

Computer Security and Privacy

Avinash Maskey

Introduction

- As discussed earlier, networks and the internet help many of us be more efficient and effective workers, as well as add convenience and enjoyment to our personal lives.
- However, there is a downside, as well. The widespread use of home and business networks and the internet increases the risk of *unauthorized computer access, theft, fraud*, and *other types of computer crime*.
- In addition, the vast amount of business and personal data stored on computers accessible via company networks and the internet increases the chances of *data loss due to crime* or *employee errors*. Some online activities can even put your personal safety at risk, if you are not careful.
- This chapter looks at a variety of security concerns stemming from the use of computer networks and the internet in our society, including *unauthorized access and use, computer viruses* and *other types of sabotage*, and *online theft and fraud*.
- Safeguards for each of these concerns are also covered, with an explanation of precautions that can be taken to reduce the chance that these security problems will happen to you. Personal safety issues related to the Internet are also discussed.

Why be Concerned about network and internet security?

- From a computer virus making your computer *function abnormally*, to a hacker using your personal information to make *fraudulent purchases*, to *someone harassing you online* in a discussion group, a variety of security concerns related to computer networks and the Internet exist.
- Many Internet security concerns today can be categorized as computer crimes. **Computer Crime**—sometimes referred to as **Cyber Crime**—includes any illegal act involving a computer.
- Many computer crimes today are committed using the internet or another computer network and include *theft of financial assets or information, manipulating data (such as grades or account information)*, and acts of *sabotage (such as releasing a computer virus or shutting down a Web server)*.
- **Cybercrime** is an important security concern today. It is a multibillion-dollar business that is often performed by seasoned criminals.
- In fact, according to the FBI, organized crime organizations in many countries are increasingly turning to computer crime to target millions of potential victims easily, and phishing attacks and other internet scams are expected to increase in reaction to the recent troubled economy.

Computer Security

- The terms *computer security*, *information security*, *network security* are frequently used interchangeably.
- *Computer security* basically is the protection of computer systems and information from harm, theft, unauthorized access, modification or destruction. It is the process of preventing and detecting unauthorized use of computer system.
- *Information security* means protecting information and information systems from unauthorized access, use, modification or destruction.
- *Network security* is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification ,thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment over computer networks.

Objectives of Computer Security

- **Information Security** programs are built around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.
 - **Confidentiality:**
means information is not disclosed to unauthorized individuals, entities and process. **For example**, if we say I have a password for my Gmail account but someone saw while I was login into a Gmail account. In that case my password has been compromised and Confidentiality has been breached.
 - **Integrity:**
means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. **For example**, if an employee leaves an organization then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.

Objectives of Computer Security

- **Availability:**

means information must be available when needed. **For example**, if one needs to access information of a particular employee to check whether employee has outstanding the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management. *Denial of service* attack is one of the factors that can hamper the availability of information.



Security Control

- *Security controls* are parameters implemented to protect various forms of data and infrastructure important to an organization.
- Any type of safeguard or countermeasure used to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets is considered a security control.

Types of Security Controls

- There are several types of security controls that can be implemented to protect hardware, software, networks, and data from actions and events that could cause loss or damage.
- For example:
 - **Physical security controls:** include such things as data center perimeter fencing, locks, guards, access control cards, biometric access control systems, surveillance cameras, and intrusion detection sensors.
 - **Digital security controls:** include such things as usernames and passwords, two-factor authentication, antivirus software, and firewalls.
 - **Cyber security controls:** include anything specifically designed to prevent attacks on data, including DDoS mitigation, and intrusion prevention systems.
 - **Cloud security controls:** include measures you take in cooperation with a cloud services provider to ensure the necessary protection for data and workloads. If your organization runs workloads on the cloud, you must meet their corporate or business policy security requirements and industry regulations.

Unauthorized Access (UA) and Unauthorized Use (UU)

- *Unauthorized access* occurs whenever an individual gains access to a computer, mobile device, network, file, or other resource without permission—typically by hacking into the resource.
- *Unauthorized use* involves using a computing resource for unauthorized activities. Often, they happen at the same time, but unauthorized use can occur when a user is authorized to access a particular computer or network but is not authorized for the particular activity the user performs.
- For instance employees of some companies may be prohibited for checking personal e-mail or visiting personal Facebook pages at work might be classified as unauthorized use.
- *Authentication* and *Authorization* is used to safeguard against unauthorized access and unauthorized use.

Examples of UA and UU

- **Hacking:**

Hacking refers to the act of breaking into a computer or network. It can be performed in person by hacking into a computer the hacker has physical access to, but it is more often performed via the Internet or another network. Unless authorized (such as when a company hires a professional hacker to test the security of its system), hacking in the United States and many other countries is a crime.

- **War Driving and Wi-Fi Piggybacking:**

Unauthorized use of a Wi-Fi network is called *war driving* or *Wi-Fi piggybacking*, depending on the location of the hacker at the time. *War driving* typically involves driving in a car with a portable device looking for unsecured Wi-Fi networks to connect to. *Wi-Fi piggybacking* refers to accessing someone else's unsecured Wi-Fi network from the hacker's current location (such as inside his or her home, outside a Wi-Fi hotspot location, or near a local business). Both war driving and Wi-Fi piggybacking are ethically—if not legally—questionable acts.

