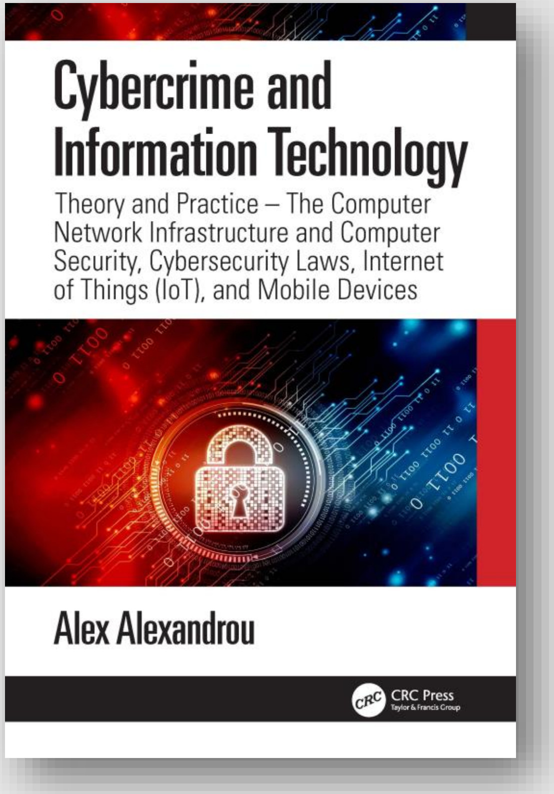


Cybercrime and Information Technology

Theory and Practice – The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices

Alex Alexandrou

CRC Press
Taylor & Francis Group

CYBERCRIME AND INFORMATION TECHNOLOGY: THEORY AND PRACTICE

The Computer Network Infostructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices

COMPUTER SECURITY TECHNOLOGY AND PRINCIPLES

Chapter 6, Lecture 1

Your Name

Objectives

- Understand computer security technology, its history and evolution.

- Understand the CIA Triad Model and NIST’s Standards for Security Categorization of Federal Information and Information Systems (FIPS 199).

- Recognize the significance of identification, authentication, and authorization in computer security.

- Understand different types of cyberattacks.

Objectives

- Recognize computer security prevention mechanisms.

- Understand modern encryption methodology.

History & Definitions

For every type of cyberattack, there is a defense mechanism. For every defense mechanism, there is a new and unknown cyberattack.

History

Ancient civilizations invented various clever ways to hide information and messages from adversaries.

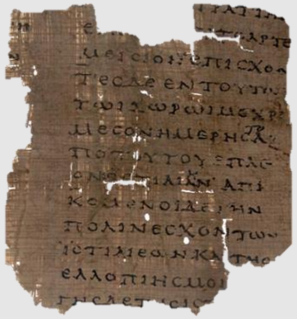
- Two well-known techniques for keeping information confidential are steganography and cryptography.
  - **Steganography**, means covered writing, and derives from the Greek word steganós (στεγανός), meaning covered, and graphy (γραφή), writing.
    - In steganography, information is concealed or hidden from view, and no means are used to change the structure of the information.
  - **Cryptography**, means hidden writing, and originates from the Greek words crypto (κρυπτός) meaning hidden, and graphy (γραφή), writing.
    - In cryptography, information is encrypted by encoding or changing the information structure.
    - Cryptography began thousands of years ago, protecting secrets by applying a code to encrypt and then decrypt a message.
    - A parallel technique, called cryptanalysis, was invented to breach or break the adversary's code.
    - The algorithm or process of implementing both an encryption and decryption is called cipher or cypher.

History & Definitions (cont.)

Examples

Steganography

- According to Herodotus (c.486–425 B.C.), the first example concerns an aristocrat, Histaeus, who wanted to send a secret message to his son-in-law in Greece, urging revolt against the Persians. He shaved the head of a trustworthy slave and tattooed the message onto his scalp. After the hair grew back, the slave was sent to deliver the message.
- Another example was when alerted Sparta to an invasion from the Persians by concealing the message under writing tablets using wax.
  - These were usually two pieces of wood, hinged as a book, with each face covered with wax. One wrote on the wax; the recipient melted the wax and reused the tablet.



Fragment from Herodotus Histories Book VIII.

Cryptography

- In the Old Testament contains encrypted text using Atbash ciphers, a traditional Hebrew method (c. 600-500 B.C.), accomplished by replacing a letter with another letter that is an equal number of places from the end of the alphabet.
  - For example, the letter “A” would be replaced by the letter “Z” and the letter “B” by the letter “Y”.
- In India, according to the Kama Sutra, an ancient text on sexuality written between 400 BCE and 300 CE, lovers would encrypt writing communication between themselves.
- Ancient Greeks also used a wooden baton or *scytale* (σκυτάλη) to send cipher messages during military conflicts. Spartans used a belt containing a strip of parchment that contained a written message.
  - When the messenger, wearing the belt, arrived at his destination, the receiver decrypted the message, by wrapping the parchment strip around a *scytale* of the same diameter.

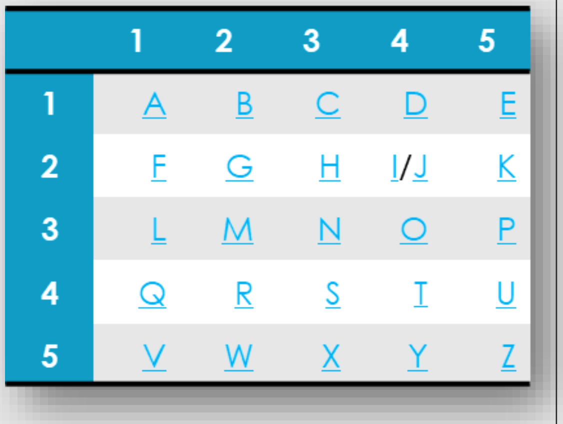
A scytale

History & Definitions (cont.)

Examples

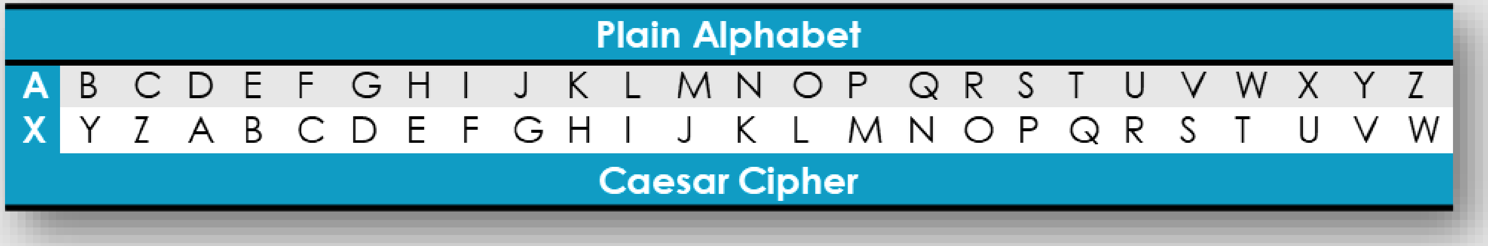
Cryptography

1. Polybius Square (was invented by Cleoxenus and Democleitus, and was further developed by Polybius)
   - The method divides the alphabet into five rows of squares, each described by coordinates in the grid. To decrypt the message the recipient must know the letters represented by each set of coordinates. Using this simple example, the word “Love” (letters underlined) converts to 31 34 51 15).
   - Julius Caesar on the other hand, used a method called the Caesar cipher or Caesar code, that moved each letter a fixed number of places. The word “LOVE” becomes “ILSB” and the word “THE” becomes “QEB” by replacing each letter with the letter three places to the left.



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Polybius Square



Plain Alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Caesar Cipher

The Caesar cipher with three shifted places

History & Definitions (cont.)

Examples

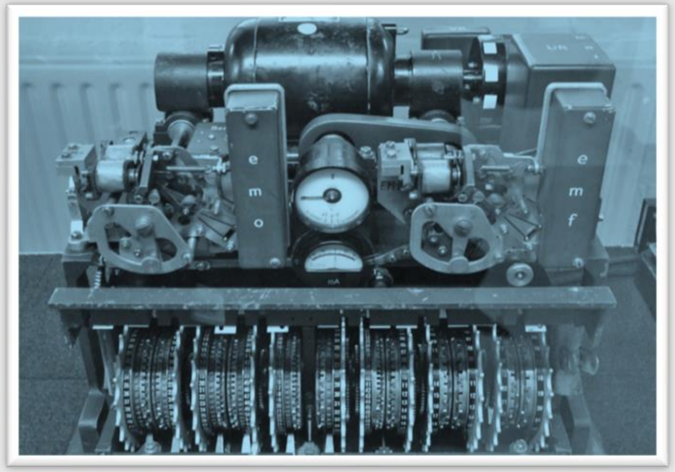
Modern Cryptography

1. During World War II, the Germans developed and used numerous mechanical and electromechanical machines for encrypting communication.

2. Their best-known cipher machines are the Enigma, built by the Chiffriermaschinen Aktiengesellschaft (Cipher Machines Corporation), and the SZ-40/SZ-42, built by Standard Elektrik Lorenz.

Modern cryptography uses complicated algorithms such as Blockchain, Public-key cryptography, and Cryptographic hash functions.

Enigma Machine



Lorenz-SZ42 Machine

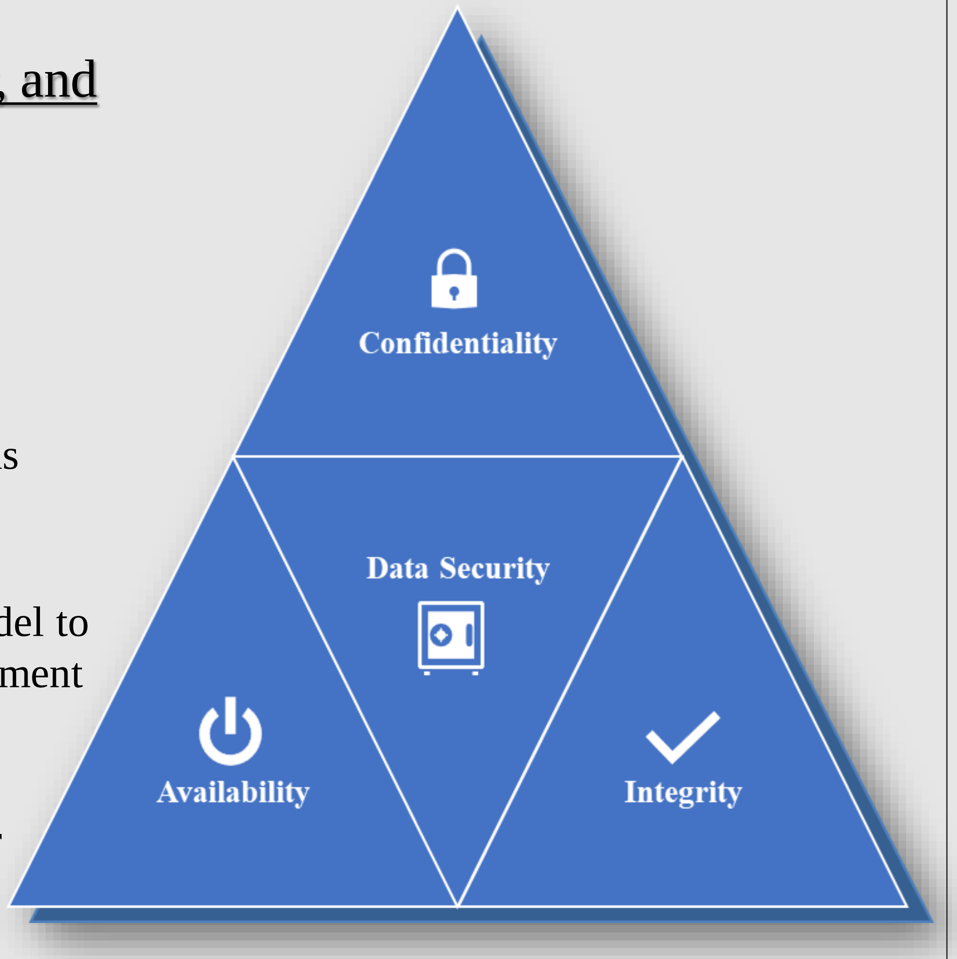
History & Definitions (cont.)

