NURTURE
Education Solutions
TOMORROW'S HERE

Subject: Cyber Security Fundamentals

Module Number: 01

Module Name: Cyber Security Fundamentals

Syllabus

Cybersecurity Fundamentals

Evolution of Cybersecurity, Principles of Cybersecurity, CIA – Confidentiality, Integrity, Availability, Vulnerabilities, People-process-technology based vulnerabilities, Zero-day vulnerability, Threats – Actors, Tools, Types of cyber-attacks, Countermeasures – Cryptography, hashing, authentication, authorization, accountability

Aim:

The aim of this module is to equip students to understand the basics and importance of cyber security.

Objectives:

The objectives of this module are as follows:

- Identify the need of Cyber Security.
- Discuss the principles of cyber security.
- Classify the CIA triad and countermeasures.
- Summarize the different types of threat countermeasures.

Outcomes:

At the end of this module, you are expected to:

- Recall significant evolution of cybersecurity.
- Describe the principles of cybersecurity.
- Distinguish Confidentiality, Integrity and Availability concepts.
- List the different types of vulnerabilities of cyber systems.

Table of Contents

What is Cybersecurity?

The process of protecting computers, servers, mobile devices, electronic systems, networks and data from hostile intrusions is known as cyber security.

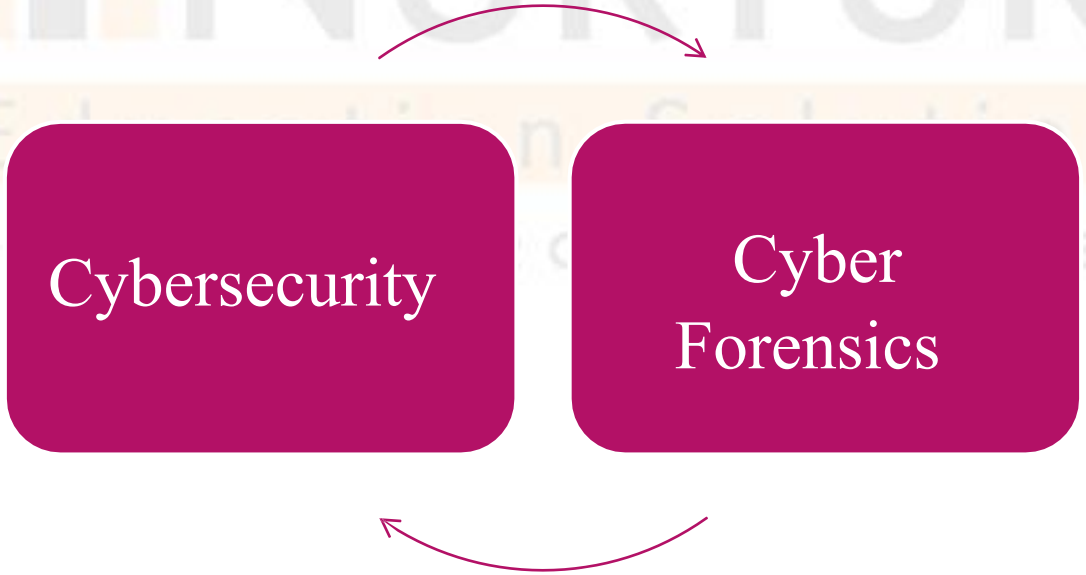
Cyber security vs. Information security

Information security and cyber security are sometimes conflated.

- Cyber security is concerned with preventing unauthorized access to computer systems, as well as damage or inaccessibility.
- Information security is a broad term that refers to the safeguarding of all information assets, whether physical or digital.

Relationship between Cyber Security and Computer Forensics

- Cyber security aims to guard electronic assets from breaches, whereas Computer Forensics explains how a policy became violated and who was liable for it.



Evolution of Cybersecurity – First Uses

- Cybernetics: The term that was coined in the late 1940s. Cybernetics is the study of human and machine communication and control systems. The origin of the word comes from the Greek phrase ‘Kubernetes’, which means ‘steersman’ and ‘cyber’ come from ‘kubernan’, which means ‘to steer’ [Oxford Dictionary].
- Cyberspace: William Gibson, a science fiction author, created the word ‘cyberspace’ in his novel Neuromancer in 1984 [Carr, 2009].
- Late, cyber got a lot of attention and has been used as a prefix like cyberfriend, cybersnob, cyborg, cybersecurity, cyber‑crime, cyberwarfare and so on [New York Magazine, 1993].

