Unit -3 Security

Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe e-payments/transactions –

1. **Confidentiality** – Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.
2. **Integrity** – Information should not be altered during its transmission over the network.
3. **Availability** – Information should be available wherever and whenever required within a time limit specified.
4. **Authenticity** – There should be a mechanism to authenticate a user before giving him/her an access to the required information.
5. **Non-Repudiability** – It is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.
6. **Encryption** – Information should be encrypted and decrypted only by an authorized user.
7. **Auditability** – Data should be recorded in such a way that it can be audited for integrity requirements.

4 Reasons You Need e-Commerce Security
Privacy of Data
Trust
Authentication
Confirmation

3.1 Computer crime

Alternatively known as cyber crime, e-crime, electronic crime, or hi-tech crime. Computer crime is an act performed by a knowledgeable computer user, sometimes called a "hacker," that illegally browses or steals a company's or individual's private information. Sometimes, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Why do people commit computer crimes?

In most cases, someone commits a computer crime to obtain goods or money. Greed and desperation are powerful motivators for some people to try stealing through computer crimes. Some people may also commit a computer crime because they are pressured, or forced, to do so by another person.

Some people also commit computer crimes to prove they can do it. A person who can successfully execute a computer crime may find great personal satisfaction. These types of people, sometimes called black hat hackers, like to create chaos and wreak havoc on other people and companies.

Another reason computer crimes are sometimes committed is because they're bored. They want something to do and don't care if they commit a crime.

Examples of computer crimes

Below is a list of the different types of computer crimes today. Clicking any of the links gives further information about each crime.

- Child pornography - Making, distributing, storing, or viewing child pornography.
- Click fraud - Fraudulent clicks on Internet advertisements.
- Copyright violation - Stealing or using another person's Copyrighted material without permission.
- Cracking - Breaking or deciphering codes designed to protect data.
- Cyber terrorism - Hacking, threats, and blackmailing towards a business or person.
- Cyberbullying or Cyberstalking - Harassing or stalking others online.
- Cybersquatting - Setting up a domain of another person or company with the sole intention of selling it to them later at a premium price.
- Creating Malware - Writing, creating, or distributing malware (e.g., viruses and spyware.)
- Data diddling - Computer fraud involving the intentional falsification of numbers in data entry.
- Denial of Service attack - Overloading a system with so many requests it cannot serve normal requests.
- Data theft - Stealing others' personal or confidential information.
- Doxing - Releasing another person's personal information without their permission.
- Espionage - Spying on a person or business.
- Fake - Products or services that are not real or counterfeit. For example, a fake antivirus and fake technical support are examples of something fake.
- Fraud - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.
- Green Graffiti - A type of graffiti that uses projectors or lasers to project an image or message onto a building.
- Harvesting - Collect account or account-related information on other people.
- Human trafficking - Participating in the illegal act of buying or selling other humans.
- Identity theft - Pretending to be someone you are not.
- Illegal sales - Buying or selling illicit goods online, including drugs, guns, and psychotropic substances.
- Intellectual property theft - Stealing practical or conceptual information developed by another person or company.
- IPR violation - An intellectual property rights violation is any infringement of another's Copyright, patent, or trademark.
- Phishing or vishing - Deceiving individuals to gain private or personal information about that person.
- Pig butchering - SMS scam to get people to invest into a cryptocurrency scam.

- Ransomware - Infecting a computer or network with ransomware that holds data hostage until a ransom is paid.
- Salami slicing - Stealing tiny amounts of money from each transaction.
- Scam - Tricking people into believing something that is not true.
- Sextortion - Extortion where a victim's private data of a sexual nature is acquired illegally by another person.
- Slander - Posting libel or slander against another person or company.
- Software piracy - Copying, distributing, or using software not purchased by the software user.
- Spamming - Distributed unsolicited e-mails to dozens or hundreds of different addresses.
- Spoofing - Deceiving a system into thinking you are someone you're not.
- Swatting - The act of calling in a false police report to someone else's home.
- Theft - Stealing or taking anything (e.g., hardware, software, or information) that doesn't belong to you.
- Typosquatting - Setting up a domain that is a misspelling of another domain.
- Unauthorized access - Gaining access to systems you have no permission to access.
- Vandalism - Damaging any hardware, software, website, or other objects.
- Wiretapping - Connecting a device to a phone line to listen to conversations.