Different terminologies have been used to describe computer security.

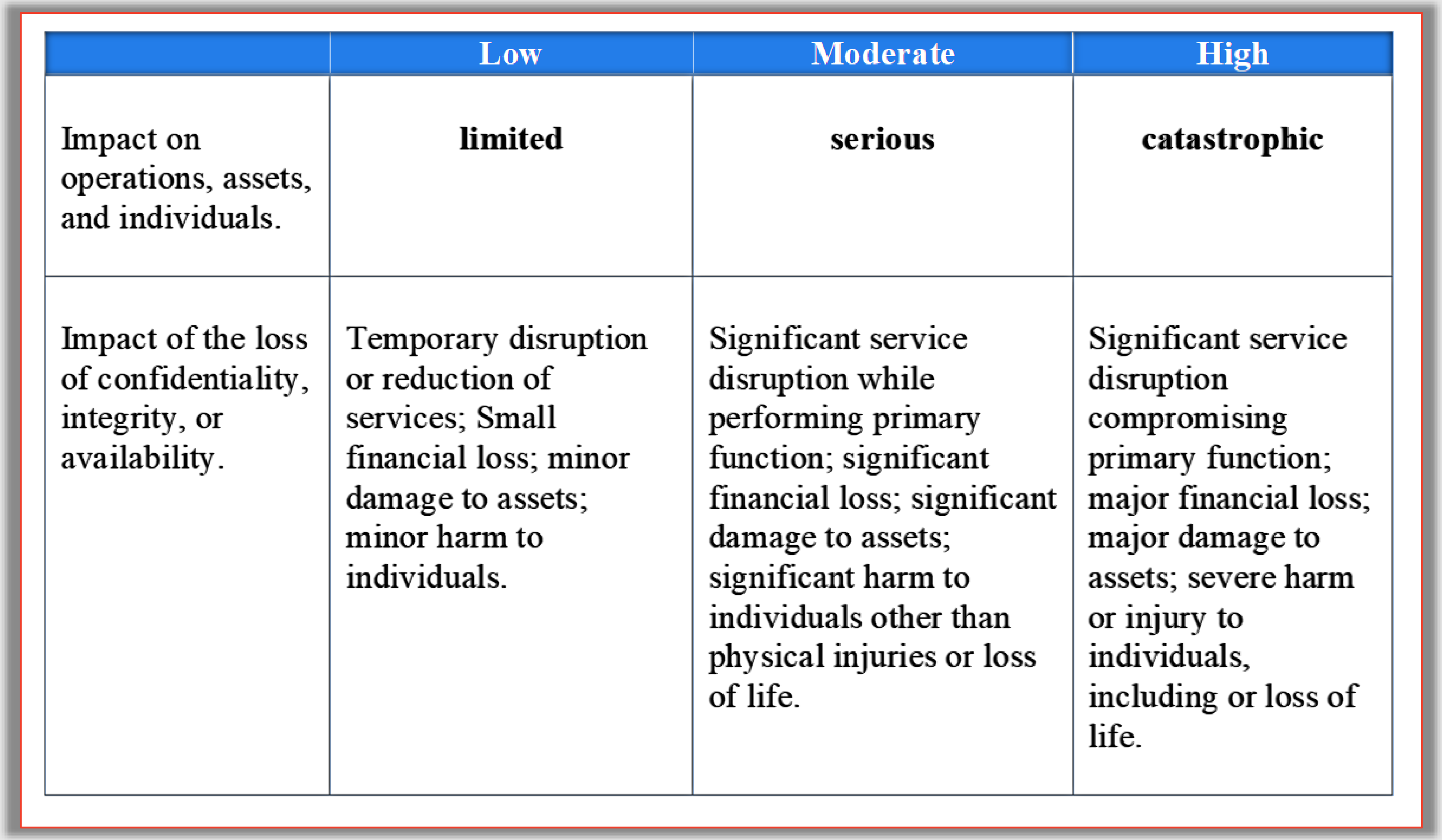
- **Application security** is a general term for securing applications.
  - It includes security features within applications, and measures often used for finding, fixing and preventing security vulnerabilities against cyberthreats. Examples include e-mail, Directory Services, Web browsers, video conferencing applications like Zoom and Skype, and file transfers.
- **Cybersecurity** refers to protection from criminal activity facilitated by the Internet.
  - It also relates to the protection of internet-connected devices, computer programs, networks, and data from cybercriminals.
    - In other words, cybersecurity protects physical security, which consists of sites, equipment, infrastructure, etc., and logical security, which consists of software safeguards such as user passwords, access, and authentication of Information and Communications Technology (ICT).
- **Network security** involves the use of countermeasures to protect the networking infrastructure, both software and hardware, from intruders.
  - Information security, or InfoSec, refers to safeguarding data in storage, in transit and while being used.

CIA Triad Model

- The three letters in "CIA triad" stand for confidentiality, integrity, and availability.
- The CIA triad forms the basis for the development of security systems and policies.
  - These three concepts are commonly known as the CIA Triad Model, which has been used in information security to direct policies of keeping and protecting confidential and sensitive data.
  - The National Institute of Standards and Technology (NIST) has used this model to define information security and cybersecurity and to help organizations implement information security programs.
  - The NIST’s Standards for Security Categorization of Federal Information and Information Systems (FIPS 199) has defined the levels of potential impact for Confidentiality, Integrity, and Availability as Low, Moderate and High.



CIA Triad Model (cont.)



	Low	Moderate	High
Impact on operations, assets, and individuals.	**limited**	**serious**	**catastrophic**
Impact of the loss of confidentiality, integrity, or availability.	Temporary disruption or reduction of services; Small financial loss; minor damage to assets; minor harm to individuals.	Significant service disruption while performing primary function; significant financial loss; significant damage to assets; significant harm to individuals other than physical injuries or loss of life.	Significant service disruption compromising primary function; major financial loss; major damage to assets; severe harm or injury to individuals, including or loss of life.

Understanding Security terminology

- The world of computer security is constantly changing. Attacks occur daily and continue to evolve.
- Computer security consists of sets of protocols and best practices showing organizations and individuals how to prevent and monitor unauthorized access. The most important terms associated with computer security:
  - **Access control**—is a system that permits, restricts, and monitors requests for access to a wide range of hardware and software, including access to computer systems and network resources, information processing services, and entry or exit points to facilities.
  - **Anti-virus software or antivirus protection**—is a program that prevents, detects, monitors, and removes malicious software from a computing system, device or network.
  - **Behavioral analytics**—in enterprise security, behavioral analytics software senses abnormal network behavior such as patterns of unusual data transfer. Behavior analytics software detects intrusions that elude firewalls and antivirus software.
  - **Biometrics**—are unique physical or behavioral characteristics that either identify (who are you?) or verify (prove that it is you…. are you who you claim to be?) the user. Physical or physiological characteristics can consist of DNA, facial patterns, fingerprints, hand geometry, a person's vein patterns, and iris pattern-recognition. Behavioral characteristics can include handwriting patterns, voice recognition, typing or keystroke patterns, and signature analysis.
  - **Cloud security**—is the safeguarding of cloud-based computing systems, including applications, cloud access, data, and infrastructures, using controls, policies, and systems.

Understanding Security terminology (cont.)

- **Crime-as-a-Service (CaaS)**—an on-demand marketplace found on the Dark Web, where one can purchase cybercrime services and attack tools like exploit kits, ransomware, worms, and phishing tools.

- **Software-as-a-Service (SaaS)**—describes the current method of licensing popular software. Instead of purchasing and installing the software from disks, the software is now cloud-based, and we license and download our copies. Examples include Microsoft Office 365, Google Apps, Dropbox, Cisco WebEx, GoToMeeting, and Adobe Photoshop, InDesign and Acrobat.

- **Cyberwarfare**—a nation-state-sponsored cyber-attack on another nation-state to harm, alter, destroy, or steal information, to disseminate lies and misinformation, or to conduct espionage and sabotage a computer network.

- **Data Breach**— access to a computer system or network resulting in disclosure of information. It may transpire intentionally or unintentionally. When the breach follows hackers gaining unauthorized access, it is intentional; when caused by an employee's negligence, such as accidental loss of computing devices, stolen or unattended sensitive documents, the breach is unintentional.

- **Exploit**—refers to a program or a code written to attack or take advantage of a vulnerability and break into a computer system or a network.

- **Hacker**—is an individual accessing a computer device or a computer system without the user's knowledge and authorization. In assessing the hacker, the essential factor is whether a law, for example the Computer Fraud and Abuse Act (18 U.S.C. §1030), is being broken.

Understanding Security terminology (cont.)

- Hackers are classified into the following types:
  - **Black-hat hackers** are cybercriminals who break into or gain unauthorized access to a computer system with malicious intentions. The primary motivations are financial gain, cyber espionage, and competition between hackers.
  - **White-hat hackers or Ethical hackers** are the “good guys of hacking,” who utilize the same techniques as black-hat hackers, but access systems with permission to identify security vulnerabilities and exploits.
  - **Gray-hat hackers** are somewhere between black and white hat, and do not have criminal motives. They will identify security vulnerabilities and exploits in computing systems without permission from the owner. After the defect is found the gray-hat hacker will inform the owner of the system and demand a small fee to repair the vulnerability, mentioning that otherwise the hack might be published. The motive is mostly personal enjoyment.
  - **Script kiddies or Amateurs** are individuals who use tools and follow instructions that are easily found online. Assumed to be juveniles who lack the ability to write complex programs or exploits, their main objectives are to impress friends, curiosity, enjoyment of a challenge, or an attempt to enter a professional hacking group.
  - **Hacktivists** are individual hackers driven by an ideology or are politically inspired.