Current Importance of Cyber

- From a business standpoint
- Business continuity, critical infrastructures
- E-commerce
- Trade secrets, blueprints and digital assets
- Information about the employees
- Individual point of view
- In the cyber sphere, we have a digital persona that can purchase, read, chat and work.
- Accounts in a bank
- Privacy

Importance of Cybersecurity

- In 2015, United States firms ranked cyber as their 5th most important risk (AON Inpoint, 2017)
- The world Economic Forum (WEF) (2016) defined cyber attacks were in the top 5 cyber attacks in 2014 in terms of likelihood, as well as Critical information infrastructure breakdown in terms of impact.
- Global cybersecurity investment is estimated to reach $120 billion in 2017, up from $3.5 billion in 2004 (Morgan, 2017).
- By 2019, the global cost of cybercrime is anticipated to be $2.1 trillion (Morgan, 2016)
- As the cost of cybercrime rises, businesses increase their investments in cybersecurity to safeguard their trade secrets, business continuity and supply chain network.

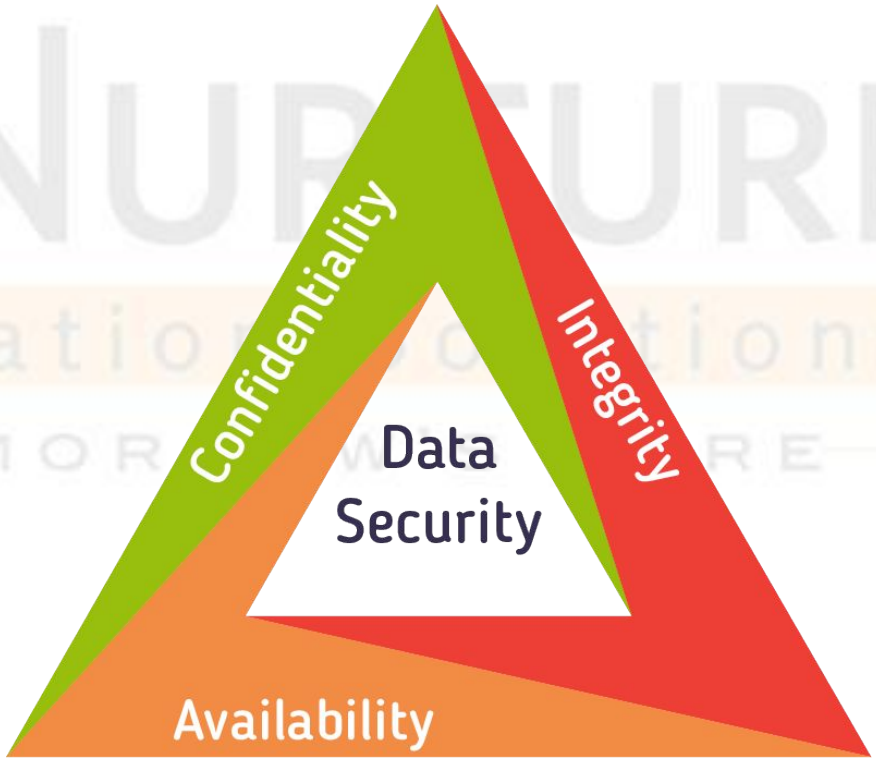
Data Breaches and its Cost

- Target, 2013, 70 million customers credit card information were stolen.
- Chase, 2014, 83 million customers information.
- Home Depot, 2014, 56 million customers credit cards were stolen.
- Office of Personnel Management, 2015, 25 million people affected, security clearance info were stolen.
- Ashley Madison, 40 million users' confidential information were stolen.

Basic Principles of Cybersecurity

There are three broad characteristics of information (cyber) security:

- CIA
- Confidentiality
- Integrity and
- Availability



Basic Principles of Cybersecurity : Confidentiality

- In simple terms, confidentiality refers to information that should not be shared with unintended people or entities.
- Confidentiality ensures that sensitive information is only accessed by authorised individuals and kept out of the hands of those who are not authorised to hold it.

