Cybersecurity

22CIE55

COURSE OBJECTIVES

- Gain a comprehensive understanding of cybersecurity principles, including definitions, challenges, and human factors.
- Analyze the origins, categories, and methods of cybercrimes, including tools and defenses.
- Examine vulnerabilities in software platforms and operating systems, and strategies for prevention, detection, and mitigation.
- Educate on the security requirements and risk management strategies for databases and cloud environments.
- Introduce security concerns of cyber-physical systems (CPS) and guide on using threat intelligence tools and recovery processes.

COURSE OUTCOMES

- Understand and articulate key principles and challenges of cybersecurity, including human factors and the cybersecurity kill chain.
- Identify and describe various categories of cybercrimes and implement appropriate tools and methods for defense.
- Recognize, prevent, and mitigate vulnerabilities in software and operating systems, ensuring secure software lifecycle processes.
- Understand security requirements for databases and cloud environments, employing risk analysis and security tools to protect data and services.
- Assess security and privacy concerns of CPS, apply threat intelligence tools, and manage investigation and recovery processes following cybersecurity incidents

Syllabus

- ..\..\..\CBIT\AI AND DS DEPT\CS 2024\AUDIT 1 2024-25\cyber security syllabus.pdf

Cybersecurity: Definition

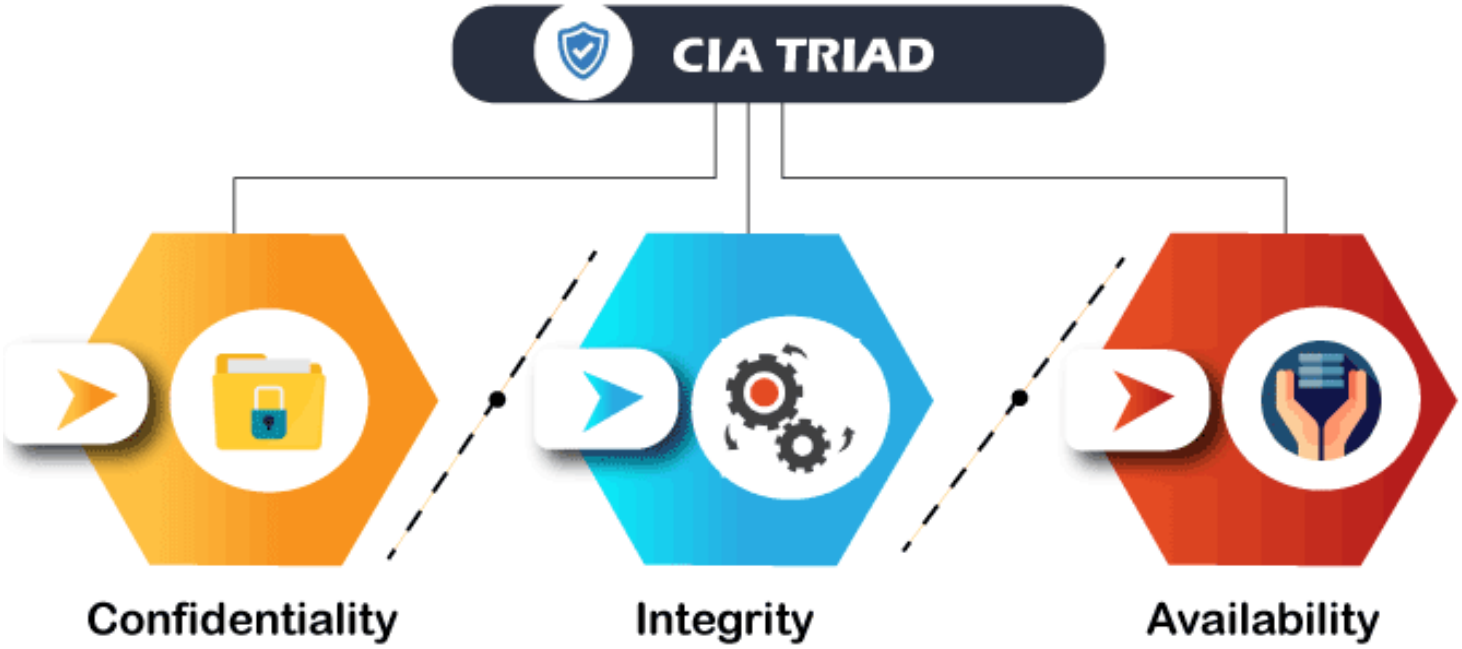
- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
- Cybersecurity is the protection of internet-connected systems such as hardware, software, and data from cyberthreats.
- Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks.

Cyber Security Definition

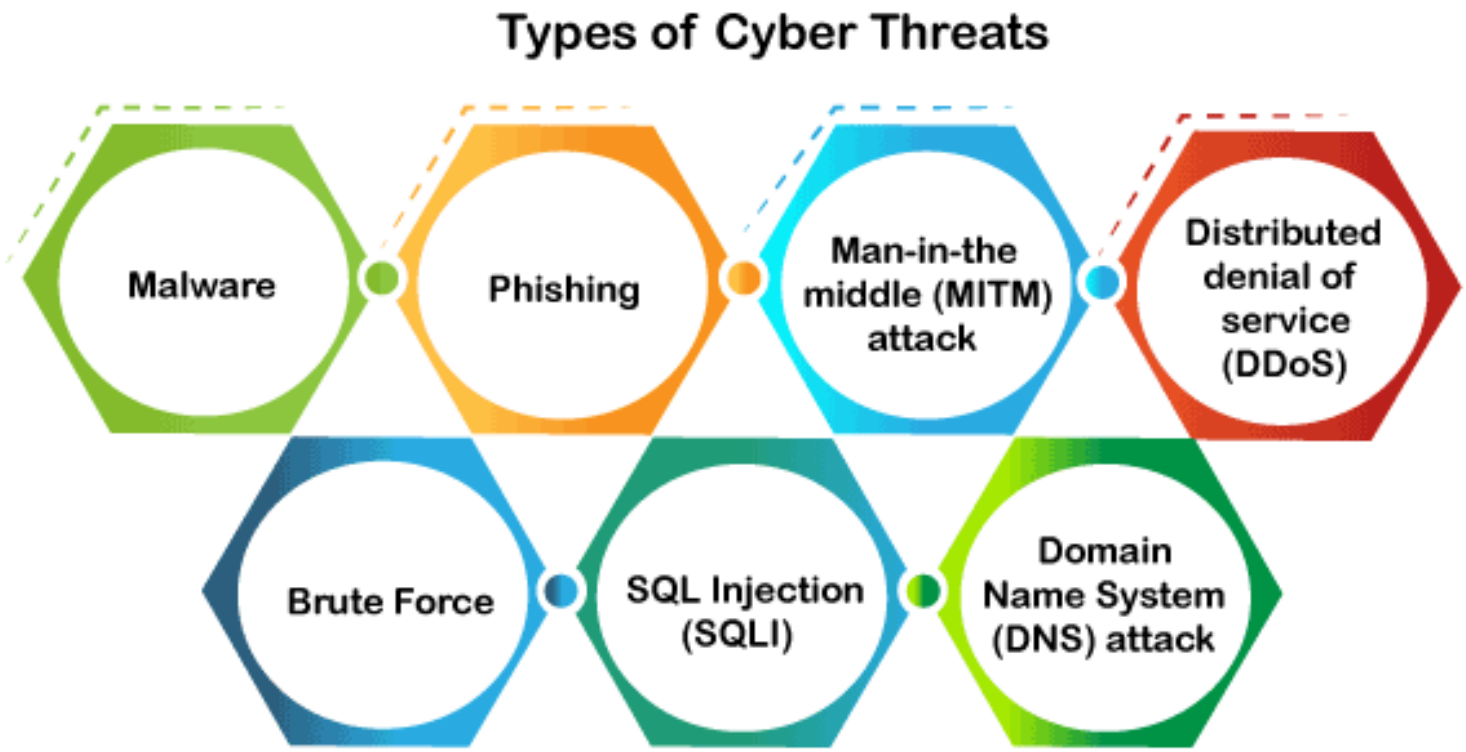
- Cyber security refers to the protection of information systems (hardware, software, and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

- Information security is a large contributor to the notion of cyber security, widely regarded as comprised of three main elements: confidentiality, integrity, and availability of information. Other properties, such as authenticity, accountability, non-repudiation, and reliability, can also be involved.

Cyber Security Goals



Types of Cyber Security Threats



CyBOK Knowledge Areas

The CyBOK (**Cyber Security Body of Knowledge**) is divided into nineteen top-level Knowledge Areas (KAs), grouped into five broad categories:

1. Human, Organisational, and Regulatory Aspects
2. Attacks and Defences
3. Systems Security
4. Software and Platform Security
5. Infrastructure Security

- These categories capture knowledge relating to cyber security per se, making sense of some of that knowledge, and providing auxiliary and background knowledge in diverse fields such as law.

Saltzer and Schroeder Principles

- **Economy of mechanism**: Keep the design as simple as possible.
- **Fail-safe defaults**: Operations should be denied by default.
- **Complete mediation:** Every access must be checked.
- **Open design:** Security should not depend on secrecy.
- **Separation of privilege:** Multiple parties should be involved in decision-making.
- **Least privilege:** Grant the minimum necessary permissions.
- **Least common mechanism:** Minimize shared resources.
- **Psychological acceptability**: Security mechanisms should be easy to use.
- **Work Factor:** the cost of circumventing a security mechanism should be compared with the resources of a potential attacker when designing a security scheme.
- **Compromise Recording :**it is more desirable to record the details of intrusion that to adopt a more sophisticated measure to prevent it.