Examples of UA and UU

- **Interception of Communications:**

- Instead of accessing data stored on a computer via hacking, some criminals gain unauthorized access to data, files, messages, VoIP calls, and other content as it is being sent over the Internet. For instance, unencrypted (unsecured) messages, files, logon information, and more sent over a wireless network (such as while using a public Wi-Fi hotspot or over an unsecured home or business Wi-Fi network) can be captured and read by anyone within range using software designed for that purpose. Once intercepted, the data can be used for unintended or fraudulent purposes.
- A relatively recent trend is criminals intercepting credit and debit card information during the card verification process; that is, intercepting the data from a card in real time as a purchase is being authorized. Often, this occurs via *packetsniffing software* installed at payment terminals (such as restaurant cash registers or gas station credit/debit card readers) by hackers—the packetsniffing software gathers data during transactions and then sends it to the hackers, who may then use it for fraudulent purposes.

Protecting Against Unauthorized Access And Unauthorized Use

Introduction

- The first step in protecting against unauthorized access and unauthorized use of a computer system is *controlling access to an organization's facilities and computer networks* to ensure that only authorized individuals are granted access.
- In addition, steps need to be taken to ensure that authorized individuals access only the resources that they are supposed to access.

Access Control Systems

- *Access control systems* are used to control access to facilities, devices, computer networks, company databases, Web site accounts, and other assets.
- They can be *identification systems (IDS)*, which verify that the person trying to access the facility or system is listed as an authorized user, and/or authentication systems, which determine whether or not the person attempting access is actually who he or she claims to be.
- *In businesses*, access control systems are often integrated into a comprehensive *identity management (IDM) system* designed to manage users' access to enterprise systems, such as to grant them secure and appropriate access to the systems they are allowed to access in as convenient a manner as possible.
- An emerging trend is to use **single sign on (SSO)** systems that grant employees access to a number of secure resources with a single authentication.
- The *three most common types of access control systems* are discussed next.

TIP



To prevent a hacker from obtaining your logon info from an unused (*zombie*) online account, delete your old accounts if you are no longer going to use them.

Access Control Systems - Possessed Knowledge Access Systems

- A *possessed knowledge access system* is an identification system that requires the individual requesting access to provide information that only the authorized user is supposed to know. *Passwords and cognitive* authentication systems fall into this category.
- *Passwords*, the most common type of possessed knowledge, are secret words or character combinations associated with an individual. They are typically used in conjunction with a username (often a variation of the person's first and/or last names or the individual's e-mail address).
- For some applications (such as ATM machines), a PIN or personal identification number—a secret combination of numeric digits selected by the user—is used instead of a password. Numeric passwords are also referred to as passcodes.
- One of the *biggest disadvantages of password-based systems* is that any individual possessing the proper password will be granted access to the system because the system recognizes the password, regardless of whether or not the person using the password is the authorized user, and passwords can be guessed or deciphered by a hacker or a hacker's computer easily if secure password selection strategies are not applied.

Password Strategies

Make the password at least eight characters and include both uppercase and lowercase letters, as well as numbers and special symbols.

Choose passwords that are not in a dictionary—for instance, mix numbers and special characters with abbreviations or unusual words you will remember but that do not conform to a pattern a computer can readily figure out.

Do not use your name, your kids' or pets' names, your address, your birthdate, or any other public information as your password.

Determine a *passphrase* that you can remember and use corresponding letters and symbols (such as the first letter of each word) for your password. For instance, the passphrase “My son John is five years older than my daughter Abby” could be used to remember the corresponding strong password “Msji5yotMd@”.

Develop a system using a basic password for all Web sites plus site-specific information (such as the first two letters of the site and a number you will remember) to create a different password for each site, but still ones you can easily remember. For instance, you can combine your dog's name with the site initials followed by a number that is significant to you to form a password such as “RoverAM27” for Amazon.com.

Do not keep a written copy of the password in your desk or taped to your monitor. If you need to write down your password, create a password-protected file on your computer that contains all your passwords or use a password manager program.

Use a different password for your highly sensitive activities (such as online banking or stock trading) than for other Web sites. If a hacker determines your password on a low-security site (which is easier to break into), he or she can use it on an account containing sensitive data if you use the same password on both accounts.

Change your passwords frequently—at least every 6 months.

Access Control Systems - Possessed Knowledge Access Systems

- A growing trend in possessed knowledge access systems is the use of *cognitive authentication systems* instead of, or in conjunction with, usernames and passwords.
- Cognitive authentication systems use information that an individual should know or can remember easily. Some systems use personal information about the individual (such as his or her city of birth, first school attended, or amount of home mortgage) that was pulled from public databases or the company database and the individual must supply the correct answer in order to be granted access.
- Other systems (such as the password recovery systems used by many secure Web sites to verify individuals when they forget their password) allow the individual to supply answers to questions when the account is created and then the individual can supply those answers again for authentication purposes when needed.
- Possessed knowledge systems are often used in conjunction with the possessed object access systems and biometric access systems that are discussed next. Using two different methods to authenticate a user is called two-factor authentication. Typically, the methods used are some type of *possessed knowledge (something you know)* along with either a *possessed object (something you have)* or a *biometric feature (something you are)*.

Access Control Systems - Possessed Knowledge Access Systems

Fig: Password Security

I'm A Current Online Customer

Email Address

Password:
(Password is case sensitive.)

Fig: Facebook Two Factor Authentication

90 11:17

Code Generator

342116

A new security code will appear every 30 seconds.

1. An OTP is sent to your phone.

2. Enter that code here when prompted.

facebook Log Out

Enter Security Code to Continue

It looks like you haven't logged in from this browser before. Please enter the security code from your Code Generator app.

Having trouble?

Mobile Find Friends Badges People Pages Places Apps Games Music
About Create Ad Create Page Developers Careers Privacy Cookies Terms Help

Facebook © 2013 - English (US)

Access Control Systems - Possessed Object Access Systems

- *Possessed object access systems* use physical objects for identification purposes and they are frequently used to control access to facilities (**called physical access**) and computer systems (**called logical access**).
- Common types of possessed objects are *smart cards*, *RFID-encoded badges*, *magnetic cards*, and *smartphones that are swiped through* or *placed close to a reader to be read* (see Figure)



PHYSICAL ACCESS

The object (in this case a mobile phone containing an appropriate microSD card) is read by a reader to provide access to a facility.