Examples:

- Bank Account Statement
- Personal Information
- Credit Card Numbers
- Trade Secrets, etc.

Basic Principles of Cybersecurity : Integrity

- Integrity in the context of information security (InfoSec) indicates that when a sender provides data, the receiver must get the exact same data that the sender sent.
- In transit, data must not be altered.

Example:

- If someone sends the message ‘Hello!’ for example, the receiver must also get ‘Hello!’ That is, it must be the exact identical data that the sender sent. Any data addition or deletion during transport would compromise the integrity of the data.

Basic Principles of Cybersecurity : Availability

- The term ‘availability’ refers to the fact that information is available to authorised persons whenever they need it. Data and system unavailability can have catastrophic effects.
- It is important to have disaster recovery strategies and procedures in place to prevent or limit data loss. Unpredictable events, such as natural hazards and fire, must be included in a disaster recovery plan.
- In order to prevent or reduce total data loss from such incidents, it is recommended that you run a backup process on a regular basis.

Self Assessment Question

1. _____ is the practice and precautions taken to protect valuable information from unauthorized access, recording, disclosure or destruction.

a. Network Security

b. Database Security

c. Information Security

d. Physical Security

Answer: c

Self Assessment Question

2. In cybersecurity, what does CIA stand for?

a. Confidentiality, Integrity, Availability

b. Central Intelligence Agency

c. Cybersecurity Investigation Agency

d. Cybersecurity, Internet, Accessibility

Answer: a

Self Assessment Question

3. What does confidentiality of data refer to?

a. Rules which allow access only to all parties

b. Rules which hide data

c. Rules which restrict access only to those who need to know

d. Rules which prevent data from being changed

Answer: c

Major Concepts of Cyber Security

- Vulnerability
- Actors
- Threats

Major Concepts of Cyber Security: Cyber Vulnerability

- Openness to attack or destruction
- Openness (of a system) to attack or harm impacting the confidentiality, integrity and availability of information in the context of cybersecurity.

Bases of Vulnerability

- People
- Process
- Technology

Cyber Vulnerability: Technology-Based Vulnerability

- A vulnerability is a defect in software that allows malware to be installed and run without the user being aware of it.
- As a result, vendors produce and distribute software ‘patches’ to address known flaws.
- Vulnerabilities open the door to exploitation. By carrying out a threat, a threat agent exploits a vulnerability.
- Poor or no authentication, as well as weak, default or hardcoded passwords, are key factors of these easily hacked systems.
- Example: insecam.org is a website that promotes the use of insecure security cameras.

Cyber Vulnerability: Technology Based Vulnerability – Zer0 Day

- Zer0-day vulnerability: it refers to a flaw in a program that is unknown to producer.
- Zer0-day attack: vulnerabilities of a software resolved by releasing updates or patches by the producer firm. A firewall or antivirus program can only stop attacks what it is designed for. A zer0-day attack is that exploits a vulnerability that is not discovered yet by a firewall or antivirus program. Therefore, software update or patches are very important to keep the cyber security.
- Companies generally are vulnerable to zer0-day attacks.
- A signature-based firewall can only stop this kind of attack after the signature of the attack is determined and put into the firewall.

Cyber Vulnerability: People Based Vulnerability

- Is the human being the centre of the universe? Is humankind the weakest link in the chain?
- "Any action that motivates a person to take an action that may or may not be in their best interest,"
- Social engineering methods may inflict more damage than other advanced assault kinds since they are based on human emotions.
- In terms of cybercrime, there are various sorts of social engineering.
- Baiting, smishing, vishing, phishing and spear phishing

Cyber Vulnerability: People Based Vulnerability – Social Engineering

- Apart from cybersecurity, social engineering is an older tactic. Targets may fall into the trap based on emotions such as fear, ambition and worry.

Baiting:

- You do not have to be online to be a victim of social engineering.
- They can even happen when you are not online.
- Giving a USB stick infected with a worm, trojan or other malware as a gift or dropping it on purpose is another technique to influence the victim.
- When a user plugs it into her computer and opens the files, malware is installed on the machine.