NIST Principles

The NIST principles extend the Saltzer and Schroeder principles and are categorized into three families:

1. **Security Architecture and Design:** Clear abstraction, modularity, layering, and hierarchical trust.
2. **Security Capability and Intrinsic Behaviours:** Economic security, performance security, human-factored security.
3. **Life Cycle Security:** Secure evolvability, trusted communication channels, and self-reliant trustworthiness.

Old Techniques and Broader Results

- According to the Kaspersky Global IT Risk Report 2016, the top causes for the most costly data breaches are based on old attacks evolving over time:

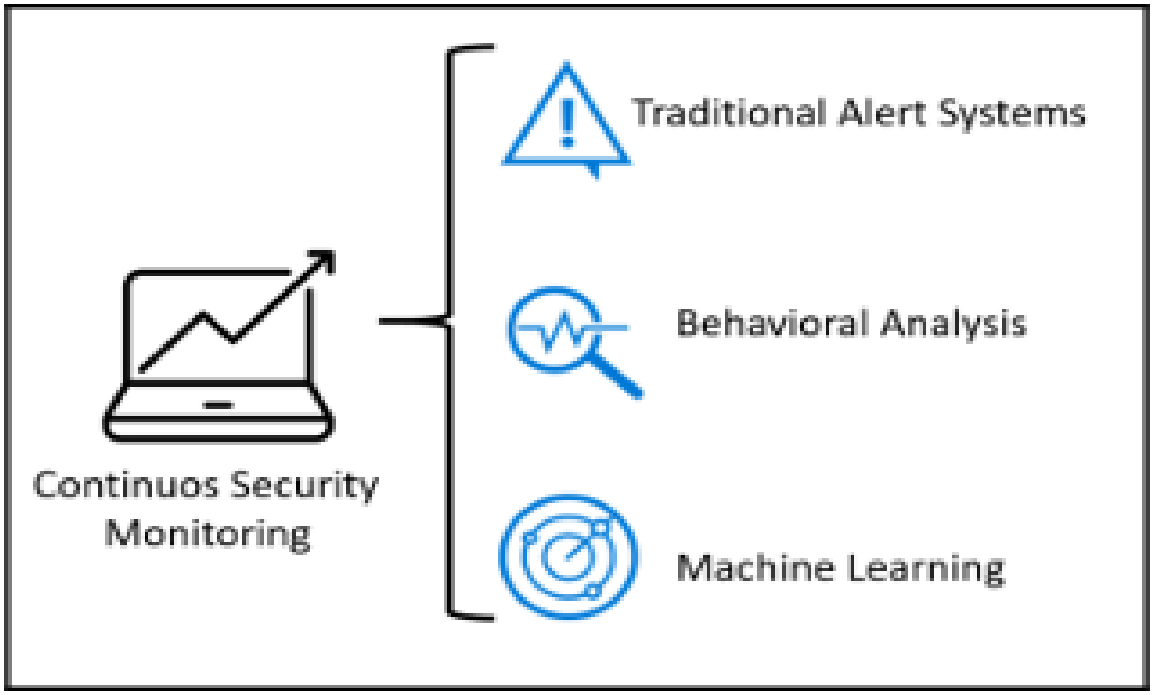
  - Viruses, malware, and trojans
  - Lack of diligence and untrained employees
  - Phishing and social engineering
  - Targeted attack
  - Crypto and ransomware

- These attacks, especially those correlated with human error, continue to pose significant challenges. The targeted attacks involve a specific focus, prolonged access, and data exfiltration, making them particularly difficult to detect and mitigate.

The Shift in the Threat Landscape

- In 2016, a significant shift in the threat landscape occurred when Russian intelligence-affiliated adversaries were found in the United States Democratic National Committee (DNC) network Known as Cozy Bear and Fancy Bear, these groups exemplify government-sponsored cyber attacks aimed at data exfiltration and information warfare.

Continuous security monitoring must leverage at least the three methods shown

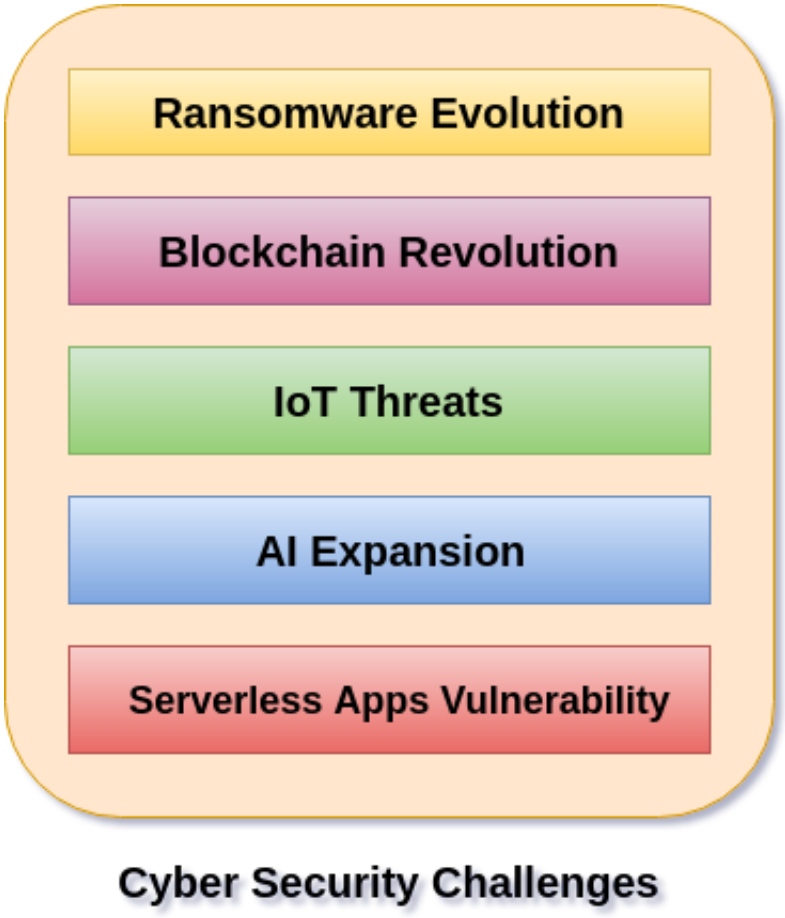


Enhancing Your Security Posture

To address the evolving cybersecurity challenges, organizations must enhance their security posture by:

- Solidifying protection systems across devices
- Enhancing detection systems to quickly identify attacks
- Reducing the time between infection and containment by improving response processes
- Investing in threat intelligence, machine learning, and analytics is crucial to staying ahead of potential threats.

TASK-1 -Cybersecurity challenges



Cyber Security Challenges

Prepare a report on "how do these challenges impact security"?

Cybercrime: Definition and Origins of the word

Cybercrime: "a crime conducted in which a computer was directly and significantly instrumental."

Alternative definitions of Cybercrime are as follows:

1. **Any illegal act** where a special knowledge of computer technology is essential for its perpetration (to commit a crime), investigation or prosecution.
2. **Any traditional crime** that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
3. **Any financial dishonesty** that takes place in a computer environment.
4. **Any threats to the computer** itself, such as theft of hardware or software, damage and demands for money.
5. **"Cybercrime (computer crime)** is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them."

The term “cybercrime” relates to several **other terms** that may sometimes be used to describe crimes committed using computers.

- Computer-related crime
- Computer crime
- Internet crime
- E-crime
- High-tech crime, etc. are the other synonymous terms

Two types of cybercriminal attack

The legal systems around the world introduce laws to combat cybercriminals' attacks. Two types of attack are as follows.

1. Techno-crime: An act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system. Ex: hacking, phishing, malicious software

2. Techno-vandalism: These acts of "brainless" defacement of websites and other activities, such as copying files and publicly publicizing their contents, are usually opportunistic. Ex: ATM attacks, Bluetooth attacks, application misuse, satellite dish crimes etc. "Tight internal security" and "strong technical safeguards" should prevent the vast majority of such incidents.

There is a very thin line between the two terms "computer crime" and "computer fraud"; both are punishable

How do cybercrimes differ

Cybercrimes (harmful acts committed from or against a computer or network)

differ from most crimes in four ways:

(a) how to commit them is easier to learn.

(b) they require few resources relative to the potential damage caused.

(c) they can be committed in a jurisdiction without being physically present in it.

(d) they are often not clearly illegal.

Important Definitions related to Cyber Security

- Cyberterrorism→ terrorist intent
- Cybernetics→ information and its use
- Phishing→ an attack using mail programs
- Cyberspace→ humans interact over computer networks.
- Cybersquatting→ encourages the subject to buy the domain from them
- Cyberpunk → “anarchy” via machines
- Cyberwarfare→ information attacks against an unsuspecting opponent’s computer networks, destroying and paralyzing nations

CYBER OFFENSES- How Criminals Plan Cyber Attacks

- Criminals use many methods and tools to locate their target's vulnerabilities. The target can be an individual and/or an organization. Criminals plan passive and active attacks.
- Active attacks are usually **used to alter the system** (i.e., computer network) whereas passive attacks attempt to **gain information** about the target.

Phases involved in planning cybercrime:

1. Reconnaissance (information gathering)
2. Scanning and scrutinizing the gathered information
3. Launching an attack (gaining and maintaining the system access)

Categories of Cybercrime

Cybercrime can be categorized based on the target of the crime and whether the crime occurs as a single event or as a series of events.

1. Crimes targeted at individuals: Financial fraud, sale of non-existent or stolen items, child pornography, copyright violation, harassment, etc.
2. Crimes targeted at property: Stealing mobile devices, transmitting harmful programs, disrupting systems.
3. Crimes targeted at organizations: Cyber terrorism, damaging programs and files, stealing private information.
4. Single event of cybercrime: For example, opening an attachment that contains a virus.
5. Series of events: For example, interacting with the victim to establish a relationship and then exploiting that relationship.