Black-hat, gray-hat, and white-hat hackers.

Understanding Security terminology (cont.)

- **Intrusion Detection System (IDS)**—is a hardware or a software application installed on the network that detects, logs and screens for malicious attacks and intrusions based on security policies or rule violations on the network. The IDS identifies possible incidents, compares anomalies to normal activities and recognizes deviations.

- **Intrusion Prevention System (IPS)**—is a hardware or a software application that detects and blocks intrusions on the network by examining network traffic flows and attempts to prevent any exploit from reaching its destination. The IPS is designed to block threats, analyze, and stop data packets from being delivered based on a predefined set of security rules and policies.

- **Intrusion Detection System (IDS)**—is a hardware or a software application installed on the network that detects, logs and screens for malicious attacks and intrusions based on security policies or rule violations on the network. The IDS identifies possible incidents, compares anomalies to normal activities and recognizes deviations.

Understanding Security terminology (cont.)

- **Protocols**—are a digital language and set of specifications used by systems to communicate with each another. Important protocols are the Transmission Control Protocol (TCP) and Hypertext Transfer Protocol Secure (HTTPS).
- Each protocol uses precise rules and has an exact purpose on a specific port. Some of the most common security protocols include:
  - Secure Sockets Layer (SSL) and Transport Layer Security (TLS), protocols for encrypting and securing communications over a network. The SSL has been replaced by the TLC but is still commonly used.
  - The Secure Shell (SSH) protocol provides secure remote login from one computer to another via an unsecured network (SSH client connecting to the SSH server).
  - The Hypertext Transfer Protocol Secure (HTTPS) sends data between a web browser and a website. HTTPS is encrypted using TLS in order to increase security of data transfer.
  - The Pretty Good Privacy (PGP) is an encryption protocol that allows a receiver to authenticate the identity of a sender who has sent the message and verify that it was not altered in transit.
    - The PGP uses a combination of symmetric and asymmetric encryption and has been used in encrypting and decrypting texts, e-mails, files, and other messages.

Understanding Security terminology (cont.)

- **Security Audit**—is an impartial assessment and examination of an organization’s information security systems. Review of regulations, operational procedures, and practices.
  - Assessment of infrastructure
  - Audit of specific applications
  - Assessment of physical security

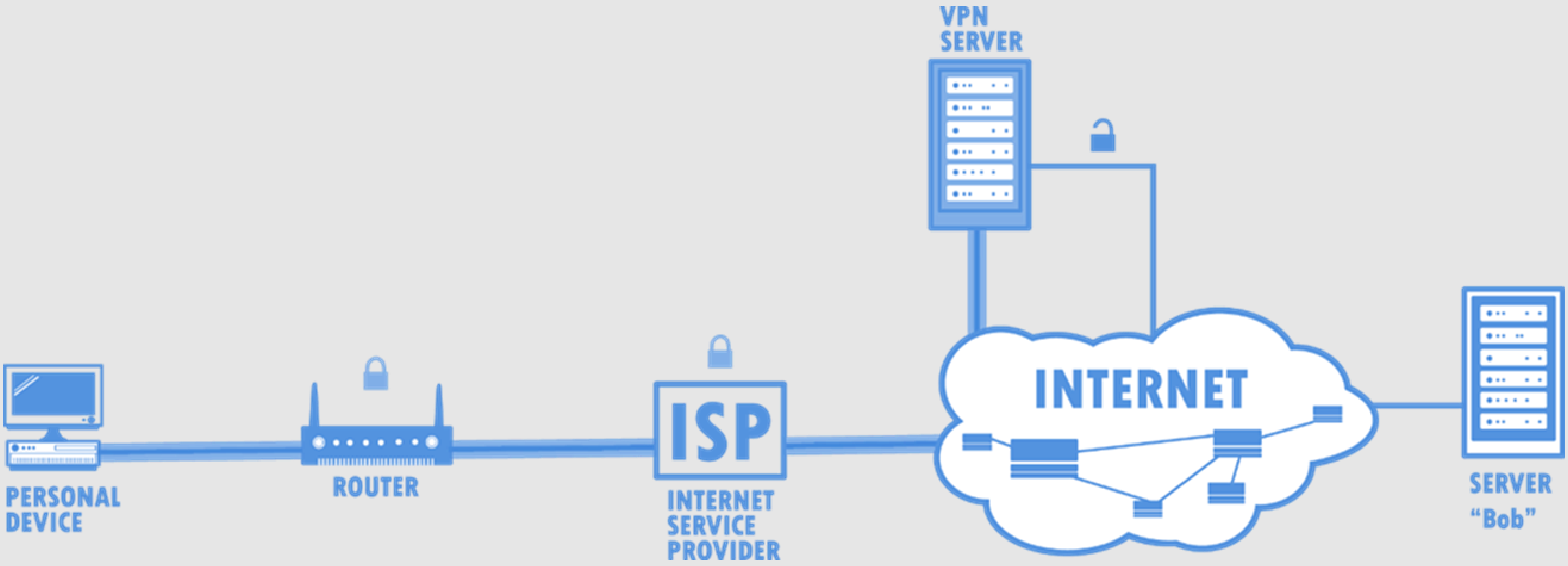
- **Security Threat**—refers to a possibility or an action that can compromise computing systems.

- **Spam**—any unwelcome electronic messages sent in bulk. Spam may be an advertising campaign or a malicious worm or virus with a primary mission to infect.

- **Virtual Private Network (VPN)—**is a point-to-point secure network connection for traffic across the Internet.

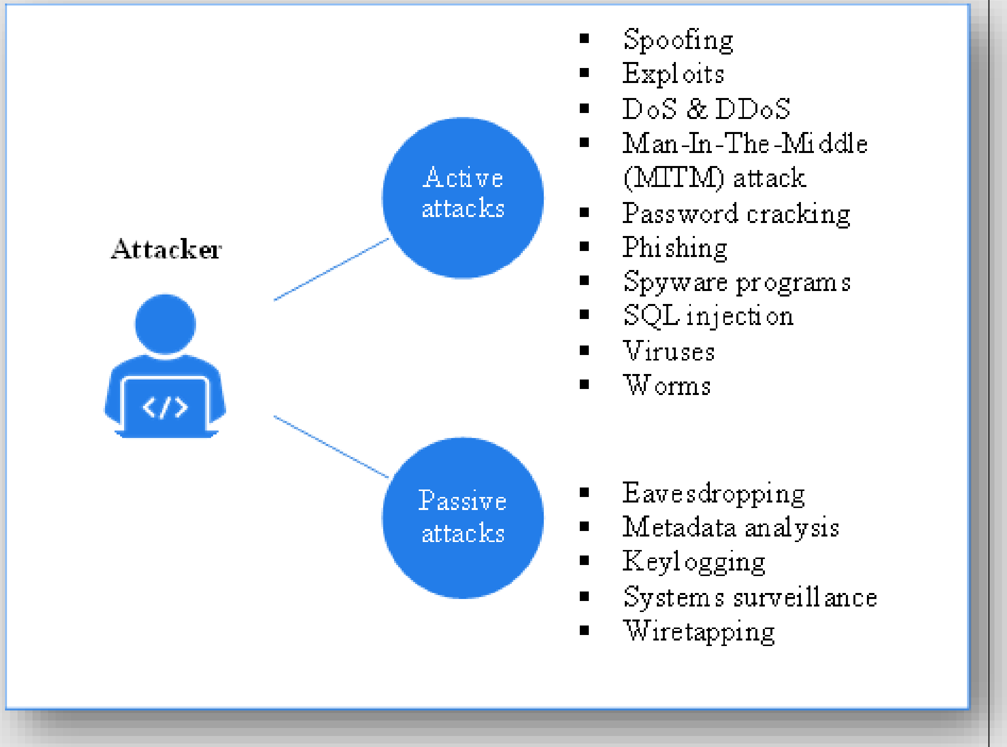
- **Vulnerability**—refers to a security flaw or weakness in a computing system or software that can be exploited by hackers.

Understanding Security terminology (cont.)



Types of Cyber-attacks

- In computer security, cyber-attacks are classified as **Active and Passive**.
- When cybercriminals modify system resources, data, or affect the operation, the attack is classified as Active.
- When cybercriminals do not modify system resources, but instead use the information by monitoring or copying, the attack is classified as Passive.
  - Example of Active attacks include exploits, DoS, DDoS, malware, phishing, brute force attacks like password cracking, viruses, and worms.
  - Passive attacks consist of system surveillance like keystroke loggers that record every keystroke, malware that can eavesdrop on emails and other communications like voice recordings and metadata analysis.
- Attacks may occur from inside an organization's network, or from an outside source like a hacker.

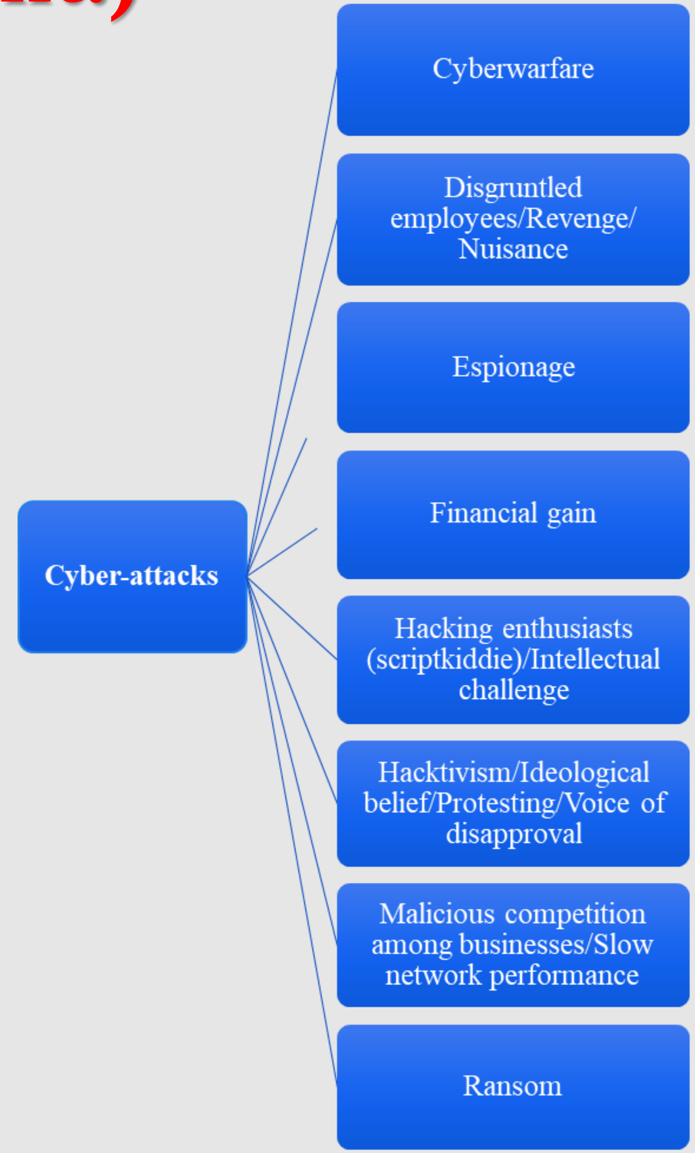


- Spoofing
- Exploits
- DoS & DDoS
- Man-In-The-Middle (MITM) attack
- Password cracking
- Phishing
- Spyware programs
- SQL injection
- Viruses
- Worms

- Eavesdropping
- Metadata analysis
- Keylogging
- Systems surveillance
- Wiretapping

Types of Cyber-attacks (cont.)