Cyber Vulnerability: People-based Vulnerability – Social Engineering (Contd….)

- Smishing is a kind of phishing that uses text messages instead of emails.
- The purpose is the same: recover the victim's personal information, such as passwords and user names.
- Smishing is more dangerous than phishing because people use their phones more than computers.
- Hackers trick targets by sending text messages that contain a link. It is easy for people to be misled by fraudulent SMS messages that appear to be authentic or from a reliable source.
- **Vishing** is the practice of misleading someone over the phone.

Cyber Vulnerability: People-based Vulnerability – Social Engineering (Contd….)

Phishing:

- It involves sending emails that appear to come from a valid and trustworthy source in an attempt to induce recipients to click on a link or download a file.
- They are usually sent in large quantities. They include generic information rather than target-specific information.
- Phishing emails may appear to be from your bank, school, workplace, hospital or government.

Cyber Vulnerability: People-based Vulnerability – Social Engineering (Contd….)

Spear Phishing:

- Targets are more vulnerable to specialised phishing emails if they enter some of their personal information on phishing emails.
- Individuals or small groups of people are targeted in spear-phishing attacks.
- Spear phishing emails contain more precise information on victims, making them more susceptible to being misled.

Cyber Vulnerability: Process-based Vulnerability

- 'Security is a process, not a product', stated prominent cybersecurity expert Bruce Schneier (2000).
- Hiring a security expert or purchasing cutting-edge security does not fix all of the issues. Perhaps the most ignored stage in managing company security is the security process or design.
- The security process refers to the strategy used by a company to maintain its networks secure. Designing a security architecture/framework is free, but it comes at a significant cost to enterprises.

Cyber Vulnerability: Process-based Vulnerability – Security Processes

- Principle of least privilege: limit the privilege. An associate has access only to do his/her task.
- Continuously monitoring the end-points: watching firewalls, intrusion detection systems, routers, servers, keeping data logs.
- Risk analysis: according to the risk score, secure the weakest chain in the link. Use the budget more wisely based on the risk score and vulnerabilities.
- Defense in depth: using multiple security tools, products and techniques.
- Content filtering: for spam or phishing emails
- Employee training: increases the awareness of employees against social engineering.

Major Concepts of Cyber Security: Cyber Actors

- Functional users
- Security Experts
- Insiders
- Hackers
- Penetration testers
- Organised crime
- Competitors
- Hacktivists and cyber-terrorists
- Law enforcement
- Nation states

Major Concepts of Cyber Security: Cyber Actors (Contd….)

‘If you know your enemy and yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battler’.

Sun Tzu, The Art of the War

Cyber Actors: Functional Users, Security Experts

Functional Users:

- Individuals or organisations for whom the cyber system was designed to work
- For instance, a bank depositor for ATM machines or a student for the university's email service.

Security Experts:

- Individuals or organisations which generate strategies, defense tools, products and techniques against hackers and malware.
- Ex: CERT, McAfee, Bruce Scheiner

Cyber Actors: Hackers

- Black hat hackers: malicious hacker
- Grey hat hackers: break into a system without permission and demand money to fix it, if rejected, they might not damage the system.
- Crackers: break into systems with malicious intent. Gain unauthorised access, damage integrity of vital data or make systems unavailable.
- Script kiddies: use scripts created by sophisticated hackers to attack computer and network systems, and deface websites. Script kiddies have low technical skills and they are more dangerous because of their high numbers and available tools and scripts.
- White hat hackers: pen-testers to test the vulnerabilities of the organisation with their permission – also falls under own Actor category

Cyber Actors: Insiders

- IT personnel of a company may cause a great disturbance to organisations.
- S/he may sell confidential information or break into systems herself to destroy the organisation. Since she would have the accessibility, it would be very easy to shut down the system.
- A current or a former employee can cause loss of money, reputation, hardware or software as an act of revenge.
- Therefore, to mitigate the risks, security processes should be established such as:
  a. Need to know principle
  b. Canceling former employees access
  c. Limiting current employees' access
  d. Changing password periodically

Cyber Actors: Hacktivist and Cyber Terrorist

Hacktivists

- An individual or a group that carries out cyberattack to draw attention to humanitarian or global problems such as global climate, freedom of speech, etc.
- Cyber Terrorist
- A group of hackers organise cyberattack to cause alarm, fear or panic with a political ideology.
- Cyber-terrorist attacks aim more severe and permanent damage than hacktivism.