Tools and Methods Used in Cybercrime

Forms of Cyber Attacks

Cyber attacks can take various forms, targeting different aspects of computer systems and networks:

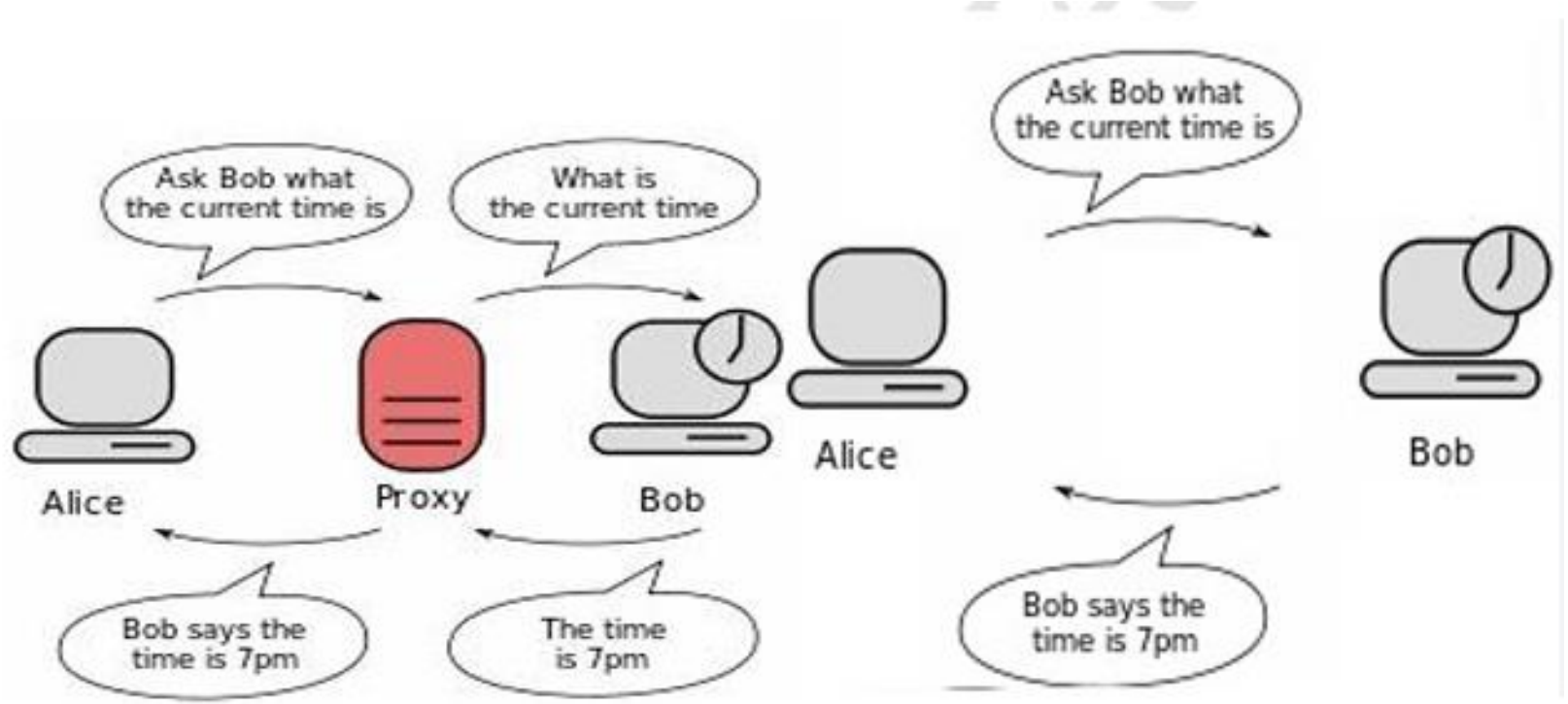
1. Initial Uncovering: Attackers gather information about the target using reconnaissance techniques.
2. Network Probe: More invasive techniques are used to scan the target system.
3. Crossing the Line Toward E-crime: Attackers exploit vulnerabilities to gain access.
4. Capturing the Network: Attackers install tools to maintain control over the network.
5. Grab the Data: Attackers steal confidential data and exploit it for malicious purposes.
6. Covering Tracks: Attackers hide their activities to avoid detection.

Tools and Methods Used in Cybercrime

Cybercriminals use a variety of tools and methods to conduct their attacks:

1. Proxy Servers and Anonymizers: Hide the attacker's identity and location.
2. Phishing: Deceive victims into providing confidential information.
3. Password Cracking: Recover or guess passwords to gain unauthorized access.
4. Keyloggers and Spyware: Monitor and record keystrokes and other activities.
5. Viruses and Worms: Infect systems to cause damage or spread malicious code.
6. Trojan Horses and Backdoors: Provide unauthorized access and control.
7. Steganography: Hide information within other files.
8. DoS and DDoS Attacks: Disrupt services by overwhelming the target with traffic.

. Proxy Servers and Anonymizers

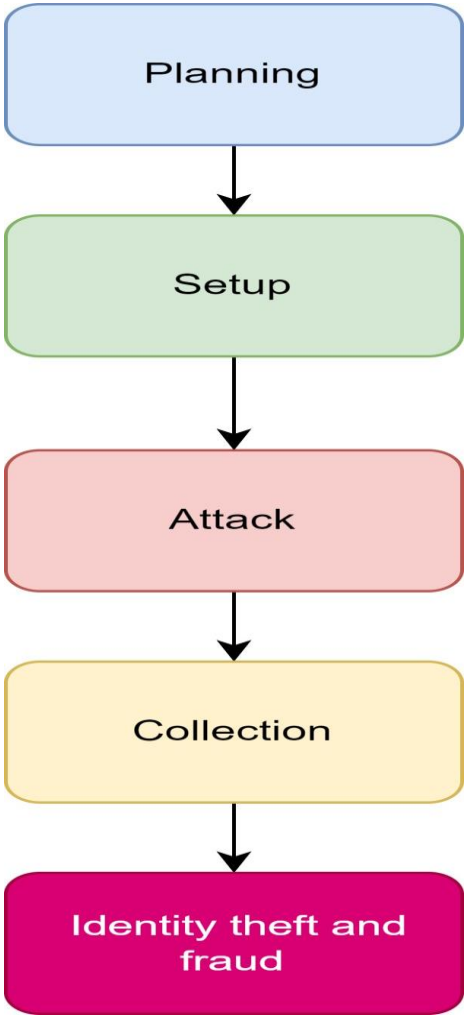


Proxy Servers and Anonymizers

- *Proxy server* is a computer on a network which acts as an intermediary for connections with other computers on that network.
- A proxy server has following purposes:
  - **1.** Keep the systems behind the curtain.
  - **2.** Speed up access to a resource (through “caching”).
  - **3.** Specialized proxy servers are used to filter unwanted content such as advertisements.
  - **4.** Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address.
- *An anonymizer* or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable.
- It accesses the Internet on the user’s behalf, protecting personal information by hiding the source computer’s identifying information.

Phishers work as follows

- **Planning**: Criminals called as a phishers, decide the target & determine how to get an Email address
- **Setup**: Once phishers know which business/business house to spoof and who their victims are, they create methods for delivering the message & collect the data about the target.
- **Attack**: Phisher sends a phony message that appears to be from a reputed source
- **Collection**: Phisher records the information of victims entering into web pages or pop-up window
- **Identity theft and fraud**: Phishers use Information that they have gathered to make illegal purchases and commit fraud.



Password Cracking

Manual password cracking is to attempt to logon with different passwords. The attacker follows the following steps:

- Find a valid user account such as an Administrator or Guest;
- Create a list of possible passwords;
- Rank the passwords from high to low probability;
- Key in each password
- Try again until a successful password is found.

Passwords can be guessed sometimes with knowledge of the user's personal information. Examples of guessable passwords include

1. Blank (none);
2. The words like "password," "passcode" and "admin";
3. Series of letters from the "QWERTY" keyboard, for example, qwerty, asdf or qwertyuiop
4. User name or login name;
5. Name of user's friend/relative/pet;
6. User's birthplace or date of birch, or a relative's or a friend’s;
7. User's vehicle number, office number, residence number or mobile number;
8. Name of a celebrity who is considered to be an idol (e.g., actors, actress, spiritual gurus) by the user.

Password Cracking tools

- iMobie AnyUnlock
- SIMUnlockPro
- UnlockBoom
- CrackStation
- Password Cracker
- Brutus Password Cracker
- Aircrack
- RainbowCrack
- THC Hydra
- Cain and Abel
- Medusa
- John The Ripper
- ophCrack
- WFuzz

- Password cracking
  - Online attacks
  - Offline attacks

Online attacks

1. An attacker can create a **script file (i.e., automated program**) that will be executed to try each password in a list, and when matches, an attacker can gain access to the system.
2. 2. Popular Online attack is **Man-in-the-middle (MITM)** attack/ **"bucket-brigade attack"/Janus attack.**
   - It is a form of eavesdropping, here attacker establishes a connection between a victim and the server to which the victim is connected. When a victim client connects to the fraudulent server **The MITM server intercepts the call**, hashes the password, and passes the connection to the victim server.
   - It is used to obtain **the passwords for E-mail accounts** on public websites such as Yahoo, Hotmail, and Gmail.
   - It is also used to get **the password for financial websites,** to gain access to banking websites.

Offline attacks

- Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used.
- Offline attacks require physical access to the computer and **copying the password file** from the system onto removable media.

