Application-layer firewalls

As attacks against Web servers became more common, so too did the need for a firewall that could protect servers and the applications running on them, not merely the network resources behind them. Application-layer firewall technology first emerged in 1999, enabling firewalls to inspect and filter packets on any OSI layer up to the application layer.

The key benefit of application-layer filtering is the ability to block specific content, such as known malware or certain websites, and recognize when certain applications and protocols, such as HTTP, FTP and DNS are being misused.

Firewall technology is now incorporated into a variety of devices; many routers that pass data between networks contain firewall components and most home computer operating systems include software-based firewalls. Many hardware-based firewalls also provide additional functionality like

basic routing to the internal network they protect.

Proxy firewalls

Firewall proxy servers also operate at the firewall's application layer, acting as an intermediary for requests from one network to another for a specific network application. A proxy firewall prevents direct connections between either sides of the firewall; both sides are forced to conduct the session through the proxy, which can block or allow traffic based on its rule set. A proxy service must be run for each type of Internet application the firewall will support, such as an HTTP proxy for Web services.

Firewalls in the perimeter less age

The role of a firewall is to prevent malicious traffic reaching the resources that it is protecting. Some security experts feel this is an outdated approach to keeping information and the resources it resides on safe. They argue that while firewalls still have a role to play, modern networks have so many entry points and different types of users that stronger access control and security at the host is a better technological approach to network security.

Virtualization strategies such as virtual desktop infrastructure can dynamically respond to different scenarios by offering tailored access control to applications, files, Web content and email attachments based on the user's role, location, device and connection. This approach to security does provide additional protection that a firewall can't, but information security requires defense-in-depth, and firewalls still offer essential low-level protection as well as important logging and auditing functions.

Firewall DMZ Zone

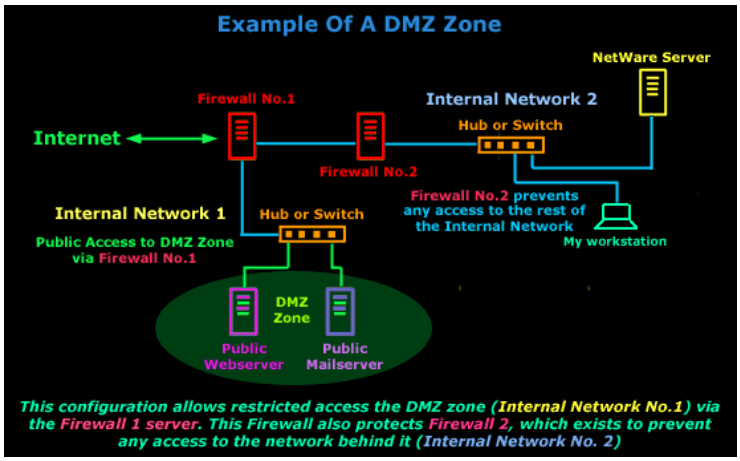
The De-Militarized Zone, or DMZ, is an expression that comes from the Korean War. There, it meant a strip of land forcibly kept clear of enemy soldiers. The idea was to accomplish this without risking your own soldiers' lives, thus mines were scattered throughout the DMZ like grated Romano on a plate of fettuccine. The term has been assimilated into the networking world, without the cheese.

Another meaning to the term DMZ Zone is *a portion of your network, which although under your control, is outside your heaviest security*. Compared to the rest of your network, machines you place in the DMZ are less protected, or flat-out unprotected, from the Internet.

Once a machine has entered the DMZ, it should not be brought back inside the network again. Assuming that it has been compromised in some way, bringing it back into the network is a big security hazard.

Use of the DMZ

If you decide to build one, what do you do with it? Machines placed in the DMZ usually offer services to the general public, like Web services, domain name services (DNS), mail relaying and FTP services (all these buzzwords will be explained next). Proxy servers can also go in the DMZ. If you decide to allow your users Web access only via a proxy server, you can put the proxy in the firewall and set your firewall rules to permit outgoing access only to the proxy server.



DMZ Zone

References:

http://www.functionx.com
http://www.techcricklets.com
http://searchsecurity.techtarget.com
https://www.cs.cmu.edu

Books:

1. Cyber Threat, by MacDonnell Ulsch, Wiley Publication
2. Computer Security - ESORICS 2013,
   By Jason Crampton, Sushil Jajodia, Keith Mayes, Springer Publication