Cyber Actors: Competitors and Law Enforcement

Competitors:

- Competitors can be the sponsor of a cyberattack. Competitors could get competitive advantage of hacking other firms or slow down their service.
- Law Enforcement:
- Organisations that monitor cybercrimes.
- Ex: INTERPOL, NSA.

Cyber Actors: Nation States

- The attack is carried out by state-sponsored hackers.
- Important actors: USA, Russia, China, Israel

Examples:

- Russians carried out a cyberattack to Georgia due to conflict between Russia and Georgia government (DDoS attack to Georgian president's website, 2008).

Cyber Actors: Penetration tester, Organised Crime

Penetration Tester:

- Penetration testers check security vulnerabilities of web-based applications, networks and systems with the permission of that organisation.
- It could be a proactive way to find out vulnerabilities before they are exploited by a hacker.
- Organised Crime
- A group of criminals that target victims to demand money, extort information. These groups may carry out for someone else who pays them to get confidential information, trade secrets or blueprints.
- Ex: Ransomware attacks

Self Assessment Question

1. _____ is a weakness that can be exploited by attackers

a. System with Virus

b. System without firewall

c. System with vulnerabilities

d. System with a strong password

Answer: c

Self Assessment Question

2. Which of this is an example of physical hacking?

a. Remote Unauthorised access

b. Inserting malware loaded USB to a system

c. SQL Injection on SQL vulnerable site

d. DDoS (Distributed Denial of Service) attack

Answer: b

Self Assessment Question

3. Stuxnet is a _____

a. Worm

b. Virus

c. Trojan

d. Antivirus

Answer: a

Major Concepts of Cyber Security: Cyber Threat

- Event with the potential to adversely affect operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations
- In the context of cybersecurity, a situation that has the potential to impact information confidentiality, integrity, or availability.

In the context of the military:

- A threat is defined as the product of capability and intent.
- For example, an aircraft's intent is predicted by the flight pattern or status of its active sensors (trackers), and its cargo is its capabilities.

Cyber Threat Taxonomy

- Physical attack: fraud, sabotage, theft, vandalism, information leak, terrorist attack
- Unintentional damage: due to human error; maintenance, third party, using unreliable sources, loss of information on cloud or on disks, lack of a proper planning
- Natural disasters: earthquake, flood, fire, radiation leak, explosion
- Failures / malfunction: failure of hardware or software
- Outage: absence of employee, internet outage
- Cyber‑crime/ abuse: denial of service, identity theft, malware injection, social engineering, manipulating hardware or software, unauthorized activities, manipulating DNS, remote control
- Legal threats: violation of rules and regulations, failure to meet contractual requirements, abuse of personal data

Cyber Threat: Examples

- Malware : Virus, Trojan Horse, Spyware and Rootkits need a host program to keep their tracks
- Worms, Automated Virus and Zombie live and spread out independently
- Adware
- DoS and DDoS
- Ransomware