LOGICAL ACCESS

The object (in this case a smart card employee badge) is read by a reader (this reader is integrated into the computer) to provide access to that computer system.

Access Control Systems - Possessed Object Access Systems

- *Possessed objects* also include USB security keys or tokens (USB flash drives that are inserted into a computer to grant access to a network, to supply Web site usernames and passwords, or to provide other security features), access cards, smartphones, and other devices used to supply the OTPs used to log on to Web sites.
- An emerging option is integrating OTP capabilities into the hardware of devices, such as laptops that include *Intel Identity Protection Technology (IPT)*, in order to automatically authenticate the devices being used to log on to participating Web sites.
- *One disadvantage of using possessed objects* is that they can be lost or, like passwords, can be used by an unauthorized individual if that individual has possession of the object.
- *This disadvantage can be overcome* by using a second factor, such as a username/password combination or a fingerprint or other type of biometric data.

Access Control Systems - Biometric Access Systems

- ***Biometrics*** is the study of identifying individuals using measurable, unique physiological or behavioral characteristics.
- Biometric access systems typically identify users by a particular unique biological characteristic (such as a ***fingerprint, a hand, a face, veins, or an iris***), although personal traits are used in some systems.
- ***For instance***, some systems today use ***keystroke dynamics*** to recognize an individual's unique typing pattern to authenticate the user as he or she types in his or her username and password; other systems identify an individual via his or her voice, signature, or gait.
- ***To identify and authenticate an individual***, biometric access systems typically use a biometric reader (such as a fingerprint reader, finger or palm vein reader, or a hand geometry reader) to identify an individual based on his or her fingerprint, veins, or hand image, or a digital camera to identify an individual based on his or her face or iris, in conjunction with software and a database.

Access Control Systems - Biometric Access Systems



Courtesy Gérard Voulton/Morpho/Safar

FINGERPRINT READERS

Typically used to protect access to work facilities or computers, to log on to secure Web sites, for law enforcement identification, and to pay for products or services.



VEIN READERS

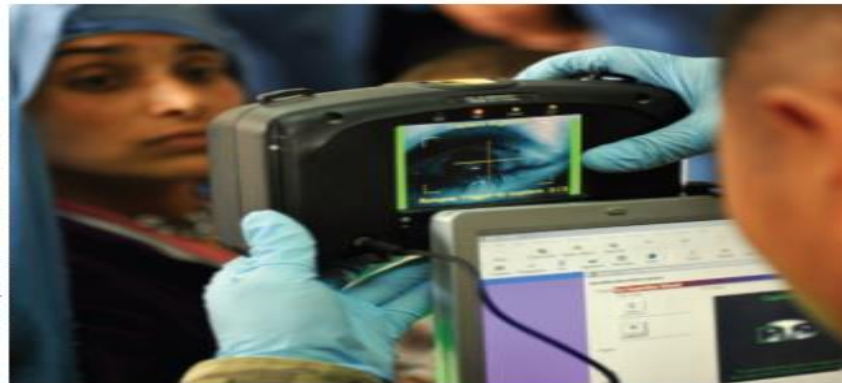
Beginning to replace hand geometry readers to control access to facilities (such as government offices, prisons, and military facilities) and to punch in and out of work.



U.S. Air Force photo/Senior Airman Chris Willis

FACE RECOGNITION SYSTEMS

Typically used to control access to highly secure areas, to identify individuals for law enforcement purposes, and to log on to devices or apps, as shown here.



IRIS RECOGNITION SYSTEMS

Typically used to control access to highly secure areas and by the military, such as to identify Afghan patients as shown here.

Access Control Systems - Controlling Access to Wireless Networks

- As already discussed, *wireless networks*—such as *Wi-Fi networks*—are less secure, in general, than *wired networks*. There are Wi-Fi security procedures, however, that can be used to protect against unauthorized use of a wireless network and to encrypt data sent over the network so that it is unreadable if it is intercepted.
- The original Wi-Fi security standard was **WEP (Wired Equivalent Privacy)**. WEP is now considered insecure and has been replaced with the more secure **WPA (*Wi-Fi Protected Access*)** and the even more secure **WPA2** standards. However, Wi-Fi security features only work if they are enabled.
- *To protect against unauthorized access*, Wi-Fi network owners should secure their networks by changing the router or access point settings to enable one of the encryption standards and to assign a *network key* or *passphrase (essentially a password)* that must be supplied in order to access the secured network.

Access Control Systems - Controlling Access to Wireless Networks

- In addition, the *name of the network* (called the **SSID** – Service Set **ID**entifier) can be hidden from view by switching off the SSID broadcast feature.
- While hiding the network name will not deter serious hackers, it may reduce the number of casual *war drivers* or *neighbors accessing the network*.
- Once a network is secured, users who want to connect to that network need to either select or supply the network *SSID name* (depending on whether or not the SSID is being broadcast) and then enter the *network key* assigned to that network.

Computer Sabotage

- ***Computer sabotage***—acts of malicious destruction to a computer or computer resource—is another common type of computer crime today.
- Computer sabotage can take several forms, including ***launching a computer virus*** or a ***denial of service (DoS) attack***, ***altering the content of a Web site***, or ***changing data or programs located on a computer***.
- A ***common tool*** used to perform computer sabotage is a ***botnet***, discussed next. Computer sabotage is illegal in the United States, and acts of sabotage are estimated to cost individuals and organizations billions of dollars per year, primarily for labor costs related to correcting the problems caused by the sabotage, lost productivity, and lost sales.