- A **cyber-attack** is an intentional exploitation and malicious action that targets computing systems, networks, and personal computing devices.
- The **attack vector in cybersecurity** refers to methods used to gain unauthorized access or to penetrate the targeted computing system.
- A database that provides references and descriptions of officially known security vulnerabilities and exposures is called the **Common Vulnerabilities and Exposures (CVE).**
  - The CVE standardizes and classifies security vulnerabilities for public use.
  - This database system was launched in 1992 and is sponsored by U.S. Department of Homeland Security (DHS) and the Cybersecurity Infrastructure Security Agency (CISA), which operates as DHS's Federally Funded Research and Development Center.
  - The MITRE Corporation is a not-for-profit organization that manages and maintains the CVE list and website.
  - An example of a recent vulnerability described in the CVE is the Android version of Chrome named CVE-2020-16010 and refers to an exploit that cybercriminals are abusing and which needs to be patched.


Cyber-attacks
Cyberwarfare
Disgruntled employees/Revenge/ Nuisance
Espionage
Financial gain
Hacking enthusiasts (scriptkiddie)/Intellectual challenge
Hacktivism/Ideological belief/Protesting/Voice of disapproval
Malicious competition among businesses/Slow network performance
Ransom

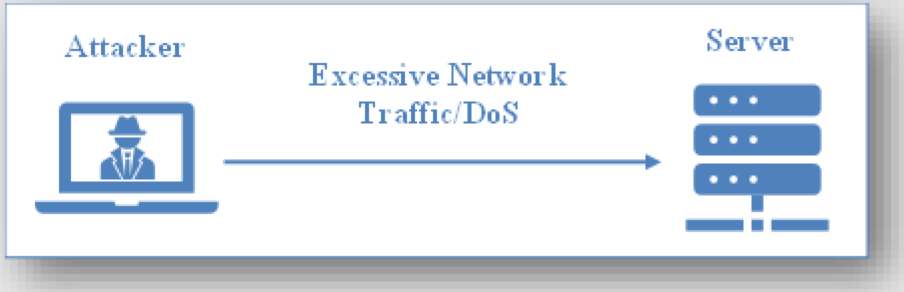
Types of Cyber-attacks (cont.)

I. Adware

- Adware, or advertising-supported software, is considered undesirable software, intended to force the user to view or click on an advertisement on the screen.
  - Adware exists in all computing device platforms and is usually safe, legitimate, and not malicious. cybercriminals could take advantage of the adware developers and might use it as a gateway for malware infection.

II. Denial of service attacks

- Denial-of-service (DoS) is an attack that occurs when a hacker makes computer resources inaccessible to its users.
  - The two common methods of DoS attacks are: flooding network services by using up resources and crashing network services.

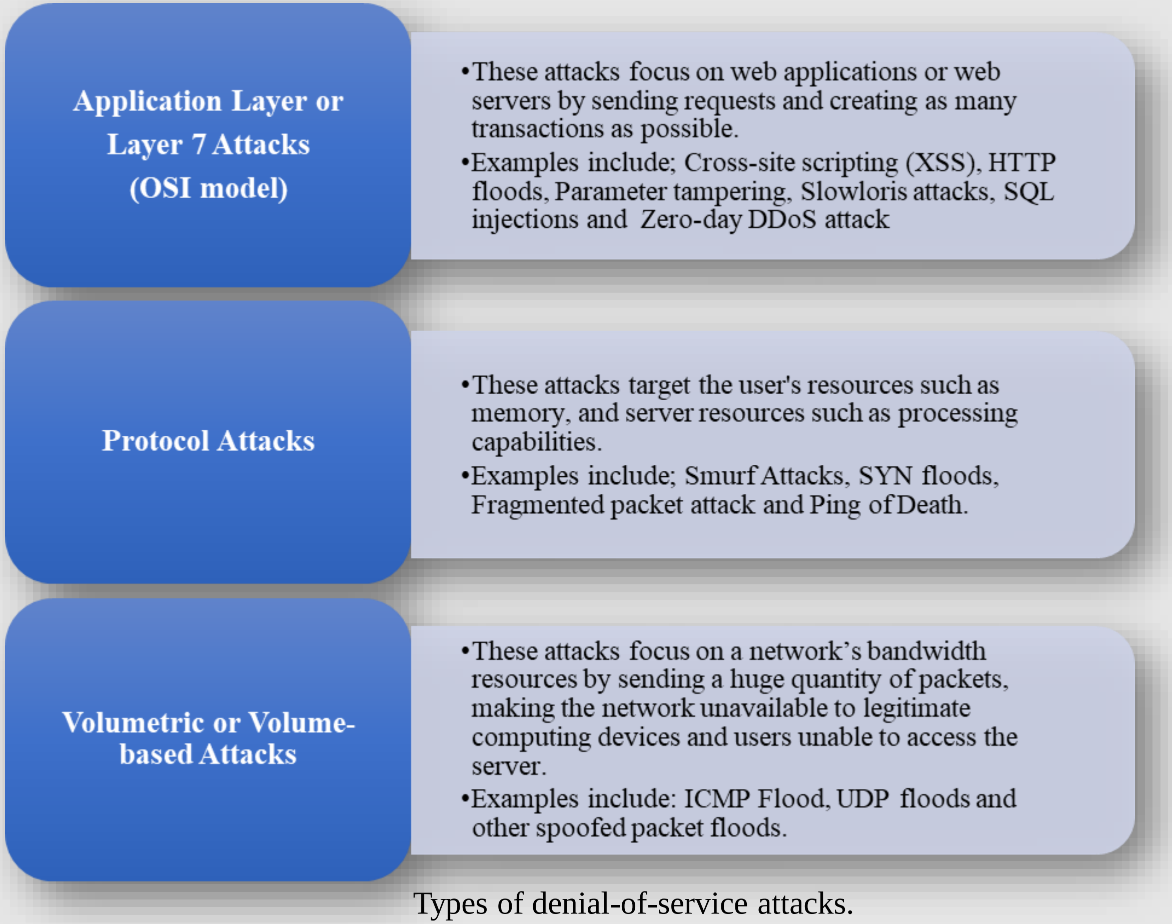


A DoS attack

Types of Cyber-attacks (cont.)

II. Denial of service attacks (cont.)

- Denial-of-service attacks come in various forms and can be classified as Application Layer Attacks (measured in requests per second), Protocol Attacks (measured in packets per second) and Volumetric or Volume-based Attacks (measured in bits per second).



Application Layer or Layer 7 Attacks (OSI model)

- These attacks focus on web applications or web servers by sending requests and creating as many transactions as possible.
- Examples include; Cross-site scripting (XSS), HTTP floods, Parameter tampering, Slowloris attacks, SQL injections and Zero-day DDoS attack

Protocol Attacks

- These attacks target the user's resources such as memory, and server resources such as processing capabilities.
- Examples include; Smurf Attacks, SYN floods, Fragmented packet attack and Ping of Death.

Volumetric or Volume-based Attacks

- These attacks focus on a network's bandwidth resources by sending a huge quantity of packets, making the network unavailable to legitimate computing devices and users unable to access the server.
- Examples include: ICMP Flood, UDP floods and other spoofed packet floods.

Types of denial-of-service attacks.

Types of Cyber-attacks (cont.)

II. Denial of service attacks (cont.)

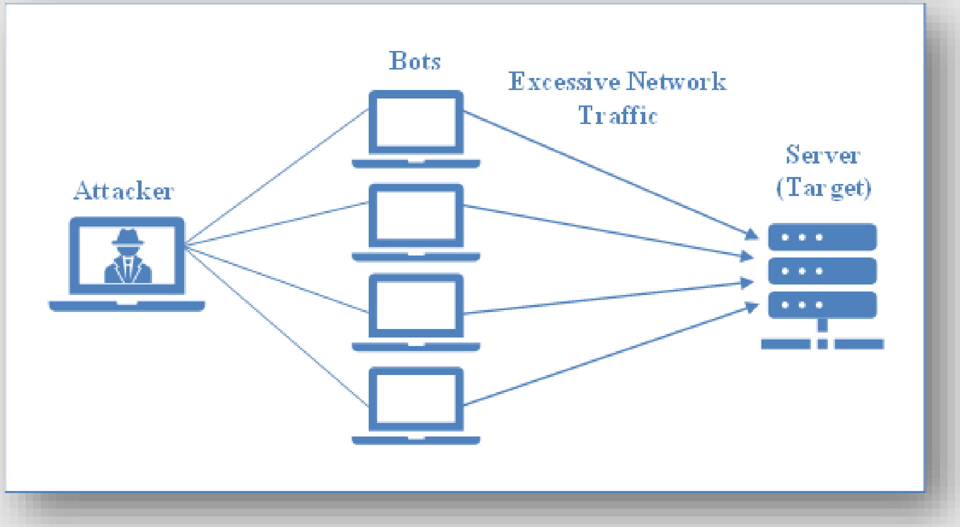
Common DoS attacks

- An Internet Control Message Protocol (ICMP) or ping flood attack.
  - This type of attack happens when a hacker sends ICMP echo requests or pings with the purpose of flooding a computing system.
    - The **ping flood** is the most basic technique used for a DoS attack. The overwhelming number of requests from incoming messages (echo-request) and outgoing responses (echo-reply) consumes a good deal of the bandwidth of a system.
    - A **SYN flood** happens when the attacker exploits weaknesses in the Transmission Control Protocol (TCP) connection sequence, by not supporting the three-way handshake.
    - A **Smurf attack** is a denial of services attack that exploits weaknesses of the Internet Protocol (IP) and Internet Control Message Protocols (ICMP) by using a source code called “smurf”.
    - **Buffer overflow** occurs when a hacker modifies a computer’s memory or overflows the buffer's limit, overwriting memory locations to control program execution and inserting malicious code into the memory of a program.
    - **The Ping of Death**. This attack is like a Smurf attack. It occurs when a hacker manipulates an IP protocol by sending large packets with the maximum value allowed in the IP header to a target.

Types of Cyber-attacks (cont.)