Keyloggers and Spyware

- **Key loggers** also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved to a file, and that file is accessed by the person using this malware. Key loggers can be software or can be hardware.
- **Working:** Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983.
- **Software keyloggers** and **hardware keyloggers** are available

Software key-loggers : Software key-loggers are the computer programs that are developed to steal the password from the victim's computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also, Microsoft windows 10 also has key-logger installed in it.

1. **JavaScript-based key logger** – It is a malicious script that is installed into a web page, and listens for the key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file (**Remote Access Trojan**).
2. **Form-Based Key loggers –** These are key-loggers that activate when a person fills a form online and when clicking the button submit all the data or the words written via file on a computer. Some key-loggers work as an API in running an application it looks like a simple application and whenever a key is pressed it records it.

Hardware Key-loggers: These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit that is attached to a keyboard itself whenever the key of that keyboard is pressed it gets recorded.

1. **USB keylogger** – There are USB connector key-loggers which has to be connected to a computer and steals the data. Also, some circuits are built into a keyboard so no external wire i used or shows on the keyboard
2. **Smartphone sensors** – Some cool android tricks are also used as key loggers such as an android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique's accuracy is about 80%. Nowadays crackers are using keystroke logging Trojans, it is malware which is sent to a victim's computer to steal the data and login details.

Prevention from key-loggers

1. **Anti-Key-logger –** As the name suggests these are the software which are anti / against key loggers and the main task is to detect key-loggers from a computer system.
2. **Anti-Virus –** Many anti-virus software also detect key loggers and delete them from the computer system. These are software anti-software so these can not get rid of the hardware key-loggers.
3. **Automatic form filler –** This technique can be used by the user to not fill forms on a regular bases instead use automatic form filler which will give a shield against key-loggers as keys will not be pressed.
4. **One-Time-Passwords –** Using OTP's as password may be safe as every time we log in we have to use a new password.
5. **Patterns or mouse-recognition –** On android devices used pattern as a password of applications and on PC use mouse recognition, mouse program uses mouse gestures instead of stylus.
6. **Voice to Text Converter** – This software helps to prevent Keylogging which targets a specific part of our keyboard.

Spyware

- **Spyware** is **malicious software** that enters a user's computer, **gathers data from the device and user, and sends it to third parties** without their consent. A commonly accepted spyware definition is a strand of malware designed to access and damage a device without the user's consent.
- Ex:

007 Spy	Spector Pro	eBlaster
Remotespy:	Stealth Recorder Pro	Stealth Website Logger
Flexispy	Wiretap Professional	PC PhoneHome
SpyArsenal Print Monitor Pro:		

Viruses and Worms

Virus: Definition and Characteristics

- A computer virus is a **program that can infect legitimate programs by modifying them to include a copy of itself.**
- Viruses spread without the knowledge or permission of users and contain malicious instructions that may cause damage or annoyance.
- A virus can start on event-driven effects (e.g., triggered after a specific number of executions), time-driven effects (e.g., triggered on a specific date), or can occur randomly.

Types of Viruses

1. Boot Sector Viruses: Infects the storage media on which the OS is stored and spreads when shared infected disks are used.

2. Program Viruses: Becomes active when the program files are executed and makes copies of itself.

3. Multipartite Viruses: A hybrid of boot sector and program viruses, infecting both program files and the record.

4. Stealth Viruses: disguises itself to avoid detection.

5. Polymorphic Viruses: Changes its virus signature every time it spreads.

6. Macro Viruses: Embedded in documents and infects every document produced.

7. Active X Java Control Viruses: Invites threats through web browser settings.

Worms: Definition and Characteristics

- A worm is a self-replicating malware program that uses a computer network to send copies of itself to other nodes.
- Unlike viruses, worms do not need to attach themselves to an existing program and can spread without any user intervention.
- Worms cause harm by consuming bandwidth and can lead to network congestion and disruption.

Types of Worms

1. Email Worms: Spread through infected email attachments.
2. Instant Messaging Worms: Spread through instant messaging applications.
3. Internet Worms: Spread through vulnerabilities in network services.
4. IRC Worms: Spread through Internet Relay Chat (IRC) channels.
5. File-Sharing Networks Worms: Spread through file-sharing networks.

Comparison of Virus and Worms

- Viruses require a host program to spread, whereas worms are self-spreading.
- Viruses modify existing programs, while worms replicate independently.
- Both can cause significant damage, but worms typically lead to network congestion and viruses lead to data corruption.

Impact and Prevention

- Impact on Systems and Networks: Both viruses and worms can lead to data loss, system failures, and security breaches.
- Prevention Strategies: Use antivirus software, keep systems updated, avoid opening suspicious emails, and regularly back up data.

Task -2 Prepare survey report on Virus Attacks, worm attacks their preventive measures

Virus attacks

1. Conficker
2. INF/AutoRun
3. Win32 PSW.OnLineGames
4. Win32/Agent (Trojan)
5. Win32/FlyStudio (Trojan with characteristic of backdoor)
6. Win32/Pacex.Gen
7. Win32/Qhost
8. WMA TrojanDownloader.GerCodec

Worm Attacks

1. Morris Worm
2. ILOVEYOU
3. Nimda
4. Code Red
5. Melissa
6. MSBlast
7. Sobig
8. Storm Worm

Trojan Horses and Backdoors

- Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm.
- Get into system from number of ways, including web browser, via E-mail, or with software download from the Internet.
- Trojan do not replicate themselves but they can be equally destructive

Examples of threats by Trojans

- Erase, overwrite or corrupt data on computer
- Help to spread other malware
- Deactivate or interface with antivirus and firewall
- Allow to remote access to your computer
- Upload and download files without user knowledge
- Gather E-Mail address and use them for spam
- Slow down, restart or shutdown the system
- Reinstall themselves after being disable
- Disable task manager or control panel
- Copy fake links to false websites, display porno sites, play sounds/videos and display images
- Log keystrokes to steal info such as password or credit card number

Backdoors

- It means of access to a computer program that bypasses security mechanisms
- Programmer uses it for troubleshooting
- Attackers often use backdoors that they detect or install themselves as part of an exploit
- Works in the background and hides from the user
- Most dangerous parasite, as it allows a malicious person to perform any possible action
- Programmer sometimes leave such backdoor in their software for diagnostic and troubleshooting purpose. Attacker discover these undocumented features and use them.

Examples of Backdoor Trojans

1. **Back office:** Enable user to control a computer running the Microsoft windows OS from remote location
2. **Bifrost**: Infect Windows 95 through Vista 3.
3. **SAP backdoors**: SAP is an Enterprise Resource Planning (ERP) system and nowadays ERP is the heart of the business technological platform.

How to protect from Trojan Horses and Backdoors

- Stay away from suspect websites/web links:
- Surf on the web cautiously-Avoid connecting with and/or downloading any information from peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats.
- Install antivirus/Trojan remover Software

Steganography

- Greek word that means “Sheltered writing”. It is a method that attempts to hide the existence of a message or communication. It comes from 2 Greek words: Steganos means “Covered” and graphein means “to write” or “concealed writing”
- **Steganalysis:** Detecting messages that are hidden in images, audio/video files using steganography.
- For example, in a digital image the least significant bit of each word can be used to comprise a message without causing any significant change in the image.