Computer Sabotage - Botnet

- A computer that is controlled by a hacker or other computer criminal is referred to as a ***bot or zombie computer***; a group of bots that are controlled by one individual and can work together in a coordinated fashion is called a ***botnet***.
- ***Criminals*** (called ***botherders***) are increasingly creating botnets to use for computer sabotage, such as to spread malware and to launch denial of service (DoS) attacks, discussed shortly.
- ***Botherders*** also often sell their botnet services to send spam and launch Internet attacks on their clients' behalf, as well as to steal identity information, credit card numbers, passwords, corporate secrets, and other sensitive data, which are then sold to other criminals or otherwise used in an illegal manner.
- ***Bots*** are also used to perform ***click fraud***—automatically clicking on Internet ads to increase the fees that a company must pay.
- ***Click fraud*** is a type of internet crime that occurs in pay-per-click online advertising; the practice of repeatedly clicking on an advertisement hosted on a website with the intention of generating revenue for the host website or draining revenue from the advertiser.

Computer Sabotage - DoS

- A *denial of service* (**DoS**) attack is an act of sabotage that attempts to flood a network server or Web server with so many requests for action that it shuts down or simply cannot handle legitimate requests any longer, causing legitimate users to be denied service.
- *For example*, a hacker might set up one or more computers to request nonexistent information continually or to ping (contact) a server continually with a request to send a responding ping back to a false return address.
- DoS attacks today are often directed toward popular or controversial sites and typically are carried out via multiple computers (referred to as a distributed denial of service attack or DDoS attack). DDoS attacks are typically performed by botnets created by hackers; the computers in the botnet participate in the attacks without the owners' knowledge.

Protecting Against Computer Sabotage

- One of the most important protections against computer sabotage is using security software, and ensuring that it is kept current.
- **Security Software:**
 - To be protected against a computer virus or other type of malware; all computers and other devices which is used to access the Internet or a company network in both homes and offices should have security software installed.
 - *Security software* typically includes a variety of security features, including a firewall, protection against spyware and bots, and protection against some types of online fraud. It also includes, *protection against a spam filter, parental controls, password managers, diagnostic software, and backup features.*
 - *Mobile security software* also often includes *antitheft software.*
 - One of the most important components of security software is *antivirus software*, which protects against computer viruses and other types of malware.

Protecting Against Computer Sabotage – Few Tips

TIP



To ensure you have the latest security updates for your antivirus program, enable *automatic updates*.


TIP



According to a recent Harris Interactive survey, less than one-third of users have security software installed on their mobile devices, compared to 91% on their laptops.

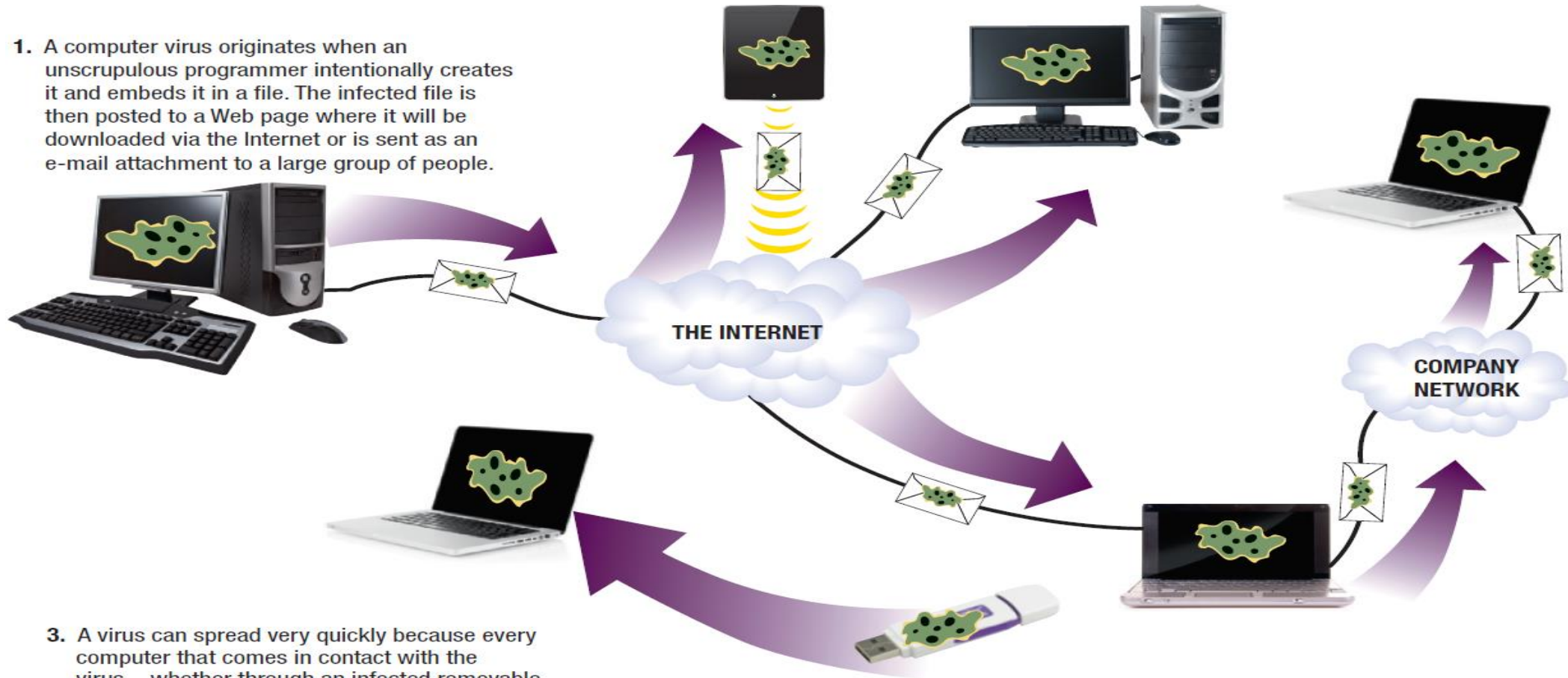
TIP



If you suspect your computer is infected with a malware program that your regular antivirus software cannot detect or remove, try a software program that specializes in removing hard-to-remove malware, such as the free *Malwarebytes Anti-Malware* program 

How a computer virus or other type malicious software might spread?