III. **Distributed denial-of-service (DDoS)** attacks are more advanced.

- They occur when multiple computing systems coordinate a synchronized attack.
  - A hacker exploits security vulnerability to take control of multiple computers and turns them into botnets or bots (zombie computers).
  - The hacker then uses the bots to attack other computers or networks.
  - The botnets can be made up of a single handful of bots or thousands of them, located around the world.
  - These infected computers are managed through a command and control server.
  - DDoS attacks provide an opportunity for hackers to gain access to numerous compromised computing devices.



A DDoS attack

Types of Cyber-attacks (cont.)

IV. Malware

- Malware is short for 'malicious software,' and consists of computer viruses, worms, Trojan horses, ransomware, spyware, and other types of destructive software or code.
  - ***Virus*** is a type of malicious code or a program that replicates and spreads from one computer to another after an initial execution.
  - A ***Trojan horse*** is named after famous wooden horse that tricked the Trojans and allowed the ancient Greeks to conquer the city of Troy.
  - A ***Ransomware attack*** occurs when a hacker uses malicious software, usually malware or phishing spam, to extort victims by locking and encrypting their data until the victim pays a ransom in cryptocurrency.
- A ***Spyware*** is a type of malicious software that invades a computing device to gather information.
  - It does not self-replicate, evades detection and runs undetected in the background of a computing device.
- A ***Worm*** is an executable malicious program capable of replicating and distributing itself.
  - In contrast to a virus, a worm does not require user activity to be activated. Usually, worms transmit malware like ransomware.

Types of Cyber-attacks (cont.)

V. Phishing

- Phishing is a deceitful attempt to gather personal information such as usernames, passwords, and credit card information by using deceptive e-mails masked as legitimate.
  - For example, a user may receive an e-mail from a financial institution, asking for ‘missing’ information.
  - The e-mail looks genuine and all the user needs to do is click and answer the questions.
  - When the user clicks on the link, the hacker installs malware which spreads to the user’s network within seconds.

Additional phishing examples

1. Deceptive Phishing is one of the most widely used phishing scams.

The goal is to mislead the user into revealing personal confidential information by imitating a legitimate source. The phishing email usually gives the impression of urgency - that the user needs to act fast.

“I have tried to email this account many times but have received no response. If you receive this email,
Contact me as soon as possible for more details.
Sincerely,
Benjamin Ezeife”

Your account is on hold

Types of Cyber-attacks (cont.)

V. Phishing (cont.)

- More examples

"Hi Dear, we're having some trouble with your current billing information. We'll try again. But in the meantime, you may want to update your payment."

UPDATE ACCOUNT NOW

"Need help? We are here if you need it. Visit the Help Center or contact us now. Your friends at Netflix"

2. Spear Phishing is when an attacker targets specific individuals or groups within an organization or business.

    - The attacker usually needs to gather information on the target to compile a convincing phishing email.
    - Often intended to steal data, an attacker may also intend to install malware on a targeted individual's computer.
    - This technique targets individuals by email, social media, instant messaging (IM), and more.
    - Frequently, a spear phishing technique contains an email and attachment. Social media sites are ideal hunting grounds for phishing attacks.

3. Vishing is a voice phishing technique that uses verbal scams to deceive users into sharing confidential information.

    - Vishing flourishes when a cybercriminal has some information about the victim and uses this knowledge to create a sense of urgency to get the user to perform some type of action.

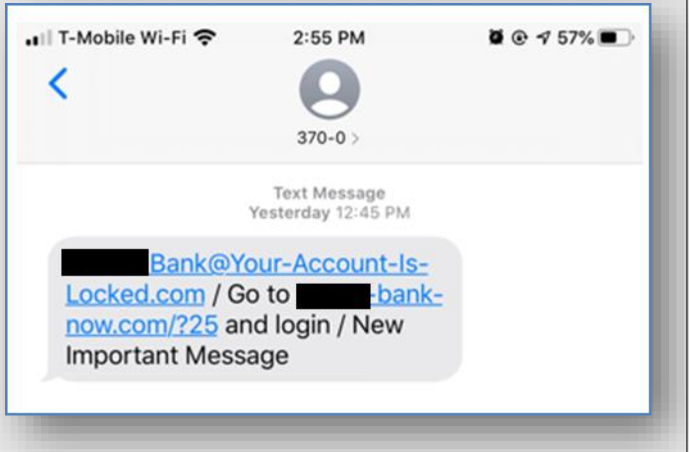
Types of Cyber-attacks (cont.)

V. Phishing (cont.)

3. Smishing is a mixture of texting and phishing that uses text messages instead of emails.

4. Pharming is a combination of two words phishing and farming.
   - The hacker directs an internet user to a fake website instead of a legitimate one.
   - The hacker may install malware on a user's computer that changes the computer's host file in order to direct traffic to a malicious website instead.

5. Social engineering happens when a cybercriminal tricks victims (manipulating) so they give up confidential information, into revealing confidential information, such as usernames and passwords.
   - For example, a cybercriminal could pose as an IT support technician and then trick the victim into providing login credentials.



Text Message
Yesterday 12:45 PM

[redacted]Bank@Your-Account-Is-Locked.com / Go to [redacted]-bank-now.com/?25 and login / New Important Message

Example of smishing technique.

Types of Cyber-attacks (cont.)

VI. Spoofing

Spoofing refers to a deceptive method that tricks the user by hiding a malicious origin as a legitimate source.

Examples of some of common spoofing attacks include:

- Address Resolution Protocol (ARP) spoofing or ARP poisoning is a Man-In-The-Middle (MITM) attack.
- Domain Name Server (DNS) spoofing or DNS cache poisoning occurs when cybercriminals alter the DNS record of URLs and then redirect online traffic to a falsified website by changing its IP address.
- IP Spoofing occurs when hackers modify an IP packet by falsifying its source address.
- MAC Spoofing changes the factory-assigned Media Access Control (MAC), the physical address of a computing device's network interface controller (NIC), also known as a network interface card.
- Website Spoofing occurs when a cybercriminal creates a fake replica of a real website like that of a bank or a university, and when a user logs into the fraudulent website, the hacker obtains the user's credentials.
- E-mail Spoofing occurs when a cybercriminal creates and sends email messages from a forged sender's email address and makes the recipient believe that the email was sent from a legitimate source.

Types of Cyber-attacks (cont.)

VII. Structured Query Language (SQL) Injection or (SQLI)

- Structured Query Language, or SQL, is a programming language used with databases to query the database for specific information.

- SQL Injection is a type of cyber-attack where hackers ‘inject’ malicious SQL code to manipulate the database and gain access to information illicitly.

VIII. Wi-Fi Hacking

- Hackers target Wi-Fi connections and attempt to exploit their vulnerabilities, particularly targeting Wi-Fi in home networks.
- Once the hacker gains access to the network, he will either target the network itself or go after its connected devices.
- The hacker will usually focus on the link with the vulnerabilities that are easiest to exploit.

Types of Cyber-attacks (cont.)

VIII. Wi-Fi Hacking (cont.)

Some of the most common Wi-Fi attacks are the following:

I. Cracking Attacks occur when a hacker uses different password-cracking techniques to break into a Wi-Fi network and gain access. Some of these include:

- Brute force attacks, meaning the hacker uses every possible combination of letters in a series of password-cracking attempts, struggling by trial and error to ‘force’ its way until the correct password is found.
- Dictionary attacks are like brute force attacks but use passwords from a list containing words from the dictionary that many people like to use for their password.
- Phishing, as discussed earlier, is a dishonest attempt to gather personal information, including usernames and passwords.
- Rainbow table is a password cracking technique that uses the rainbow hash table.

Types of Cyber-attacks (cont.)

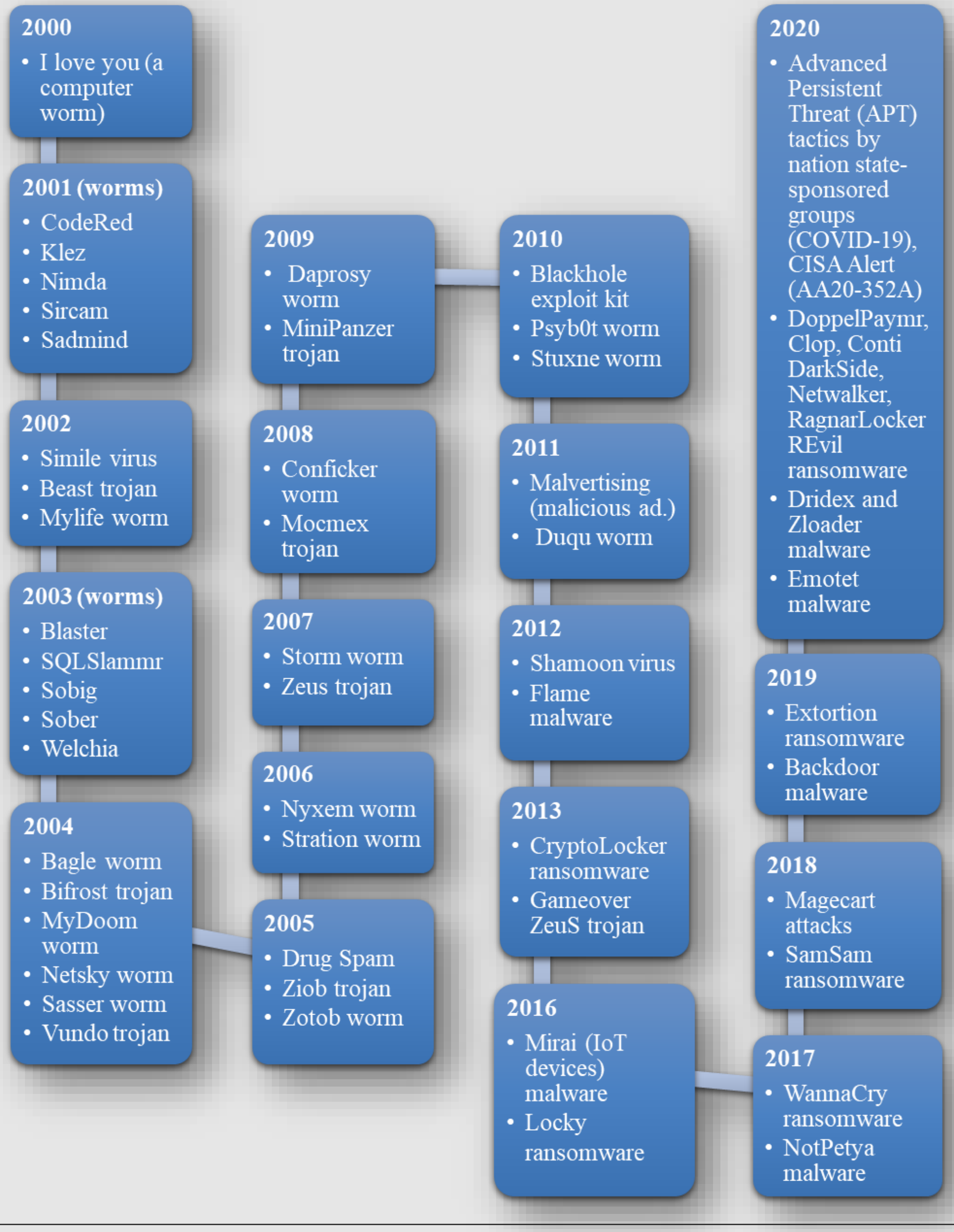
VIII. Wi-Fi Hacking (cont.)