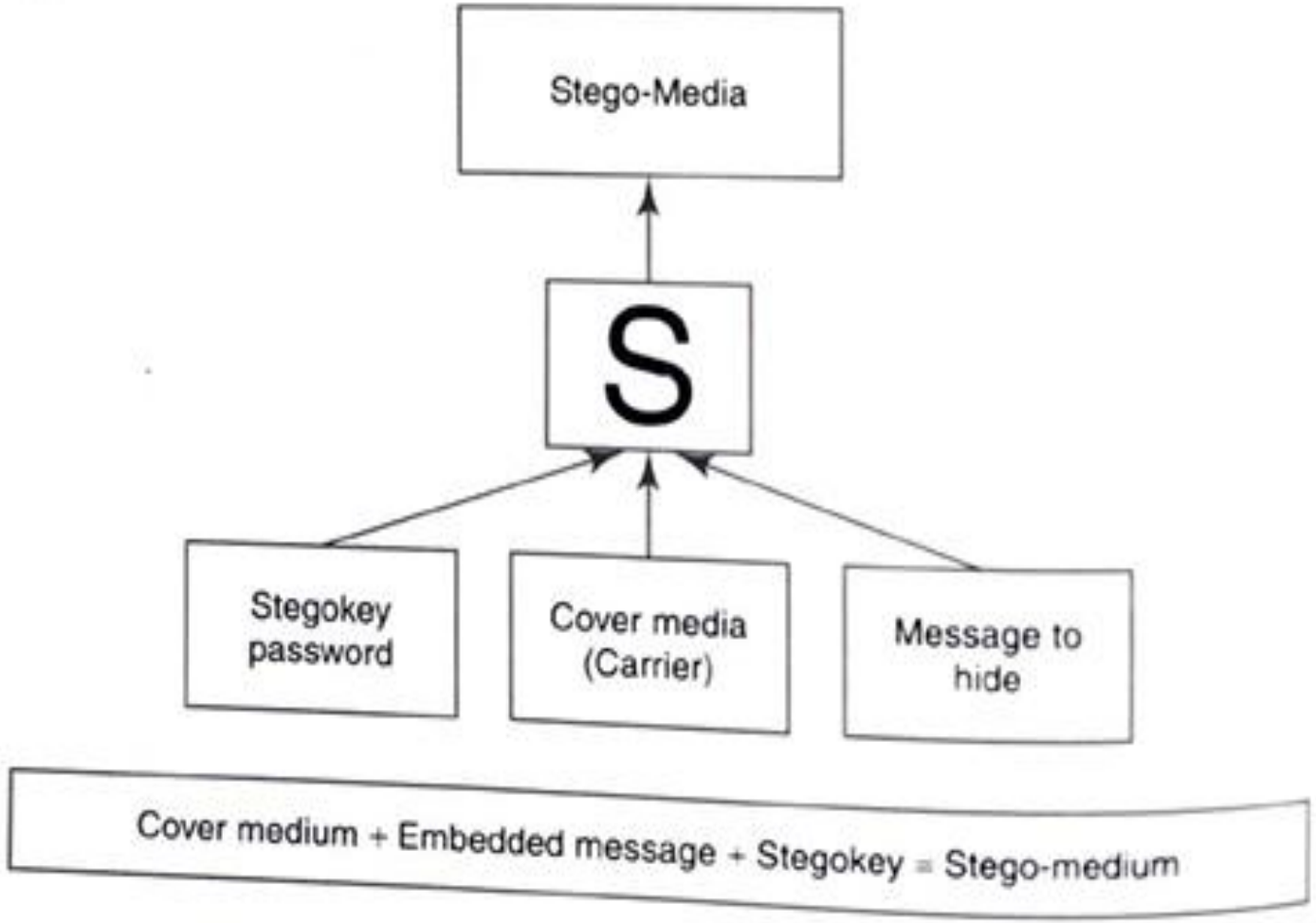


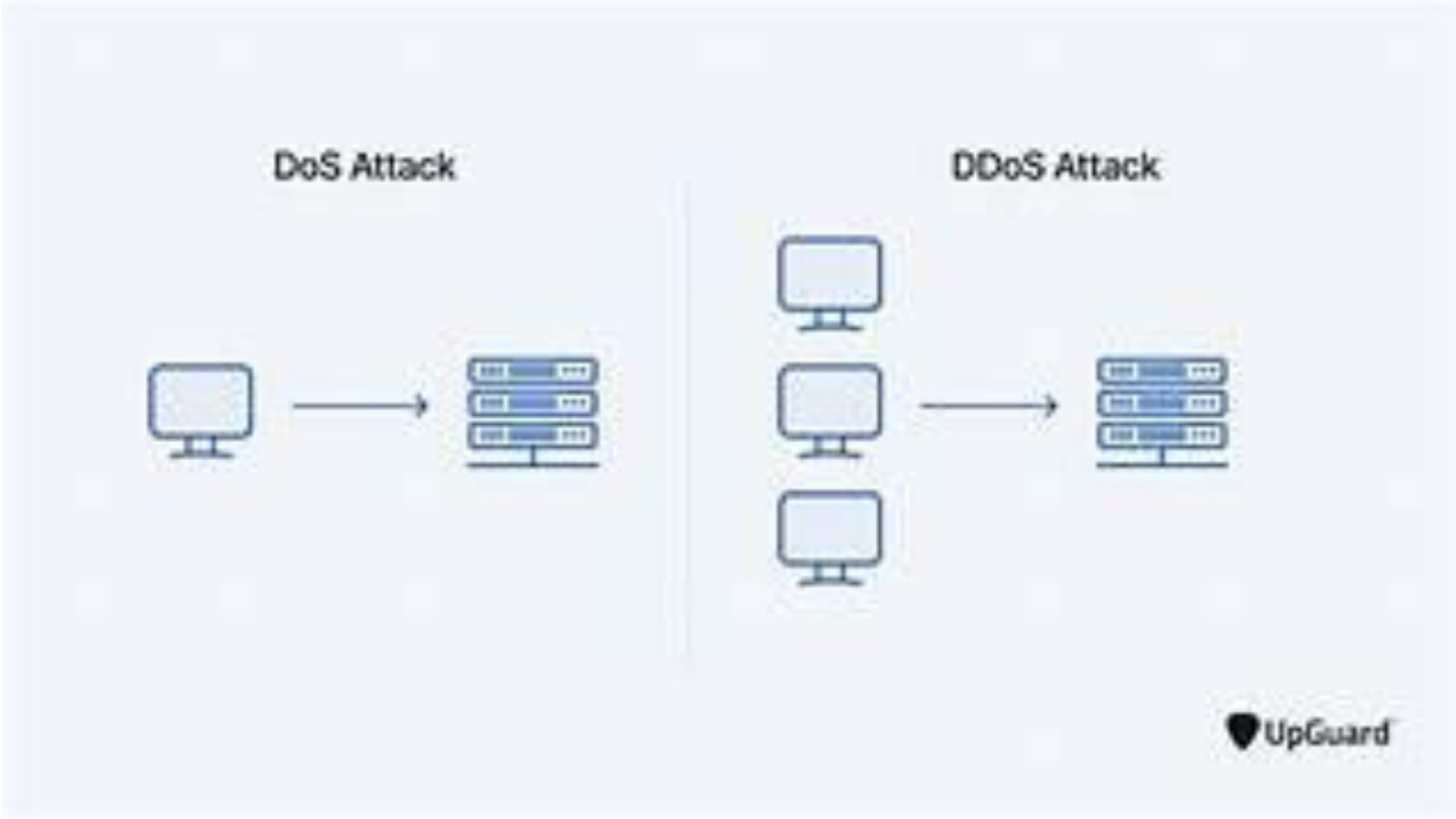
Fig. 3.4 How steganography works.

TASK-3

Explore the terminology

- i) Scareware, ii) Malvertising, iii). Clickjacking, iv)Ransomware
- Google Cookie, Cookie, DoubleClick and G-Zapper
- Strong, Weak, and Random Passwords

DOS and DDOS Attacks



DOS attack

- A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.
- The attacker floods the bandwidth of the victim's network or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide.
- The goal of DoS is not to gain unauthorized access to systems or data but to prevent intended users (i.e., legitimate users) of a service from using it.

1. Flood a network with traffic, thereby preventing legitimate network traffic.

2. Disrupt connections between two systems, thereby preventing access to a service.

3. Prevent a particular individual from accessing a service.

4. Disrupt service to a specific system or person.

DDOS attack

- A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems are called “secondary victims” and the main target is called “primary victim.”
- DDoS attacks involves hardcoding the target IP address prior to release of the malware, hence no further interaction is necessary to launch the attack.
- A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent.

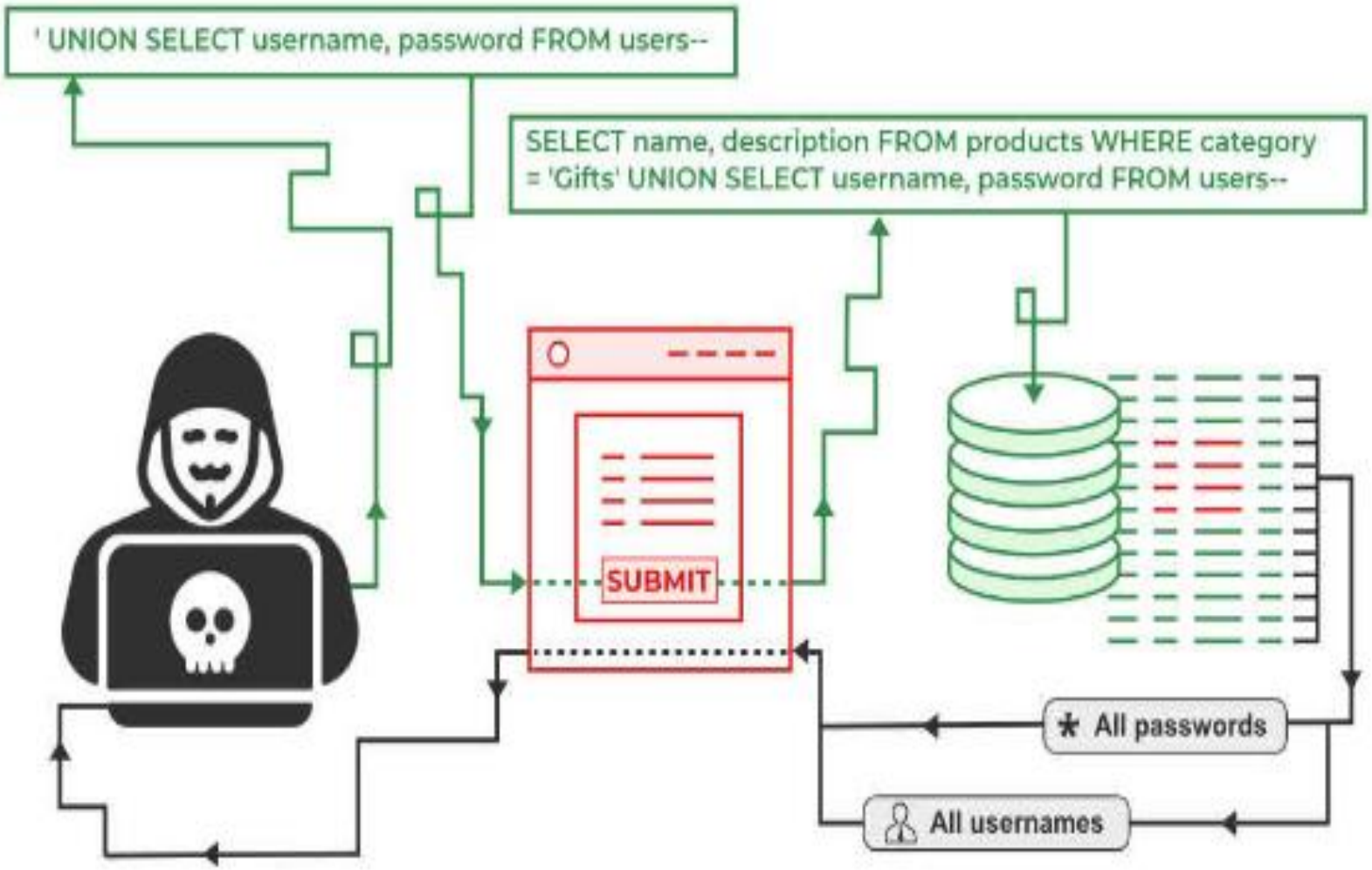
DoS and DDoS Attacks

How to Protect from DoS/DDoS Attacks

1. Implement router filters.
2. If such filters are available for your system, install patches to guard against TCP SYN flooding.
3. Disable any unused or inessential network service.
4. Enable quota systems on your OS if they are available.
5. Observe your system's performance and establish baselines for ordinary activity
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configuration information or other files.
8. Invest in and maintain "hot spares" – machines that can be placed into service quickly if a similar machine is disabled.
9. Invest in redundant and fault-tolerant network configurations.
10. Establish and maintain regular backup schedules and policies, particularly for important configuration information.
11. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft Windows NT Administrator.