1. A computer virus originates when an unscrupulous programmer intentionally creates it and embeds it in a file. The infected file is then posted to a Web page where it will be downloaded via the Internet or is sent as an e-mail attachment to a large group of people.



3. A virus can spread very quickly because every computer that comes in contact with the virus—whether through an infected removable storage medium, infected downloaded file, or infected e-mail attachment—becomes infected, unless virus-protection software is used to prevent it.

2. When the infected file is opened on a computer, the virus copies itself to that computer's hard drive and the computer becomes infected. The virus may then e-mail itself to people in the newly infected computer's e-mail address book or copy itself to any removable storage medium inserted into that computer.

Virus Prevention Strategies

Use antivirus software to check incoming e-mail messages and files, and download updated virus definitions on a regular basis.

Limit the sharing of flash memory cards, USB flash drives, and other removable storage media with others.

Only download files from reputable sites.

Only open e-mail attachments that come from people you know and that do not have an executable file extension (such as .exe, .com, .bat, or .vbs); double-check with the sender before opening an unexpected, but seemingly legitimate, attachment.

For any downloaded file you are unsure of, upload it to a Web site (such as VirusTotal.com) that tests files for viruses before you open them.

Keep the preview window of your e-mail program closed so you will not view messages until you determine that they are safe to view.

Regularly download and install the latest security patches available for your operating system, browser, Java and other plug-ins, and e-mail programs.

Avoid downloading files from P2P sites.

Introduction to Computer Crime or Cyber Crime

- ***Cyber Crime*** is a crime which involves the use of digital technologies in commission of offence, directed to computing and communication technologies.
- The modern techniques that are proliferating towards the use of internet activity results in creating exploitation, vulnerability making a suitable way for transferring confidential data to commit an offence through illegal activity.
- The activity involves like ***attacking on identity theft, phishing, social media hacks, pharming, child pornography built images, online transaction fraud, internet sale fraud*** and also deployment in internet malicious activities such as ***virus, worm*** and third party abuse like ***phishing, email scams*** etc.

PHARMING

VS.

PHISHING

- Harder to identify
- Targets multiple people at a time
- Malicious code installed to computer
- Automatically redirects without requiring users to click a link

- Easier to identify
- Targets one person at a time
- Malicious email sent to inbox
- Requires users to manually click a link to activate code

Cyber Crime May Be Broadly Classified Into Three Groups

- **AGAINST INDIVIDUALS**

- Harassment via electronic mails
- Dissemination of obscene material
- Cyber-stalking
- Defamation
- Indecent exposure
- Cheating
- Unauthorized control/access over computer system
- Email spoofing
- Fraud

- **AGAINST INDIVIDUALS PROPERTY**

- Computer vandalism
- Transmitting virus
- Unauthorized access / control over computer system
- Intellectual Property crimes
- Internet thefts

Cyber Crime May Be Broadly Classified Into Three Groups

- **AGAINST ORGANIZATION**

- Unauthorized access / control over computer system
- Cyber terrorism against the government organization
- Possession of unauthorized information
- Distribution of Pirate software

- **AGAINST SOCIETY**

- Child pornography
- Indecent exposure of polluting the youth financial crimes
- Sale of illegal articles
- Trafficking
- Forgery
- Online gambling

Software piracy

- *Software piracy* is a crime commonly defined as illegal copying, downloading, sharing, selling or installing of copyrighted software.
- Software piracy is *unauthorized reproduction of copyrighted software*. The unauthorized copying can be done for different purposes such as *personal use*, *business use* and even *selling copies of the pirated software*.

Common Types of Software Piracy

- **Soft lifting:**

Soft lifting is the act of illegal copying of software and distributing it to friends, organizations or duplication and resale in violation of the terms of the license agreement.

- **Internet piracy:**

Internet piracy is one of the fastest and easiest ways to receive pirated software. There are several websites that make software available for free download in a number of ways.

- **Hard-disk loading:**

Hard-disk loading occurs when an individual or company sells computers preloaded with illegal copies of software into the hard disks to encourage the consumer to buy their products.

Common Types of Software Piracy (Contd.)

- **Software counterfeiting:**

Software counterfeiting is illegal duplication and sale of copyrighted software in such a way that it appears to be authentic. Counterfeit software includes accompanying manuals that the original legitimate software was sold and is usually sold at prices well below that of the retail price of the legitimate software.

- **Renting:**

Renting involves someone renting out a copy of licensed software for temporary purposes. In such type of piracy, software is rented to individual computers and returned the original software to the renter.

- **Unauthorized use of academic software:**

- Many software companies sell academic versions of their software to public schools, universities and other educational institutions. When the software is labeled to use for academic or educational purposes only, it cannot be used for commercial or other for profit purposes.
- Using academic software for private use in violation of the software license is a form of software piracy and it not only hurts the software publisher, but also the institution that was the intended recipient of the software.