Some of the most common Wi-Fi attacks are the following:

II. Jamming Wi-Fi signals occurs when a hacker blocks a signal, using an illegal jamming device, for the purpose of creating noise and denying users access to a wireless point.

- A Wi-Fi De-authentication attack occurs when a hacker targets a communication when it is traveling between the Wi-Fi Access Point and the device.
- Wi-Fi Protected Setup (WPS) attack. The WPS standard uses a Personal Identification Number, which is an 8-digit pin, or a push button to connect to the router.
- Wi-Fi Protected Access (WPA) consist of a family of Wi-Fi security certifications or security technologies developed by the Wi-Fi Alliance to secure wireless computer networks.
- Man-In-The-Middle (MITM) attacks, a type of cyber eavesdropping that occurs when data sent from point A to point B is intercepted by an attacker.
- Unsecured Wi-Fi connections can be used by hackers to distribute malware.
  - If the user allows file-sharing when using an unsecure Wi-Fi connection, the hacker can easily plant malware on the victim's computer.
  - In some cases, a hacker may create a rogue hotspot and name it with a well-known store or location, hope to trick users into signing on with their devices.

The evolution of the most important attacks



2000
- I love you (a computer worm)

2001 (worms)
- CodeRed
- Klez
- Nimda
- Sircam
- Sadmind

2002
- Simile virus
- Beast trojan
- Mylife worm

2003 (worms)
- Blaster
- SQLSlammr
- Sobig
- Sober
- Welchia

2004
- Bagle worm
- Bifrost trojan
- MyDoom worm
- Netsky worm
- Sasser worm
- Vundo trojan

2005
- Drug Spam
- Ziob trojan
- Zotob worm

2006
- Nyxem worm
- Stration worm

2007
- Storm worm
- Zeus trojan

2008
- Conficker worm
- Mocmex trojan

2009
- Daprosy worm
- MiniPanzer trojan

2010
- Blackhole exploit kit
- Psyb0t worm
- Stuxne worm

2011
- Malvertising (malicious ad.)
- Duqu worm

2012
- Shamoon virus
- Flame malware

2013
- CryptoLocker ransomware
- Gameover ZeuS trojan

2016
- Mirai (IoT devices) malware
- Locky ransomware

2017
- WannaCry ransomware
- NotPetya malware

2018
- Magecart attacks
- SamSam ransomware

2019
- Extortion ransomware
- Backdoor malware

2020
- Advanced Persistent Threat (APT) tactics by nation state-sponsored groups (COVID-19), CISA Alert (AA20-352A)
- DoppelPaymr, Clop, Conti DarkSide, Netwalker, RagnarLocker REvil ransomware
- Dridex and Zloader malware
- Emotet malware

Prevention Mechanisms

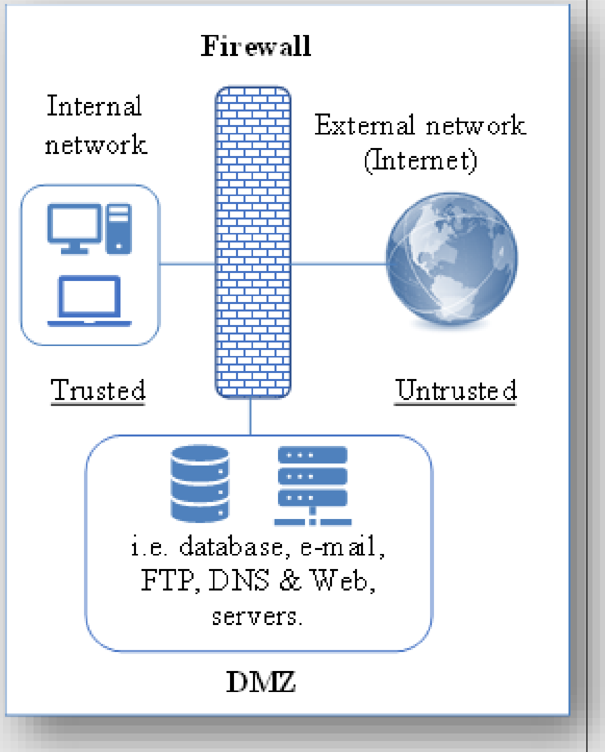
If you connect it, protect it

- A Firewall is a piece of hardware, sometimes a standalone system or part of a router, or software application, or a combination of both, that screens incoming and outcoming traffic to or from a network, according to a defined set of rules.
- Along with firewalls, other systems such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are part of the network security environment.
  - The firewall is the first line of defense, like a fence between a trusted internal network, called the subnet, and the unsafe Internet.
  - The firewall makes sure only specific types of traffic are allowed into and out of a network.
  - The IDS system detects the attack, identifies it using a database of attack types, registers the attack, and sends an alert to an IT administrator if it is malicious.
  - The IPS inspects traffic flowing in the network, looking for anything suspicious, and prevents or blocks a connection that is suspect, provides alerts, and cleans up malicious network traffic to keep it from getting to the rest of the network.
  - Like the IDS, the IPS resides between the firewall and the rest of the network.

Prevention Mechanisms (cont.)

If you connect it, protect it

- The separation between a computing device on an internal network and the internet, or the outside world, is referred to as the Demilitarized Zone (DMZ) or perimeter network.
  - This area sits between the internal network and external network.
  - The Internet cannot establish connections directly to the internal network, but it can establish connections with the DMZ. If you think of network security as an onion, the DMZ is the peel, or first layer of the onion.
- There are several ways to implement a DMZ in a network.
- One way is to use the Single Firewall Model (Figure 1), which requires three network interfaces (devices) or a three-legged firewall.



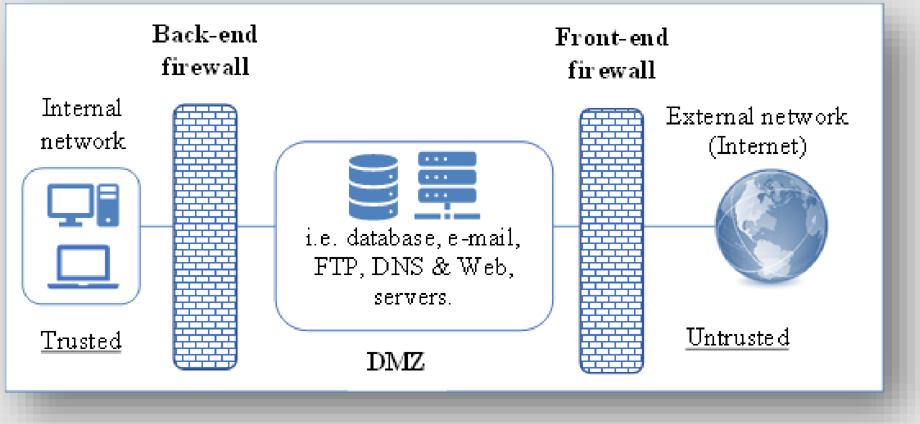
Firewall
Internal network
External network (Internet)
Trusted
Untrusted
i.e. database, e-mail, FTP, DNS & Web, servers.
DMZ

The single firewall model

1. The DMZ will be positioned inside of this firewall.
   - The first network interface, considered Untrusted, is connected into the external public Internet connection.
   - The second interface, considered Trusted, is connected into the internal network or local area network (LAN).
   - The third interface is connected directly into the DMZ.

Prevention Mechanisms (cont.)

2. The Dual Firewall Model utilizes two separate firewalls.
   - One faces the Internet, called the front-end firewall and the other faces the trusted internal network, or subnet, and is called the back-end firewall.
   - The front-end firewall is configured to allow only traffic destined for the DMZ.
   - The back-end firewall is responsible for regulating network traffic on the trusted internal network or traffic from the DMZ to the internal network.
3. Cloud computing has changed the role of the DMZ by allowing secure access between the local or on-premises network and cloud-based networks by through the use of a VPN service to connect the networks.
   - Most companies use cloud service providers and deploy Software-as-a-Service (SaaS) applications.


Back-end firewall
Front-end firewall
Internal network
External network (Internet)
i.e. database, e-mail, FTP, DNS & Web, servers.
Trusted
DMZ
Untrusted

The dual firewall model.

Prevention Mechanisms (cont.)

Types of firewalls

Firewalls use pre-determined rules to analyze incoming traffic at entry points known as ports. Ports are communication endpoints that determine how external devices exchange information and communicate on a network.

Some pre-determine rules include how to handle trusted IP addresses, protocols, port numbers and destination IP addresses.

There are other firewall types based on method of operation and varying levels of security.

Some of the most common firewall types include the following:

I. Packet-filtering firewalls are the most basic type, inspecting inbound packets arriving from the network router. Only packets that match the firewall's criteria are allowed in.

- Packet firewalls can either be stateless or stateful.
  - Stateless firewalls employ older firewall technology and analyze individual packets based on static information like source and destination.
    - This method is not preferred by security professionals because it does not address vulnerabilities such as those leading to DDoS attacks.
  - Stateful firewalls, on the other hand, are more secure and are a significant improvement, because they continuously monitor the network and the active connections.
    - They can recognize the context of incoming traffic and data packets and can detect whether the packet is a part of an abnormal stream as in a DoS attack.
- The packet-filtering firewall is not considered very secure.

Prevention Mechanisms (cont.)

Types of firewalls

II. A Network Address Translation (NAT) firewall allows network devices like routers to connect private IP networks to the Internet by replacing the private IP with a public IP address.

- The NAT acts as "receptionist or a dispatcher" between the public Internet and local network by remapping an IP address space into another one.
- The NAT firewall was developed to improve network security by filtering all incoming traffic, identifying threats and malicious actions, and blocking them.

III. The next generation firewall (NGFW) is one of the most popular firewalls.

- It provides advanced inspection threat beyond what is offered by traditional stateful firewall detection, featuring excellent application awareness and control, and the ability to block malware, prevent intrusion, recognize cloud-based threat intelligence and prevent other security applications from entering a network.

IV. Virtual firewalls or Cloud-based firewalls or Firewall-as-a-Service refer to a virtual appliance located in a private cloud that monitors traffic on physical and virtual networks with cost-efficient solutions.

V. A Web application firewall (WAF) is a type of firewall that blocks, filters, and protects data traveling in and out of web services by analyzing each HTTP & HTTPS request at the application layer.