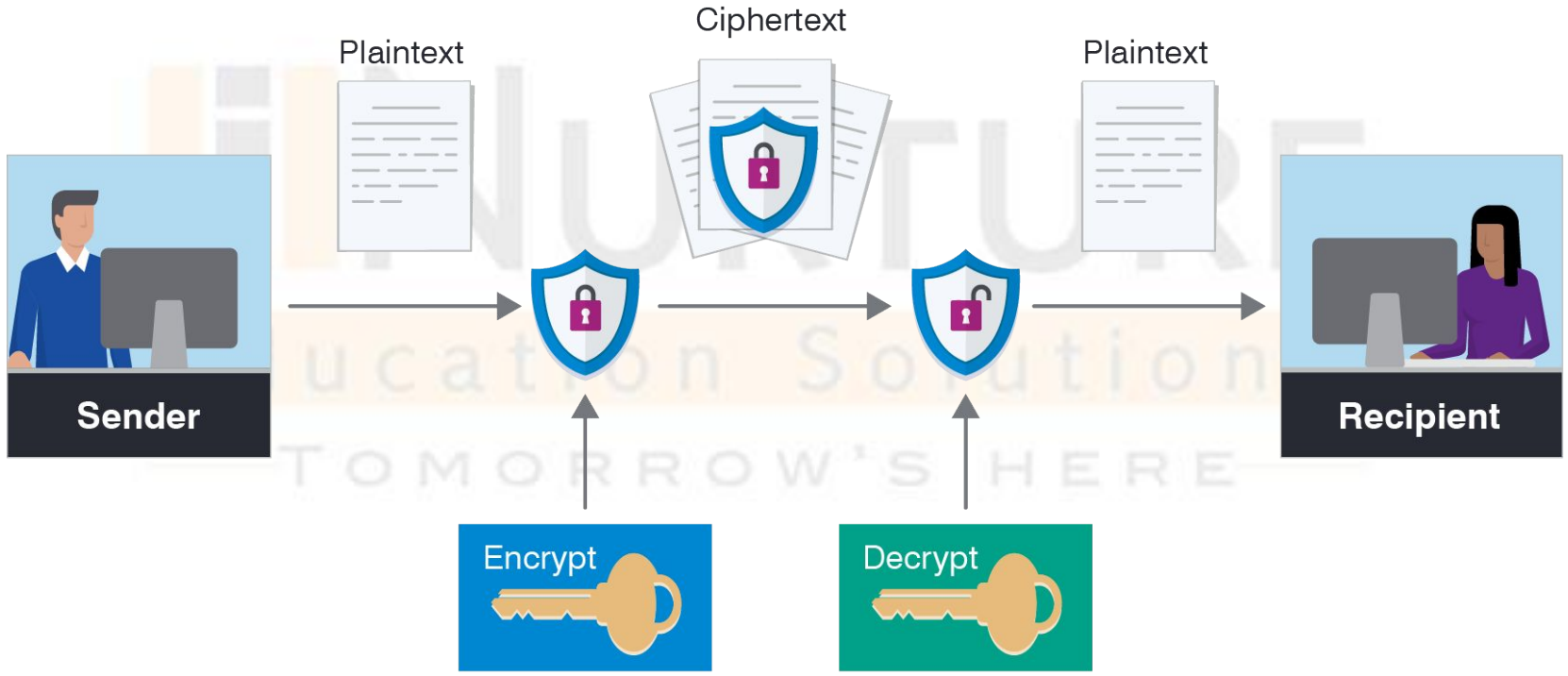
Countermeasures

- Common Countermeasures
- Encryption
- Hashing
- Authentication
- Authorisation
- Accounting

Countermeasures: Encryption

- Cryptography is derived from the Greek words kryptos, which means ‘hidden, secret’" and graphein, which means "writing“.
- Cryptology and cryptanalysis are two branches of the study of coding and patterns.
- The communication between two parties is intelligible to a third party or opponents.
- **Plaintext** refers to the message that was sent in its original form. The plaintext is converted into meaningless ciphertext by an algorithm or cypher.
- **Ciphertext** is a converted version of the original message that is based on an algorithm or cypher. It is readable but not understandable.