Antipiracy

- *Anti-piracy* is a term used by some to describe the *attempt to prevent copyright violation*.
- It is against piracy, it describes different methods to stopping piracy and focuses on how original writer can be prevented from being cheated. It is very difficult to define law that deals with intellectual property.

Ethical Issues in Computing

- *Computer ethics* is a branch of practical philosophy which deals with how computing professionals should make decisions regarding professional and social conduct.
- A simple code of conduct suggested by the *Computer Ethics Institute* (CEI) is listed below:
 - Do not use a computer to harm other people
 - Do not interfere with other people's computer work
 - Do not snoop around in other people's computer files
 - Do not use a computer to steal
 - Do not use a computer to bear false witness
 - Do not copy or use proprietary software for which you have not paid
 - Do not use other people's computer resources without authorization or proper compensation
 - Do not use other peoples' intellectual output
 - Always think about the social consequences of the program you are writing or the system you are designing
 - Always use a computer in ways that ensure consideration and respect for your fellow humans

Cyber Law

- **Cyber law** is the part of the overall legal system that deals with the internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including *freedom of expression, access to and usage of the internet, and online privacy*. Generically, cyber law has been referred to as the *Law of the Internet*.
- **Why are cyber laws needed?**
 - Just like any law, a cyber-law is created to help protect people and organizations on the internet from malicious people on the internet and help maintain order. If someone breaks a cyber-law or rule, it allows another person or organization to take action against that person or have them sentenced to a punishment.
 - These laws are mainly concerned with:
 - ❖ Regulation of information and communication technology market
 - ❖ Protection of intellectual property in the ICT sector
 - ❖ Electronic transaction
 - ❖ Non-contractual liability
 - ❖ Privacy protection
 - ❖ Computer related crime

Network Security

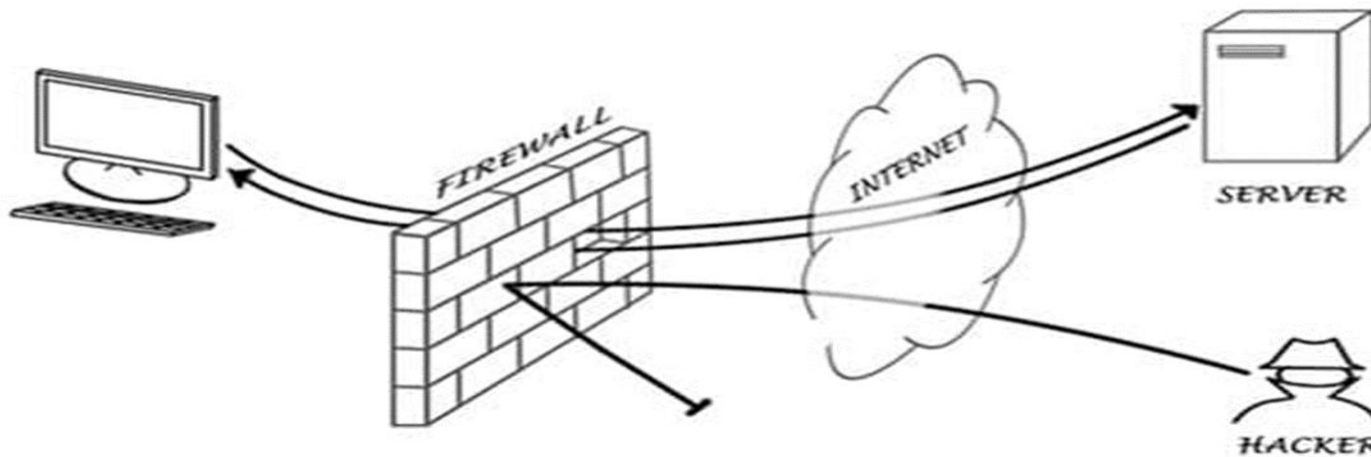
- ***Network security*** is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.
- ***Network security*** combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain accesses to network resources, but malicious actors are blocked from carrying out exploits and threats.
- **Types of network security:**
 - Access control
 - Antivirus and antimalware software
 - Application security
 - Data loss prevention
 - Email security
 - Intrusion prevention systems
 - Firewalls

Firewall

- A *firewall* is a system designed to prevent unauthorized access to or from a private network. Firewalls prevents *unauthorized internet users* from accessing *private networks* connected to the internet, especially intranets.
- A firewall establishes a barrier between a trusted internal network and the internet.
- A firewall is a *network security device* that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a *barrier between your internal network* and *incoming traffic from external sources (such as the internet)* in order to block malicious traffic like *viruses* and **hackers**.
- All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
- A *Hardware Firewall* is a device to which you connect your computers or network in order to protect them from unauthorized access.
- A *Software Firewall* is a piece of software that is installed on your computer in order to protect it from unauthorized access.

Firewall (Contd.)

- Firewall is considered as an essential element to achieve network security for the following reasons –
 - Internal network and hosts are unlikely to be properly secured.
 - Internet is a dangerous place with criminals, users from competing companies, disgruntled ex-employees, spies from unfriendly countries, vandals, etc.
 - To prevent an attacker from launching denial of service attacks on network resource.
 - To prevent illegal modification/access to internal data by an outsider attacker.



How does a firewall Work?