Identification, Authentication, and Authorization

In computer security it is important to comprehend the difference among these three terms, Identification, Authentication and Authorization.

I. Identification indicates the user's or the thing's identity, for example a username.

II. Authentication, from the Greek word "αὐθεντικός" authentikos, meaning real or legitimate, is the method that confirms the user's identity and provides access to a computer system, for example, checking the accuracy of a password.

- Password authentication is the most common method of confirming a user's identity, but passwords have many weaknesses and are susceptible to phishing attacks and password cracking techniques.
- Because complicated passwords are hard to remember, users tend to choose convenience over security, hence the '12345' password.
- Multi-factor authentication (MFA), sometime referred to as two-factor authentication (2FA), which means requiring two or more ways to identify a user.
  - For example, users can receive one-time passwords (OTP), requiring a code that is often received via e-mail, text, or from a mobile app like the Google Authenticator.
  - For additional security, a biometric authentication like fingerprint, face recognition, IRIS scan, or voice recognition can be used. Another security measure is the use of a hardware-based security key based on the FIDO U2F standard.
  - FIDO is administered by the FIDO Alliance and is a set of protocols intended to support authentication methods including biometrics, Bluetooth technology, Near-Field Communication (NFC) for mobile devices, and USB security tokens.
  - Some popular security keys are Yubico's YubiKey, CryptoTrust OnlyKey, Thetis Fido U2F Security Key, and Google Titan Security Keys.

Identification, Authentication, and Authorization (Cont.)

II. Authentication (cont.)

- Users can authenticate with the following authentication factors:
  - Something the user knows, such as a password, a PIN, or answers to a set of questions.
  - Something the user has, such as a smart card or a hardware-based security key.
  - Something the user is or does such as biometric characteristics.

- Biometric authentication includes physiological, including fingerprints, face recognition, palm vein scan, iris scan, retinal pattern, and DNA, and behavioral, including voice pitch, typing patterns, and signature.
- Token-based authentication requires a unique generated encrypted code, or token, to verify the user’s identity.
  - The token can be sent to a mobile app or a small hardware device.
  - An example of a token is the RSA SecurID token offered in RSA SecurID two-factor authentication.

III. Authorization

- Authorization happens when a user is provided with certain privileges or permissions to access computer systems or resources such as databases, files, services, computer programs, and applications.
- Authorization access is based on the level of assigned permissions given to the user, as defined by certain conditions.

Modern Encryption

- The need for people to exchange data easily and securely became more important with the introduction of computers.
- Encryption is one of the most effective way to protect data by scrambling data into secret codes, called ciphers, as they travel across the Internet.
- Complex encryption algorithms have been developed that are hard to break.
- A general understanding of modern encryption methods that can protect data at rest, data in transit, and data in use.
- It can also keep data safe from lost and stolen computers.
- Encryption can also be used by cybercriminals to encrypt data after a ransomware attack making it almost impossible retrieve and use.
- Encryption can be good or evil, protecting us or used as a weapon against us.
- We can’t cover all the different types of encryption algorithms, but we will look the most common.

Symmetric Encryption or Secret Key Cryptography (SKC)

- Symmetric encryption method, also refers to as symmetric key cryptography, secret key, or shared secret, is a method that uses the same key to both encrypt and then decrypt a message.

  - A simple example of symmetric encryption is the Caesar Cipher, which shifts each letter a fixed number of places.

  - Another example occurred in 1586, when Blaise de Vigenère used an entire word as the shift key. In symmetric encryption, both parties must have the same secret key or else know the code to decrypt the message.

  - Since the device uses only one key for both encryption and decryption, symmetric encryption may be vulnerable.

  - Another drawback to symmetric encryption is that all parties must exchange the key (key sharing), to encrypt and decrypt data, and this is not always convenient.

Symmetric Encryption or Secret Key Cryptography (SKC) (cont.)

A symmetric key cipher can be Block Cipher or Stream Cipher.

I. Block Cipher is used to encrypt blocks of data, frequently 64 or 128-bits.

- For example, the cipher may encrypt a 64-bit block and will return the blocks of cipher text in the same size.

II. A Stream Cipher starts with a secret key, or ‘seed’, and generates a keystream or stream of random or pseudorandom characters that combines the stream with the plain text to produce the ciphertext.

Symmetric Encryption or Secret Key Cryptography (SKC) (cont.)

Some examples of symmetric encryption algorithms include:

- Data Encryption Standard (DES) (uses 56-bit key length)
- Advance Encryption Standards (AES) (uses 128-bit, 192-bit or 256-bit keys)
- Blowfish (key lengths very from 32 to 448-bits length)
- RC4 (Rivest Cipher 4) (key can be any length up to 2048-bits)
- RC5 (Rivest Cipher 5) key size up to 2040-bits)
- RC6 (Rivest Cipher 6) (key sizes of 128, 192, and 256 bits up to 2040-bits)
- 3DES (uses key length 56, 112, or 168-bits)
- IDEA (International Data Encryption Algorithm) (encrypts 64-bit blocks using 128-bit key) and ChaCha20 (Google has replaced RC4 with ChaCha20 stream cipher) algorithms.
- Another stream cipher the Salsa20 which is related to ChaCha20 take a 256-bit key. So far, researchers have not found any vulnerabilities in ChaCha20 algorithm.

2^{32} = 4,294,967,296 (4.3 billion).

2^{64} = 18,446,744,073,709,551,616 (18.4 quintillion)

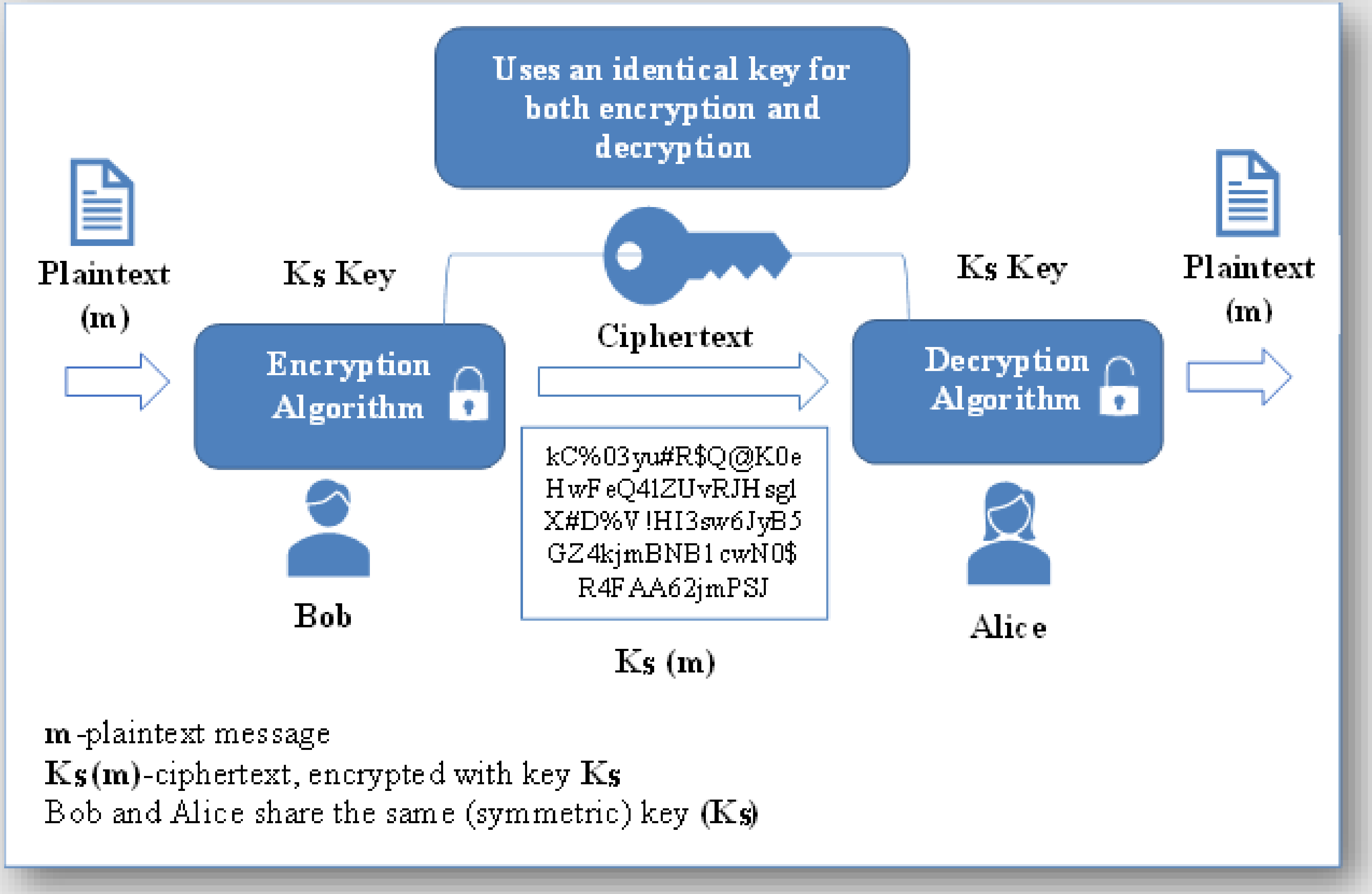
2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456 (340 undecillion, 282 decillion, 366 nonillion, 920 octillion, 938 septillion…..).

The length of the AES encryption

The key lengths indicate the number of bits in a solution used by a cryptographic algorithm.

- In 1970s, IBM developed its Data Encryption Standard (DES), which was the first major symmetric algorithm developed for computers in the United States.
- The DES's input key is 64 bits long, and the actual key used is 56-bits.
- This 56-bit key refers to the size of the key used to encrypt data. The 56-bit key can result in over 70 quadrillion possible combinations.
- If a computer tries 2^{40} (1,099,511,627,7760) solutions per day, it will take approximately about 848 sextillion years to brute-force the solution to a 128-bit key.