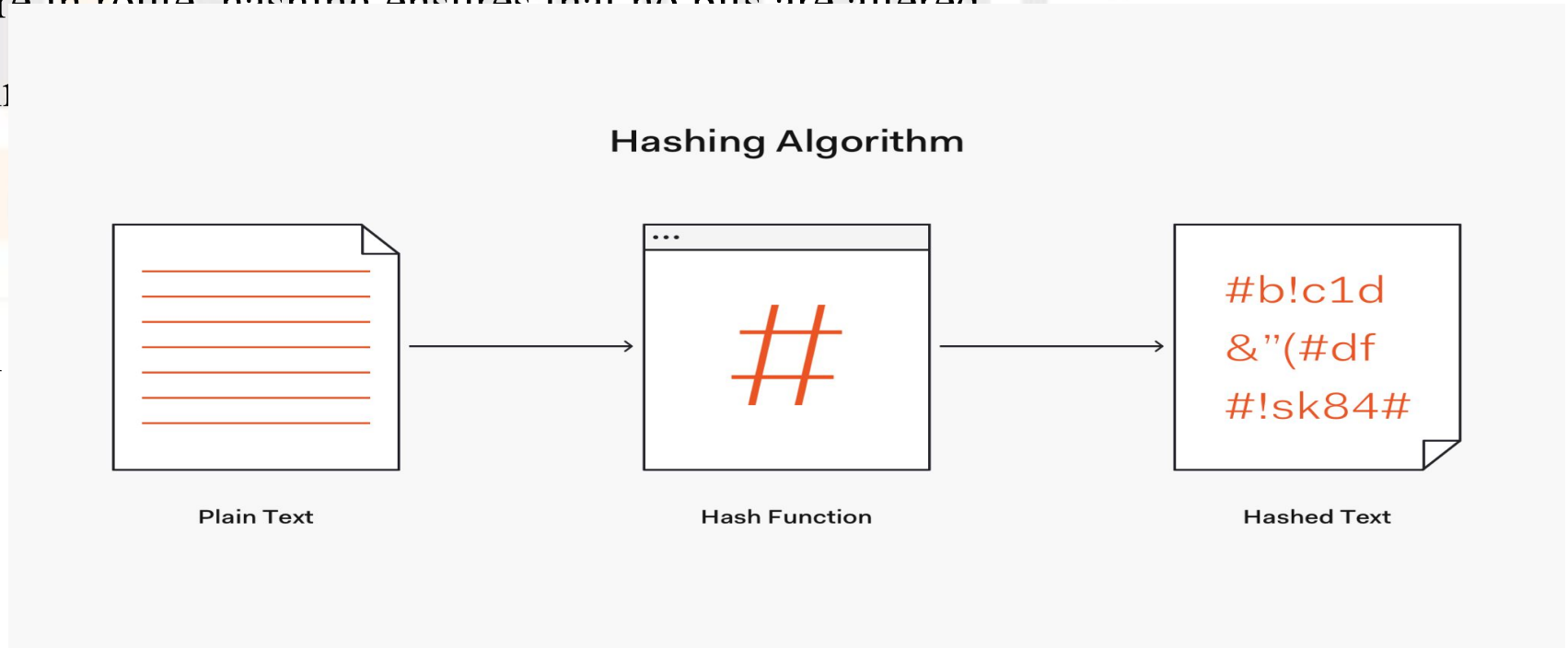
Countermeasures: Encryption (Contd…)



Different keys are used to encrypt and decrypt messages

Countermeasures: Hashing

- Hashing is a principle that falls under the Integrity category.
- Integrity refers to the fact that receivers receive the precise message that senders deliver.
- While messages are in route, hashing ensures that no bits are altered
- Widely used hashi
- MD5
- SHA-1
- SHA-256 or SHA



Countermeasures: Authentication

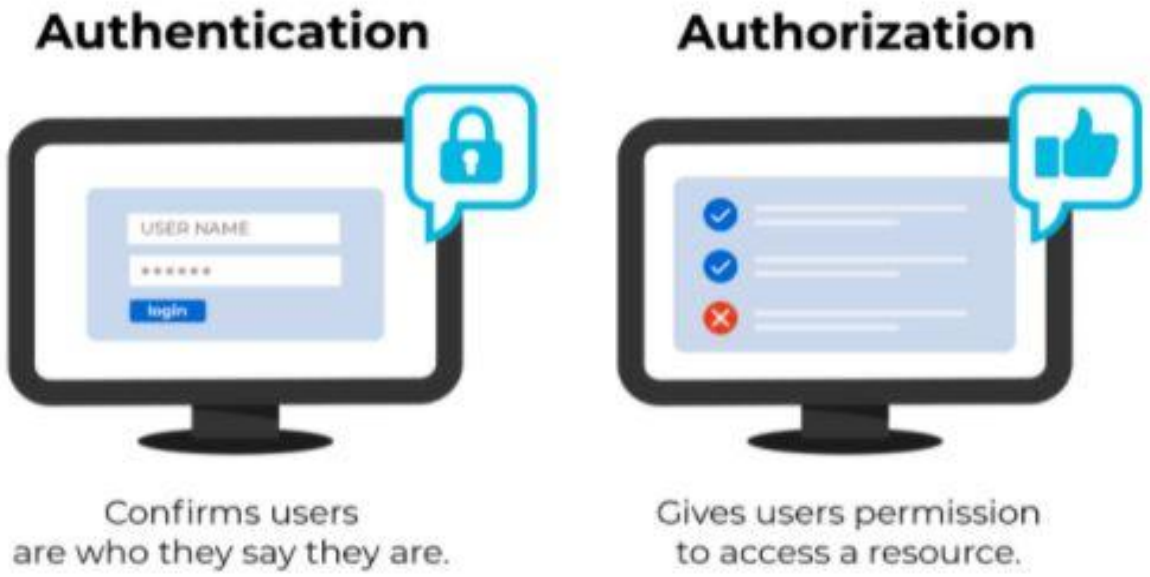
- When users log into a system, they must authenticate their identity.
- Users can use finger prints, retina scans (biometrics) or key fobs to enter their passwords.
- Multifactor authentication occurs when a user uses more than one of these techniques.
- Multifactor authentication is far more secure than single-factor authentication.
- Hackers would need your password as well as your key fob or fingerprint, for example. As a result, multifactor authentication is the combination of one digital factor and one physical factor.