- *Firewalls* carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices.
- For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22." Think of IP addresses as houses, and port numbers as rooms within the house.
- Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports)

Types of Firewall

- ***Firewalls*** can either be software or hardware, though it's best to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between your network and gateway.
- Types of Firewall are:
 - ***Packet –filtering firewalls***
 - ***Proxy firewalls (or Application-level Gateway)***
 - ***Network address translation (NAT) firewalls***
 - ***Stateful Multilayer Inspection Firewall***

Types of Firewall

- **Packet –filtering firewalls:**

- ❖ Packet-filtering firewalls, the most common type of firewall, examine packets and prohibit them from passing through if they don't match an established security rule set. This type of firewall checks the packet's source and destination IP addresses. If packets match those of an “allowed” rule on the firewall, then it is trusted to enter the network.
- ❖ Packet-filtering firewalls are divided into two categories: *stateful* and *stateless*. **Stateless** firewalls examine packets independently of one another and lack context, making them easy targets for hackers. In contrast, **stateful** firewalls remember information about previously passed packets and are considered much more secure.

Types of Firewall

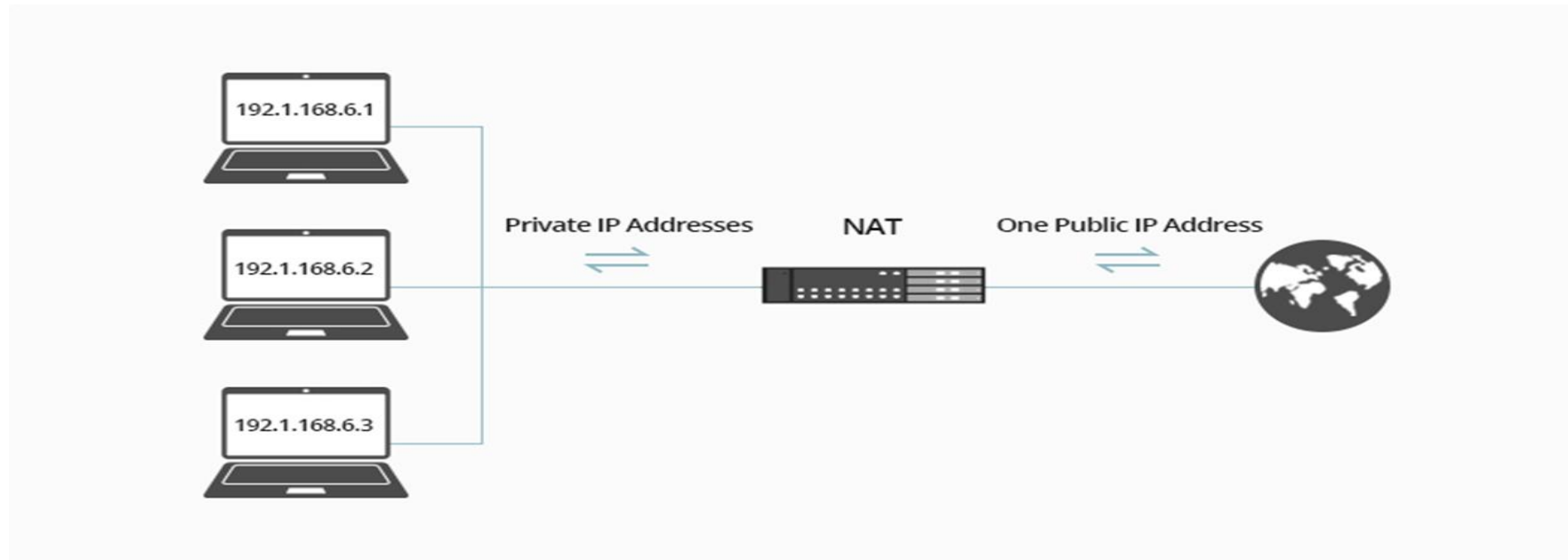
- **Proxy firewalls (or Application-level Gateway):**

- ❖ *Proxy firewalls* filter network traffic at the application level. Unlike basic firewalls, the proxy acts as an intermediary between two end systems.
- ❖ The client must send a request to the firewall, where it is then evaluated against a set of security rules and then permitted or blocked. Most notably, proxy firewalls monitor traffic for layer 7 protocols such as HTTP and FTP, and use both stateful and *deep packet* inspection to detect malicious traffic.
- ❖ It protects user anonymity.
- ❖ Costlier than some other firewall options.
- ❖ It also checks payload that means actual data that are to be transmitted.

Types of Firewall

- **Network address translation (NAT) firewalls:**

- ❖ It allow multiple devices with independent network addresses to connect to the internet using a single IP address, keeping individual IP addresses hidden. As a result, attacker scanning a network for IP addresses can't capture specific details, providing greater security against attacks.
- ❖ NAT firewalls are similar to proxy firewalls in that they act as an intermediary between a group of computers and outside traffic.



Types of Firewall

- **Stateful Multilayer Inspection Firewall:**

- ❖ State-aware devices not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.
- ❖ A further *variant of stateful inspection* is the *multilayer inspection firewall*, which considers the flow of transactions in process across multiple protocol layers of the seven-layer Open Systems Interconnection (OSI) model.
- ❖ It offer a higher level of security, good performance and transparency to end users.

Firewall Delivery Methods

- As IT consumption models evolved, so too did security deployment options. Firewalls today can be deployed as a hardware appliance or software-based service.
- **Hardware-based firewalls:**
 - A *hardware-based firewall* is an appliance that acts as a secure gateway between devices inside the network perimeter and those outside it. Because they are self-contained appliances, hardware-based firewalls don't consume processing power or other resources of the host devices.
 - Sometimes called *network-based firewalls*, these appliances are ideal for medium and large organizations looking to protect many devices. Hardware-based firewalls require more knowledge to configure and manage than their host-based counterparts.

Firewall Delivery Methods (Contd.)