SQL Injection

- **SQL Injection** is a security flaw in **web applications** where attackers insert harmful **SQL** code through user inputs.
- This can allow them to access sensitive data, change database contents or even take control of the system
- Attackers can SQL queries like **SELECT** to retrieve confidential information which otherwise wouldn't be visible.
- SQL injection also lets the attacker to perform a **denial-of-service (DoS) attacks** by overloading the server requests.


' UNION SELECT username, password FROM users--
SELECT name, description FROM products WHERE category = 'Gifts' UNION SELECT username, password FROM users--
SUBMIT
All passwords
All usernames

What is the impact of a successful SQL injection attack?

- A successful SQL injection attack can have severe consequences, including unauthorized access to sensitive data, such as personal information and financial records.
- Attackers may manipulate or delete critical data, compromising its integrity and causing operational disruptions.
- They can also bypass authentication mechanisms, gaining unauthorized access to user accounts, including administrative privileges.
- This can lead to the exposure of confidential information, identity theft, and significant financial losses.
- Additionally, SQL injection attacks can result in service downtime and damage to the organization's reputation.

Blind SQL Injection

- Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker.

How to Detect SQL injection Vulnerabilities?

- To detect SQL injection vulnerabilities, you can start by performing **input validation testing,** where special characters like ' or " are inserted into inputs to see if they cause errors.
- Automated tools like SQLMap or Burp Suite can scan for vulnerabilities by simulating attacks.
- Reviewing the source code helps identify insecure practices, such as using dynamic SQL queries without proper parameterization.
- Monitoring for unexpected database error messages can reveal potential issues.
- Finally, conducting thorough penetration testing, including both black-box and white-box methods, provides a comprehensive assessment of security weaknesses.

How to Prevent SQL Injection Attacks

SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection.

1. Input validation
2. Modify error reports
3. Other preventions

- The default system accounts for SQL server 2000 should never be used
- Isolate database server and web server. Both should reside on different machines.
- extended stored procedures (such as xp_cmdshell and xp_grantlogin) are not used or have unused triggers, stored procedures, user-defined functions, etc., then these should be moved to an isolated server.

Buffer Overflow

- Buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.
- As buffers are created to contain a finite amount of data, the extra information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.
- Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Types of Buffer Overflow

- **Stack-Based Buffer Overflow**
- **NOPs**
- **Heap Buffer Overflow**

- **Stack-Based Buffer Overflow**
- Stack buffer overflow occurs when a program writes to a memory address on the program's call stack outside the intended data structure – usually a fixed length buffer.
- The attacker may exploit stack-based buffer overflows to manipulate the program in various ways by overwriting.

- NOPs
- NOP or NOOP (no operation or no operation performed) is an assembly language which enables the developer to force memory alignment to act as a place holder to be replaced by active instructions later on in program development.
- NOP opcode can be used to form an NOP slide, which allows code to execute when the exact value of the instruction pointer is indeterminate.

- Heap Buffer Overflow
- Heap buffer overflow occurs in the heap data area when an application copies more data into a buffer than the buffer was designed to contain.

Buffer Overflow

- How to Minimize Buffer Overflow
- The following methods will definitely help to minimize such attacks:
  1. Assessment of secure code manually
  2. Disable stack execution
  3. Compiler tools
  4. Dynamic run-time checks
  5. Various tools are used to detect/defend buffer overflow

Protection Against Cyber Attacks

To protect against cyber attacks, it is essential to implement robust security measures:

1. Use strong, unique passwords and change them regularly.

2. Install and maintain antivirus and anti-malware software.

3. Employ firewalls and intrusion detection systems.

4. Regularly update software and apply security patches.

5. Educate users about safe online practices and social engineering threats.

6. Conduct regular security audits and vulnerability assessments.

7. Backup important data and have a disaster recovery plan in place.

The cyber kill chain

- The cyber kill chain is intended to defend against sophisticated cyberattacks, also known as advanced persistent threats (APTs), wherein adversaries spend significant time surveilling and planning an attack. Most commonly these attacks involve a combination of malware, ransomware, Trojans, spoofing and social engineering techniques to carry out their plan.


1
RECONNAISSANCE
2
WEAPONIZATION
3
DELIVERY
4
EXPLOITATION
5
INSTALLATION
6
COMMAND AND CONTROL
7
ACTIONS ON OBJECTIVE
CYBER KILL CHAIN
PROCESS

- **Phase 1: Reconnaissance**
  During the Reconnaissance phase, a malicious actor identifies a target and explores vulnerabilities and weaknesses that can be exploited within the network.
- **Phase 2: Weaponization**
  During the Weaponization phase, the attacker creates an attack vector, such as remote access malware, ransomware, virus or worm that can exploit a known vulnerability.

- **Phase 3: Delivery**
  In the Delivery step, the intruder launches the attack.
- **Phase 4: Exploitation**
  In the Exploitation phase, the malicious code is executed within the victim's system.
- **Phase 5: Installation**
  Immediately following the Exploitation phase, the malware or other attack vector will be installed on the victim's system.

- **Phase 6: Command and Control**
  In Command & Control, the attacker is able to use the malware to assume remote control of a device or identity within the target network.
- **Phase 7: Actions on Objective**
  In this stage, the attacker takes steps to carry out their intended goals, which may include data theft, destruction, encryption or exfiltration.

Example tools

- **Nmap:** NMap is a free and open source network mapping tool that is available for Windows, Linux, and macOS.
- **Metasploit:** This is a Linux-based hacking framework that has been used countless times by hackers.
- **Wireshark** This is a very popular tool among both hackers and pen testers. Wireshark is famous for scanning networks. The tool captures data packets in a target network and displays them in a verbose format, which is human readable.
- **Aircrack-ng** Aircrack-ng is a dangerous suite of tools that is used for wireless hacking, and has become legendary in today's cyberspace. The tools are available for both Linux and Windows operating systems.

- **John the Ripper** This a powerful password-cracking tool available on Linux and Windows operating systems that is used by hackers to perform dictionary attacks. The tool is used to retrieve the actual user passwords from encrypted databases of desktop or web-based systems and applications.
- **THC Hydra** It is similar to the previously discussed tool, the only difference being that Hydra works online while John the Ripper works offline. Hydra is, however, more powerful and thus more popular among hackers. It is available for Windows, Linux, and macOSX. The tool is commonly used for fast network login hacking. It uses both dictionary and brute-force attacks to attack login pages

- **Nikto** Nikto is a Linux-based website vulnerability scanner that hackers use to identify any exploitable loopholes in organizational websites.
- **Kismet** Kismet is also a wireless network sniffer and intrusion detection system.
- **Cain and Abel** Cain and Abel is a Windows-based password cracking tool that is effective against Microsoft operating systems.

Access and privilege escalation

- This phase comes after an attacker has already identified a target, and scanned and exploited its vulnerabilities using the previously discussed tools and scanning tools.
- The main focus of the attacker in this phase is to maintain access and move around in the network while remaining undetected.
- In order to achieve this freedom of movement without being detected, an attacker needs to perform privilege escalation.
- This is an attack that will grant the attacker an elevated level of access to a network, its connected systems, and devices.