Countermeasures: Authentication

- Following the authentication procedure, the system grants the user access to the network, websites and other resources based on the user's credentials.
- The principle of least privilege stops users from accessing confidential files unnecessarily and necessitates admin permission.

Benefits of the Principle of Least Privilege

- Better security
- Minimized attack surface
- Limited malware propagation
- Better stability
- Improved audit readiness



Countermeasures: Accounting

- Keeping logs and unsuccessful logins may aid in the resolution of a cybersecurity incident and provide useful information for investigations.
- Data logs can aid in the understanding of patterns, which can guide in the detection of aberrant events.

Summary

- Keeping logs and unsuccessful logins may aid in the resolution of a cybersecurity incident and provide useful information for investigations.
- The principle of least privilege stops users from accessing confidential files unnecessarily and necessitates admin permission.
- Cryptography is derived from the Greek words kryptos, which means ‘hidden, secret’" and graphein, which means "writing“.
- A vulnerability is a defect in software that allows malware to be installed and run without the user being aware of it.
- The term ‘availability’ refers to the fact that information is available to authorised persons whenever they need it. Data and system unavailability can have catastrophic effects.

Self Assessment Question

1. In cryptography, what is cipher?

a. Algorithm for performing encryption and decryption

b. Encrypted message

c. Both algorithm for performing encryption and decryption and encrypted message

d. Decrypted message

Answer: a

Self Assessment Question

2. Which of the following is /are offered by the Hash functions?

a. Authentication

b. Non-Repudiation

c. Data Integrity

d. All the above

Answer: d

Self Assessment Question

3. What is the process of identifying an individual?

a. Authentication

b. Authorisation

c. Accounting

d. Auditing

Answer: a

Assignment

1. Enlighten about principles of cybersecurity with an example.
2. Explain the different categories of vulnerabilities with an example.
3. Discuss about people-based vulnerabilities.
4. List out the actors involved in cyber security.
5. Describe countermeasures been followed to withstand an attack surface.
6. Write a short note on
   a. Hashing
   b. Accounting

Document Link

Topic	URL
Evolution of Cybersecurity	https://blog.avast.com/history-of-cybersecurity-avast
CIA Triad	https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
Vulnerabilities	https://www.upguard.com/blog/vulnerability

Video Link

Topic	URL
Exploit Vulnerabilities	https://www.youtube.com/watch?v=HMN9gQu-ZpQ
Vishing - Attempt	https://www.youtube.com/watch?v=lc7scxvKQOo
Hashing	https://www.youtube.com/watch?v=2BldESGZKB8
Encryption	https://www.youtube.com/watch?v=1y1M2fZqIlQ
Vulnerability, Threats and Risk	https://www.youtube.com/watch?v=26YCBoO_yQ4

E- Book Link

Topic	URL
Security in Computing	https://www.pdfdrive.com/security-in-computing-5_e-charles-p-pfleegerpdf-e33465017.html
Cryptography and Network Security	https://www.pdfdrive.com/william-stallings-cryptography-and-network-security-6e-e34874950.html