3.2 Threats and attacks on computer system

From a security standpoint, threats and attacks are two critical occurrences. From the perspective of network security, it is critical to grasp the differences between the two.

A threat in the realm of information security is the presence of a persistent hazard to information integrity. This might take the shape of a human, a computer virus or malware, or something else.

An attack, on the other hand, is the actual act of exploiting the information security system's weaknesses.

There are a number of network security dangers and attacks to be aware of, such as Information theft and fraud, putting a halt to routine business activities, viruses, cracking the passwords, Distributed Denial of Service (DDoS) attacks, eavesdropping, hacking of email, attempts at intrusion, spoofing a network, social engineering, etc.

What is a Threat?

A Threat is a possible security risk that might exploit the vulnerability of a system or asset. The origin of the threat may be accidental or environmental, human negligence, or human failure. There are various types of security threats such as Interruption, Interception, Fabrication, and Modification.

A threat is something that can gain access to, harm, or eliminate an asset by exploiting a vulnerability, whether purposefully or unintentionally. Threats can be divided into three categories −

- Floods, storms, and tornadoes are examples of natural disasters.
- Unintentional threats, such as an employee accessing incorrect information.
- Spyware, virus, adware companies, or the activities of a rogue employee are all examples of intentional dangers.
- Bugs and malware are classified as dangers because they can hurt your firm if you are exposed to a computerized attack rather than one carried out by humans.

Many firms do cyber threat assessments to determine where they should focus their monitoring, protection, and remediation efforts. So, if an asset is something you're attempting to protect, a threat is something you're trying to avoid.

What is an Attack?

An Attack is an intentional unauthorized action on a system. Attacks can be grouped into two categories −

- Active Attacks − An active attack is an attempt to change system resources or influence their operation.
- Passive Attacks − A passive attack is an attempt to understand or retrieve sensitive data from a system without influencing the system resources.

An attacker always has a motivation to misuse the system and generally wait for an opportunity to occur.

Difference between Threat and Attack:

The following table highlights the major differences between a Threat and an Attack −

Key	**Threat**	**Attack**
Intentional	Threats can be intentional like human negligence or unintentional like natural disasters.	The attack is a deliberate action. An attacker has a motive and plans the attack accordingly.
Malicious	A Threat may or may not be malicious.	An Attack is always malicious.
Definition	A Threat by definition is a condition/circumstance which can cause damage to the system/asset.	An Attack by definition is an intended action to cause damage to system/asset.
Chance for Damage	Chance to damage or information alteration varies from low to very high.	The chance to damage or information alternation is very high.
Detection	A threat is difficult to detect.	An attack is comparatively easy to detect.
Prevention	A threat can be prevented by controlling the vulnerabilities.	An attack cannot be prevented by merely controlling the vulnerabilities. Other measures like backup, detect and act, etc., are required to handle a

		cyber-attack.
Initiation	It might be started by the system or by an outsider.	It is always started by an outsider (system or user)

3.3 Software packages for privacy:

3.4 Hacking and computer virus :

Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system.

Computers have become mandatory to run successful businesses. It is not enough to have isolated computer systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. System hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cybercrimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

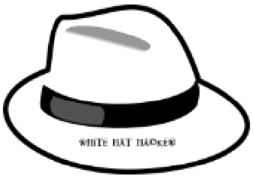
Who is a Hacker?