Symmetric Encryption or Secret Key Cryptography (SKC) (cont.)



m -plaintext message

Ks(m)-ciphertext, encrypted with key **Ks**

Bob and Alice share the same (symmetric) key (**Ks**)

Asymmetric Encryption or Public Key Cryptography (PKC) or Asymmetric cryptography

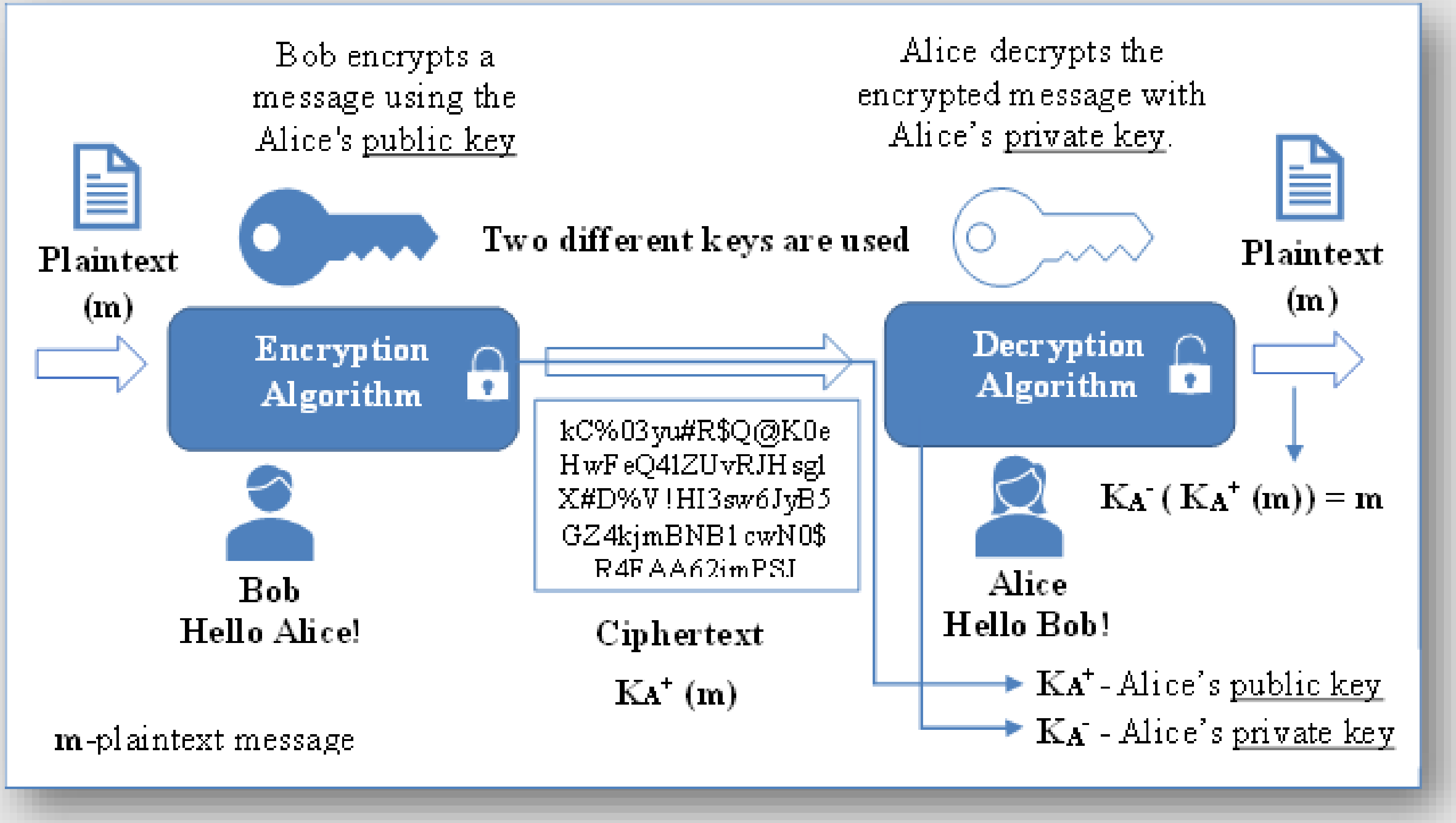
- In 1976, a revolutionary paper by Whitfield Diffie and Martin Hellman titled *“New Directions in Cryptography”* proposed a major change.
- The two researchers, along with Ralph Merkle, were the first to publish t cheoncepts of Public Key Cryptography, and they received US patent 4200770, for it.
- This type of encryption uses two mathematically different but connected cryptographic keys.
- Instead of a single key as in symmetric encryption, the public-key encryption system uses a pair of keys.
- **One key is public,** and the other is a **private, or secret key.**
- The public key may be accessed by anyone, and the private key only by the owner.

Asymmetric Encryption or Public Key Cryptography (PKC) or Asymmetric cryptography (cont.)

The sender encrypts a message using the receiver's public key; however, the receiver can only decrypt this encrypted message with his or her private key. One key will not reveal the other.

- The keys are linked mathematically so that anything encrypted with key ‘A’ can only be decrypted with key ‘B’.
- A sender can use a recipient's public-key to encrypt the message; then, only the recipient can decrypt using his or her private key.
- Or, the message can be encrypted using both the sender’s private key and the recipient’s public key.
- If the sender encrypts a message with his private key, it can be decrypted by anyone that has the matching public key.
- A recipient with the sender's public key can verify that it was the sender who created the message.
- This is called a digital signature. In other words, the sender and recipient only need to exchange public keys, which can be done over open communication lines.
- Because the public key is available to everyone, other parties can use it to encrypt messages.
- As a result, every user must generate a pair of public and private keys.
- The mathematics behind the asymmetric encryption are extraordinarily complex and beyond the scope of this chapter.
- The public and private keys are associated with each other via a mathematical relationship. It is not feasible to calculate the private key from the public key because the mathematical relationship cannot work backwards.
- In comparison with symmetric encryption, asymmetric encryption is much slower but offers better security because of the two different keys.

Asymmetric Encryption or Public Key Cryptography (PKC) or Asymmetric cryptography (cont.)



Bob encrypts a message using the Alice's public key

Alice decrypts the encrypted message with Alice's private key.

Plaintext (m)

Two different keys are used

Plaintext (m)

Encryption Algorithm

Decryption Algorithm

kC%03yu#R$Q@K0e
HwFeQ41ZUvRJHsgl
X#D%V!HI3sw6JyB5
GZ4kjmBNB1cwN0$
R4FAA62imPSJ

Bob
Hello Alice!

Ciphertext

$K_A^+(m)$

Alice
Hello Bob!

$K_A^-(K_A^+(m)) = m$

K_A^+ - Alice's public key

K_A^- - Alice's private key

m-plaintext message

The Asymmetric Encryption or Public Key Cryptography (PKC)

Digital Certificates and Certificate Authority (CA)

In cryptography, public key certificates are widely distributed by the Certificate Authority (CA).

- The CA consists of trusted third parties that validate the identities of an entity by issuing digital certificates like e-mail addresses, and websites, to individual users.
- Think of these digital certificates as passports or electronic ID cards that establish the identity of an ID holder.
- Essentially, the public key certificate certifies ownership of the public key.
- To be able to generate a new digital certificate, the applicant or owner needs to generate a Certificate Signing Request (CSR) along with a pair of private and public keys on the computing system where the certificate will be installed.
- This request provides information about the applicant.
- Then, the Certificate Authority (CA) verifies the information, and issues, or 'signs', the certificate, that now contains a public key and the identity of the applicant.
- The matching private key is kept secret by the user. In other words, the CA confirms that the public key enclosed in the certificate belongs to the owner of the computing system in the certificate.

Digital Certificates and Certificate Authority (CA) (cont.)

- Digital certificate technology is based on public key cryptography, where every entity has two keys, public and private, that work only when they are used together and act as keys to a user's encryption scheme.
- A digital certificate links the public and private key with its owner and allows a user to verify to whom a certificate has been issued.
- The Certificate Authority makes sure that the owner is not claiming a false identity.
- The user keeps the private key in a secure location and does not share it, while the public key is sent to every user with whom the user wants to communicate.
- The most common international framework for digital certificates is defined by the X.509 standard.
- The contents of an X.509 certificate include:
  - Issuer's distinguished name.
  - Subject; contains owner’s information.
  - Public key; contains the actual public key.
  - Certificate; serial number of the certificate.
  - Digital signature of issuer.
  - Validity period; when issued and date of expiration.

Digital Certificates and Certificate Authority (CA) (cont.)

Some certificate providers are Comodo, IdenTrust, GeoTrus, Network Solutions, RapidSSL, Symantec, Thawte, DigiCert, GoDaddy, GlobalSign and Trustwave.

- The Certificate Authority can verify a bank's website.
- Therefore, when we connect to the website, we can be sure that it is the real website and not a fraud.
- The digital certificate for the bank's website is issued by the same Certificate Authority.
- A public key from the user's browser encrypts data, such as deposits and withdrawals, and send them to the bank's website.
- The private key from bank's website decrypts the data sent by the browser.

Hash functions or Hashing Algorithms

- The hash algorithm converts data or a message of any length to a fixed length.
- We call this ‘hashing the data.’ The hash will be smaller than the data it represents.
- The purpose of hash functions is data integrity.
- A hash algorithm (H) accepts a variable length of data (M) as input and produces a fixed-length output hash value (h). h=H(M).
- When we change any bit or bits of (M) this results in a change to the hash code.
- To be able to find the solution to a hash message, one must guess it by trying a brute force attack, where the attacker inputs random passwords to see if they match, or by use of a rainbow table of matched hashes.
- The hash is an encryption process that converts plain input text to encrypted hash value using a mathematical algorithm.
- Instead of storing a password in plain text, computers generate and store passwords using hash functions.

Hash functions or Hashing Algorithms (cont.)

What does ‘Salting’ a hashtag mean?

- In hashing, the term “Salt” describes a unique use of random characters added to a one-way function. Salting uses the additional input to safeguard password hashes against dictionary attacks.
- A new salt is randomly generated for each password and increases the computational power of hashed passwords.
- In other words, the Salt and the password are concatenated and processed, make a password hash output unique and much less vulnerable to attack.
- For example, if Bob and Alice use the same password, such as 123456, both would share the same hash.
  - The hacker can predict the password that maps to that hash value by using dictionary and brute-force attacks.
  - If the password is known, the hacker can access all the accounts that use the hash.
  - With Salt added before the hashing process, the passwords are unique, and can better safeguard passwords in storage.
  - If we take the most common password, 123456, by applying the Secure Hash Algorithm (SHA-256), the password will be stored as

b59936bb842a7bcccc54004091069467d78b85b7372e0f843c2b346c186daa14

  - When Salt is added A1ndQngn2m3 to the password 123456, and we hash it then, the salted input becomes:123456A1ndQngn2m3
  - As a result, the hash algorithm will be something like this

70c1e0b744121ea8197422639cfee796282696f1b1070165186b1e446abada94

Hash functions or Hashing Algorithms (cont.)

The length of the hash depends on the hashing algorithm. Some common hashing algorithms include.

- Message Digest Algorithm 5 (MD5) was introduced in 1992 and creates 128-bit outputs.
  - The MD5 algorithm has been shown to have weaknesses which make it easy to break.
  - Although a hash function is designed to work only in one direction, MD5 is easy to reverse.
- Secure Hash Algorithm (SHA) family
- SHA-1 was design by the National Security Agency (NSA) in 1993 and creates 160-bit hash values.
- SHA-2 creates hash values with 224-bit, 256-bit, 384-bit or 512-bits. I
  - t was designed by the NSA in 2001 and is recommended for secure hashing.
  - The SHA-2 hash algorithm is an essential part of creating a digital signature.
- SHA-3 is the latest version of SHA family and was developed by the NSA in 2012.
  - It is designed to protect against brute-force attacks.

ANY QUESTIONS?