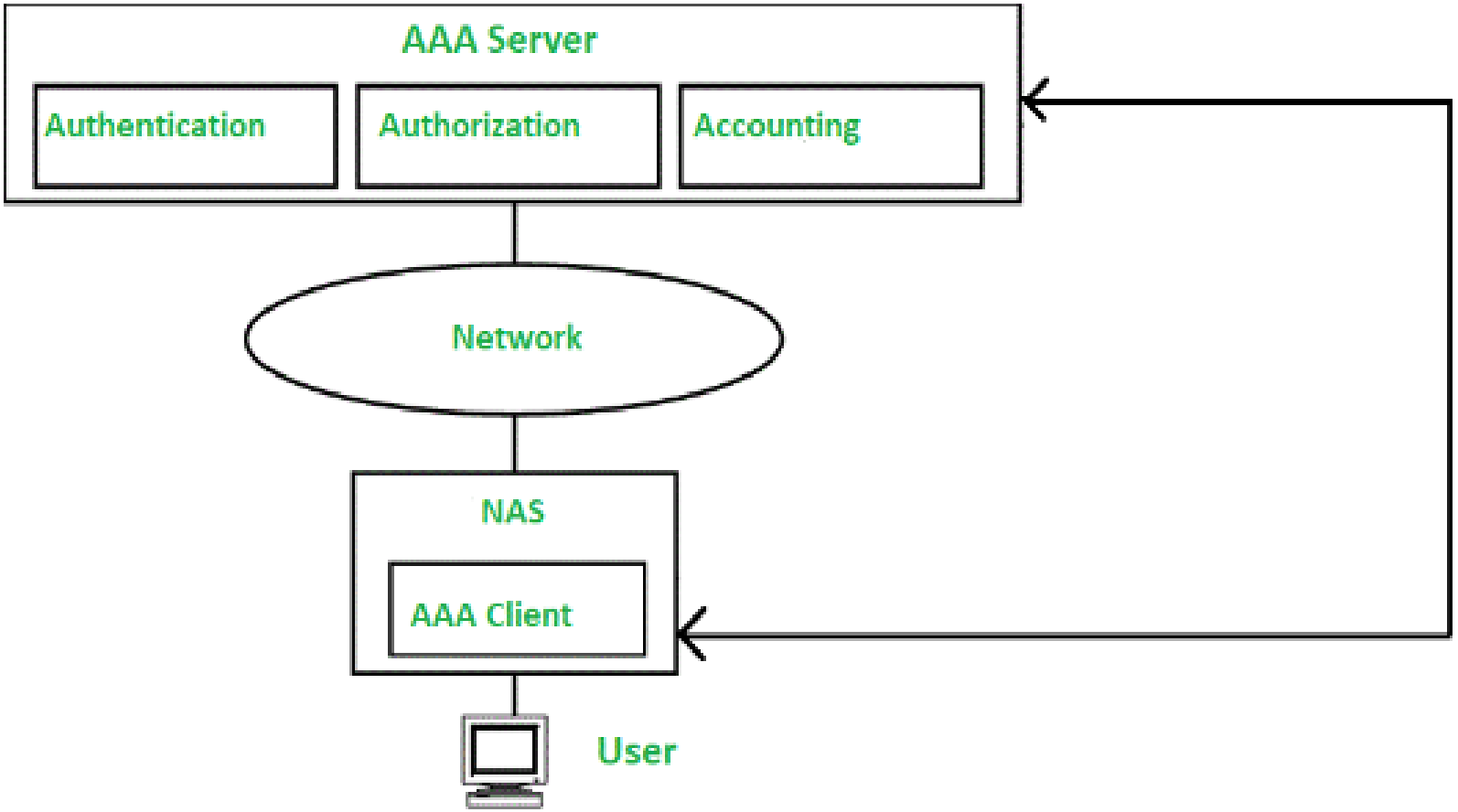
- Privilege escalation can be done in two ways: vertical, and horizontal:

Vertical privilege escalation	Horizontal privilege escalation
Attacker moves from one account to another that has a higher level of authority	Attacker uses the same account, but elevates its privileges
Tools used to escalate privileges	User account used to escalate privileges

Table 1: A comparison of horizontal and vertical privilege escalation

Authentication, Authorization, and Accounting (AAA)

- **Authentication, Authorization, and Accounting (AAA)** is an architectural framework to gain access to computer resources, enforcing policies, auditing usage, to provide essential information required for billing of services and other processes essential for network management and security.


AAA Server
Authentication
Authorization
Accounting
Network
NAS
AAA Client
User

Authentication, Authorization, and Accounting (AAA)

- Access control
- Identity management
- user authentication
- Technical aspects of accountability

1. Access Control

Access control is "the process of granting or denying specific requests ..." This process needs the following inputs

- Who issued the request?
- What is requested?
- Which rules are applicable when deciding on the request?

Security policies: Automated security policies are a collection of rules.

Automated security policies consist of rules that define the access rights over an object.

- Two fundamental security policies from the 1970s are Discretionary Access Control (DAC) and Mandatory Access Control (MAC).
- DAC allows resource owners to assign access rights to user identities at their discretion. It can refer to both resource owner policies and Identity-Based Access Control (IBAC) policies.
- MAC, on the other hand, involves labeling subjects and objects with security levels that form a lattice structure with defined bounds.

Access Control-types

- **Role-based Access Control:** In Role-Based Access Control (RBAC), roles are an intermediate layer between users and the permissions to execute certain operations. Users are assigned roles and are authorized to execute the operations linked to their active role. Separation of Duties (SoD) refers to policies that stop single users from becoming too powerful.
- **Attribute-Based Access Control** (ABAC) : "logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes".
- **Code-Based Access Control (CBAC**) : Code-Based Access Control (CBAC) assigns access rights to the executable. Policies may refer to code origin, to code identity (e.g., the hash of an executable), or to other properties of the executable, rather than to the identity of the user who had launched the executable.

Mobile Security

- Smartphones are single-user devices that handle private data, communication, and environmental observations through features like cameras, microphones, and GPS.
- In smartphone security, apps are the principals for access control, while the sensitive data and device functions are the objects of access control.
- Access control on smartphones aims to protect user privacy and maintain platform integrity.
- For instance, Android categorizes permissions into three types: **normal, dangerous, and signature.**
- **Normal permissions are low-risk** and do not require special approval, **dangerous permissions impact privacy and require user consent**, and **signature permissions affect platform integrity** and are restricted to apps **signed by the platform provider**.
- Since **Android 6.0, users have granted dangerous permissions** when they are first needed, addressing prior issues where permissions were granted too freely.

Digital Rights Management

- It is originated in the **entertainment industry** to control the **distribution and usage of digital content** like games, movies, and music.
- DRM policies regulate aspects such as access **frequency, free sampling periods, device limits, and content pricing**.
- Unlike traditional access control, which protects system owners from external threats, **DRM imposes external security policies on the system owner**.
- A notable DRM concept is **superdistribution,** where data is distributed in protected containers with usage terms attached.
- These containers can be freely shared, but require a **Superdistribution Label Reader** to enforce and track usage according to the attached terms.
- This concept contributed to the development of **Trusted Computing.**

Cont..

- **Tamper resistance in DRM** varies based on threat levels.
- **Trusted Platform Modules (TPMs)** offer **hardware-based** assurance, while **Intel SGX enclaves** provide **a software-based solution.**
- **Document readers** that prevent **copying and sticky policies** that persist with objects are other DRM approaches.
- **Attestation methods**, such as direct anonymous attestation and remote attestation, provide **trustworthy information** about a platform's configuration. For example, **content owners can verify software** configurations before releasing content.
- The **FIDO (Fast Identity Online) Universal Authentication Framework (FIDO UAF) attests to the model of authenticator devices.**
- At times, DRM was used as a broad term encompassing traditional access control as a subset.

Usage Control

- **Usage Control (UCON)** is a framework that extends traditional access control by **incorporating authorizations** based on attributes of subjects and objects, along with **obligations and conditions**.
- **Obligations are actions** that must be performed to gain access, such as agreeing to terms or logging an access request. **Conditions are external factors,** like time of day or machine location, that influence access permissions.
- **UCON** also addresses post-access provisions, such as restrictions on copying content or adjustments to access attributes (e.g., decrementing access counters).
- It distinguishes itself from traditional access control by managing entire workflows at the application level, rather than just basic access operations at the infrastructure level. In telecom services, **usage control can include limitations on traffic volume.**
- Many UCON concepts are integrated into the XACML 3.0 (eXtensible Access Control Markup Language) standard.

Enforcing Access Control

- To enforce a security policy, this policy first has to be set.
- For a given request, a decision has to be made about whether the request complies with the policy, which may need additional information from other sources.
- Finally, the decision must be conveyed to the component managing the requested resource.
- In the terminology of XACML (The eXtensible Access Control Markup Language), this involves
  - Policy **Administration** Points where policies are set,
  - Policy **Decision Points** where decisions are made,
  - Policy **Information Points** that can be queried for further inputs to the decision algorithm,
  - Policy **Enforcement Points** that execute the decision.

Delegation and Revocation

- **Delegation and granting of access rights** involve situations where one principal or subject receives access rights from another.
- "**Granting**" is often used generically to describe the process of assigning access rights to a subject.
- "**Delegation**" may refer more specifically to the temporary transfer of access rights during a process's execution.
- For instance, XACML differentiates between policy administration and dynamic delegation, where the latter allows users to create temporary policies to delegate specific capabilities.
- Access rights are not always permanent;
- they may have expiry dates, be limited to a session, or be subject to revocation.
- **Revocation mechanisms**, such as the Online Certificate Status Protocol (OCSP) for X.509 certificates, help manage this process, with OCSP supported by major browsers.
- Alternatively, **revocation lists** can be used when online checks are impractical.

2. Identity Management

- Identity management systems, as defined by NIST, handle the **creation, use, and termination of electronic identities**.
- These systems deal with the **operational aspects of managing identities, including their linkage to individuals.**
- In **sensitive areas, strong links and thorough verification are required,** such as for compliance with money laundering rules.
- In contrast, **some applications benefit from identities** that cannot be linked to individuals to preserve privacy.
- Identity management can **associate access** rights with electronic identities, either **directly or through intermediaries like roles.**
- When **identities are no longer needed, they should be terminated across all systems where they were registered**. This avoids issues like unintended access by new users or identity collisions during organizational mergers.

Cont..

- **Electronic identities vary in form and layer**. For internal system purposes, user identities need to be locally unique.
- Systems **like Linux may create these identities manually**, risking issues if identities are reused.
- Using **long random strings, as in Windows**, reduces this risk but requires **reassignment of access rights if accounts are recreated**.
- **User names and email addresses,** often used as electronic identities, can be random but are typically more practical if meaningful.
- However, reassigning these identities, such as email addresses, can lead to misdirected communications.
- **Web applications frequently use email addresses for identities** due to convenience. Alternatives like FIDO UAF use randomly generated public keys, eliminating the need for passwords and password reset channels. From a personal perspective, managing how identities are revealed across different organizations is also a key aspect of identity management.

3.User Authentication

- Access requests are made by subjects, which can be associated with security attributes upon creation or during their lifetime.
- **Authentication is the process that validates** these security attributes when a subject is created.
- When subjects are created through user actions, user authentication must ensure that the user identity linked to the subject is accurate.
- The strength of authentication should match the level of risk, hence the term "**risk-based authentication.“**
- **User authentication also supports accountability.** The "authentication ceremony" refers to the steps a user undergoes to be authenticated.
- In **some access control systems**, the **security attributes of a subject remain constant throughout its lifetime**, meaning policy changes do not affect active processes. However, these subjects have limited lifetimes, mitigating inconsistencies.
- Alternatively, s**ome systems recheck the attributes each time a subject makes a request**, such as re-authenticating a user in a banking application during a funds transfer.
- Thus, **authentication can also be viewed as the process of validating the security attributes** presented with each access request.