- **Software-based firewalls:**

- A *software-based firewall*, or *host firewall*, runs on a server or other device. Host firewall software needs to be installed on each device requiring protection. As such, software-based firewalls consume some of the host device's CPU and RAM resources.
- *Software-based firewalls* provide individual devices significant protection against viruses and other malicious content. They can discern different programs running on the host, while filtering inbound (incoming) and outbound (outgoing) traffic. This provides a fine-grained level of control, making it possible to enable communications to/from one program but prevent it to/from another.

Data Security and Message Security

- ***Data Security*** refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. Data security includes data encryption, tokenization, and key management practices that protect data across all applications and platforms.
- ***Messaging Security*** is a program that provides protection for companies messaging infrastructure. It protects all the personal message of the company which are related to company's vision and mission.

Types of Data Security

- **Confidentiality:**

allows authorized users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.

- **System Integrity:**

Integrity of information refers to protecting information from being modified by unauthorized parties. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.

- **Availability:**

Availability of information refers to ensuring that authorized parties are able to access the information when needed.

Cryptography

- ***Cryptography*** is associated with the process of converting ordinary plain text (text that can be read and understood) into cipher text (text that cannot be read and understood) and vice-versa.
- It 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 not only protects data from theft or alteration, but can also be used for user authentication.
- The art of protecting information by transforming it (encrypting it) into an unreadable format called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text.
- **Note:**
 - *Encrypt, encode, encipher* are same..
 - *Decrypt, decode, decipher* are same.

Features of Cryptography

- **Confidentiality:**

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

- **Integrity:**

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

- **Non-repudiation:**

The creator/sender of information cannot deny his or her intention to send information at later stage.

- **Authentication:**

The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Encryption and Decryption

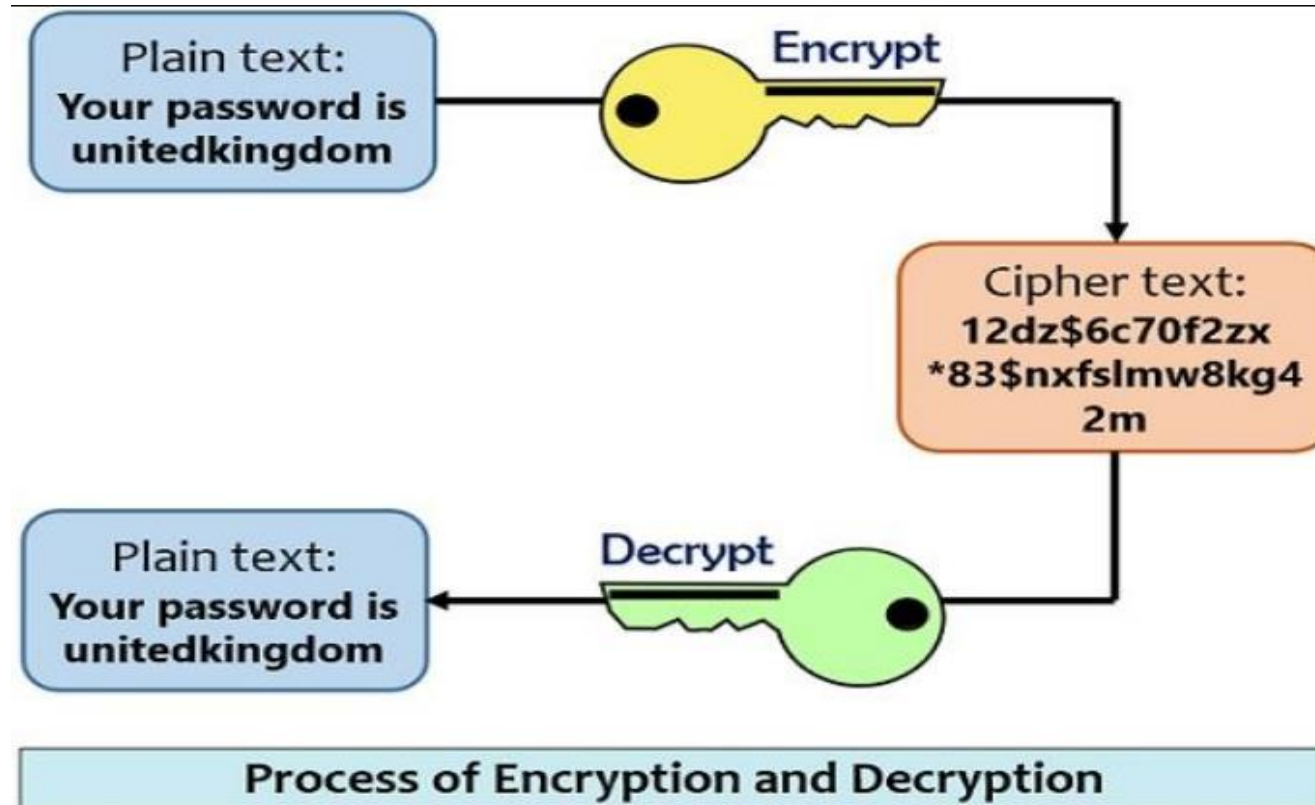
- **Encryption:**

It is security tool for computer network. It is process of converting information (known as plain text) using an algorithm to make it unreadable (known as cipher text) to anyone except those processing special knowledge, usually referred to as a key. It is the most efficient method to achieve data security. Encryption can protect confidentiality of message. For data encryption, a secret key is used. Encrypted data is called as cipher text and decrypted data is called as plain text.

- **Decryption:**

It is process of taking encoded or encrypted text and converting it back into original text. Decryption is used for un-encrypting the data with keys or algorithm. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (Cipher Text). The decryption process requires two things- a Decryption algorithm and a key. A Decryption algorithm indicates the technique that has been used in Decryption. Usually, the encryption and decryption algorithm are same.

Process of Encryption and Decryption



THANK YOU!