- **Passwords**
- **Biometrics for Authentication**
- **Authentication Tokens**
- **Behavioural Authentication**

Passwords

- When passwords are used for user authentication, various protective measures are implemented.
- On the system side, these include storing hashed or encrypted passwords, adding salt to passwords, and using shadow password files to secure sensitive data.
- On the user side, guidelines for proper password selection and handling are essential, as are security awareness programs.
- NIST's Digital Identity Guidelines offer updated recommendations based on the effectiveness of previous password rules, considering the modern reality of users managing multiple accounts.
- Key recommendations include:
  - **Avoiding automatic password expiration**; passwords should change only for a reason.
  - **Prioritizing password length over complexity**.
  - **Discouraging password hints or knowledge-based authentication** due to the availability of personal information on social networks.
  - **Enabling "show password while typing"** and allowing paste-in password fields.
- Password-based protocols for remote authentication include **RADIUS**, **DIAMETER**, **HTTP Digest Authentication**, and **Kerberos**. Further password guidance can be found in the Human Factors Knowledge Area

Biometrics for Authentication

- Biometrics offer an **alternative to password-based authentication**, reducing the cognitive load on users. The primary biometric methods used are fingerprint and face recognition. While biometric features must be unique to each user, they are not secrets, as fingerprints can be easily left on surfaces and faces are always visible. Therefore, capturing biometric data requires robust liveness detection to prevent spoofing.
- Key Assumptions for Biometric Authentication:
  - - Biometric features uniquely identify an individual.
  - - Features are stable over time (e.g., minimal effects of aging on fingerprints).
  - - Features can be conveniently captured in operational settings.
  - - Features cannot be spoofed during authentication.
- Authentication Process:

  - A template (e.g., fingerprint image) is captured and a feature vector (e.g., minutiae positions) is extracted.

  - Users register a reference feature vector initially.

  - During authentication, a new template is captured, and its features are compared with the reference.

  - Authentication succeeds if the number of matching features exceeds a threshold.

Cont..

- **Potential Failures:**

  - Failure to capture sufficient features during registration or authentication.

  - False rejects: genuine users are wrongly rejected.

  - False accepts: incorrect users are wrongly accepted.

  - Spoofing: presenting fake biometric data to deceive the system. Liveness detection mitigates this risk.

- **Applications and Adoption:**

  - Automated border control gates increasingly use fingerprint and face recognition.

  - Biometric authentication is a common feature on mobile devices.

  - The current state-of-the-art in biometric authentication is extensively surveyed.

- In summary, biometrics provide a secure and user-friendly alternative to passwords, although challenges such as feature stability, spoofing prevention, and effective liveness detection need to be addressed.

Authentication Tokens

- Authentication tokens rely on "something you have," in contrast to passwords ("something you know") and biometrics ("who you are"). Users are provided with a device (token or security key) that generates a one-time password (OTP) or responds to a challenge from the authenticator.
- Types of Tokens:

  - **Simple Tokens:** Small devices with an LED display showing an OTP, which the user enters in a log-in form (e.g., RSA SecureID, YubiKey).

  - **Challenge-Response Tokens**: Devices with a numeric keypad and a 'sign' button. Users receive a challenge, enter it on the device, press 'sign' to generate a response, and enter the response in a log-in form. Used in some e-banking services.

  -**PhotoTAN Devices**: Receive challenges as QR codes on the user's computer, scanned by the device to generate a response.

  - FIDO Authenticator: Creates public/private key pairs, with public keys as identifiers and private keys for digital signatures. It supports a challenge-response pattern for user authentication across different servers using different keys.

Contt

- **Authentication Process**:

- **Single-Stage**: Possession of the token is enough for authentication.

- **Two-Stage**: The token first authenticates the user (e.g., via PIN or fingerprint), and then the server authenticates the token.

Considerations:

- **Smartphone Apps:** These can function as tokens but are not dedicated security devices, making them more vulnerable to attacks. Smartphones may use secondary authentication mechanisms, balancing ease of use and security needs.

- In summary, authentication tokens provide a secure method based on possession, with various implementations offering different levels of security and convenience. However, using smartphones as tokens introduces potential security risks.

Behavioural Authentication

- Behavioral authentication is based on analyzing "**what you do**," making it suitable for continuous authentication. It leverages various biometric data such as keystroke dynamics, handwriting characteristics, and voice recognition. Smartphone sensors like touch screens and microphones capture these behavioral features.
- Key Requirements:
  - Behavioral features must uniquely identify a person.
  - Features should be stable and unaffected by temporary impairments.
  - Features must be conveniently captured in operational settings.
  - Features should be resistant to spoofing during authentication.

Advantages:

- Minimizes user inconvenience with continuous, non-intrusive authentication.
- - Promises high security with minimal friction.

Contt

Challenges:

- Variations in user behavior can lead to **false rejects** (e.g., voice recognition affected by a cold).
- Effective fallback mechanisms are required when behavioral authentication fails.
- Security relies on robust liveness detection to prevent spoofing by synthesizers or imitators.
- Uncertain security guarantees without a clear threat model.

- Behavioral authentication offers a promising blend of convenience and security but requires careful implementation and threat modeling to ensure reliable protection.

4. Technical aspects of accountability

Accountability

Accountability in security refers to the ability to trace actions back to the entity that performed them. This is essential for several reasons, including:

- Non-repudiation: Ensures entities cannot deny their actions.
- Deterrence: Discourages malicious behavior by establishing traceability.
- Fault Isolation: Helps identify and isolate the sources of problems.
- Intrusion Detection and Prevention: Assists in recognizing and stopping unauthorized access.
- After-Action Recovery: Facilitates the process of recovery and response after a security incident.
- Legal Action: Provides evidence to support legal proceedings.

Cont..

- Accountability plays a crucial role in processes initiated after an event has occurred.

These processes include:

- Regular Audits: Ensuring compliance with regulations.
- Technical Audits: Scanning logs for signs of cyber attacks.
- Incident Investigations: Identifying exploited vulnerabilities and responsible parties.
- The effectiveness of these processes relies on the quality of the evidence, which is often derived from event logs maintained by operating systems, networking devices, or applications. The specific events logged depend on the monitored activity.

Technical Aspects

- **Audit Policies**
- **Preserving the Evidence**
- **Analyzing the Evidence**
- **Privacy and Accountability**
- **Distributed Logs**

Audit Policies

- Accountability relies heavily on the quality of evidence collected during operations. System administrators establish audit policies to define which events are logged.
- Examples of such events include:
  - Successful and failed authentication attempts.
  - Decisions on sensitive access requests.
- Operating systems and audit tools offer menus to help administrators set these policies. Access control policies that mandate logging certain requests also influence the evidence collected.

Preserving the Evidence

The strength of accountability depends on the protection of collected evidence.

Attackers may attempt to:

1. Delete incriminating log entries after gaining sufficient privileges.
2. Modify audit policies to prevent future actions from being recorded.

Preventive measures

- Tamper Resistance:

  - Physical Measures: Using endless paper reels or WORM (Write-Once, Read-Many) memory like optical disks.

  - Cryptographic Measures: Storing logs as a hash chain to detect entry removal, although this doesn't prevent entry loss.

- Audit Policy Considerations:

  - Address disruptions in logging, such as a full log file.

  - Decide whether to overwrite old entries or stop the system until proper auditing is restored.

  - Resolve the conflict between system availability and accountability.

Audit logs can generate large volumes of data, with many entries not relevant to security, necessitating automated processing. Key techniques include:

- Signature Detection: Identifying known attack patterns.
- Machine Learning: Detecting anomalies through advanced algorithms.
- Visualization: Highlighting the most relevant events to administrators.

These methods help manage and interpret extensive data efficiently, enhancing network intrusion detection and overall security analysis.

Analyzing the Evidence

Accountability depends on several factors when supporting legal or disciplinary actions:

- User Authentication: The strength of the authentication mechanism and user resilience to phishing and social engineering attacks. While avoiding obvious phishing attacks is straightforward, well-crafted spear phishing can be challenging to detect.
- Organizational Security Policies: Policies regarding the connection of devices (e.g., USB tokens) to internal systems and access to external websites.
- Defense Against Software Vulnerabilities: Protection against exploits that allow code to run under a user's identity without their knowledge, such as drive-by downloads.

Privacy and Accountability

- Privacy rules can affect the logging of events, as employment laws may restrict the extent of employee monitoring, complicating accountability when rules are broken.
- Technical solutions can sometimes resolve conflicts between privacy and legal goals. For instance, a **company not allowed to log external website visits can still hold employees accountable for attacks by logging internal IP addresses and port numbers without recording visited sites.** If an attack is reported, the affected site can trace the attack back using the port number.
- Logging can also have unintended privacy impacts, such as with Certificate Transparency (RFC 6962). This service logs the issuance of **TLS certificates to help domain owners detect unauthorized certificates,** thus making certificate issuers accountable.
- However, logging requests for certificates for private subdomains can inadvertently disclose their existence, affecting privacy.

Distributed Logs

- Logs can be used to ensure accountability of system users and owners. For owner accountability, auditors may require sealed logging devices or a distributed system of independent nodes with barriers against collusion.
- Nodes maintaining the log must synchronize their versions, and the overhead for this synchronization depends on the failure models of the nodes and communication network, as well as the rules for joining the distributed system.