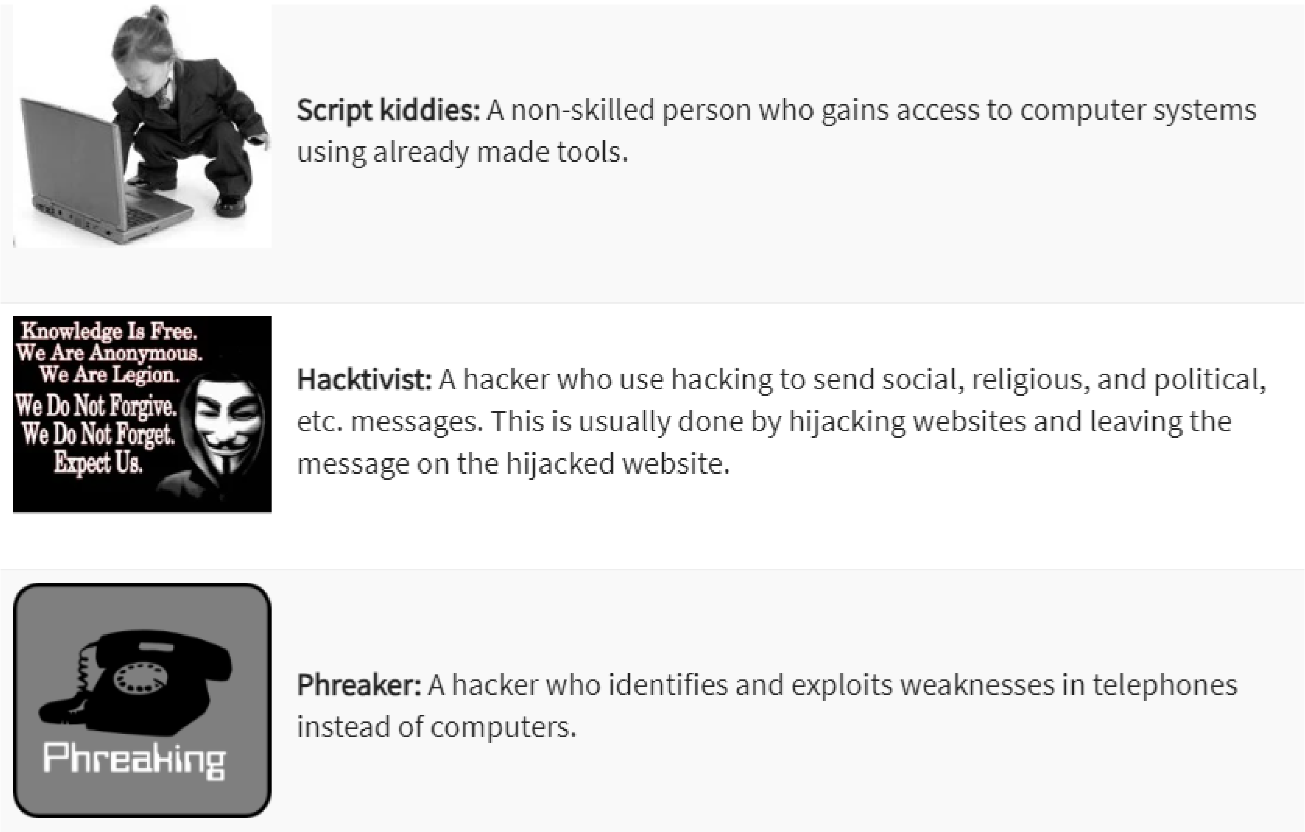
A **Hacker** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Types of Hackers:

Hackers are classified according to the intent of their actions. The following list classifies types of hackers according to their intent:

White Hat Hackers
Black Hat Hackers
Gray Hat Hackers
Script Kiddies
Green Hat Hackers
Blue Hat Hackers
Red Hat Hackers
State/Nation Sponsored Hackers
Hacktivist
The Bank Robber Hackers
The Corporate Spy
The Rogue Gamer
Cryptojackers
The Botnet Masters
The Adware Spammer
The Thrill Hacker
Malicious insider or Whistleblower
The Professional Hacking Group For
The Accidental Hacker
JanBask TRAINING
Learn and Grow

Symbol	Description
	**Ethical Hacker (White hat):** A security hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.
	Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
	Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.



Script kiddies: A non-skilled person who gains access to computer systems using already made tools.

Hacktivist: A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.

Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.

Introduction of Cybercrime:

Cybercrime is the activity of using computers and networks to perform illegal activities like spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrime hacks are committed through the internet, and some cybercrimes are performed using Mobile phones via SMS and online chatting applications.

Type of Cybercrime

- The following list presents the common types of cybercrimes:
- **Computer Fraud:** Intentional deception for personal gain via the use of computer systems.
- **Privacy violation:** Exposing personal information such as email addresses, phone number, account details, etc. on social media, hacking websites, etc.
- **Identity Theft:** Stealing personal information from somebody and impersonating that person.
- **Sharing copyrighted files/information:** This involves distributing copyright protected files such as eBooks and computer programs etc.

- **Electronic funds transfer:** This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.
- **Electronic money laundering:** This involves the use of the computer to launder money.
- **ATM Fraud:** This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.
- **Denial of Service Attacks:** This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
- **Spam:** Sending unauthorized emails. These emails usually contain advertisements.

What is Ethical Hacking?

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get **written permission** from the owner of the computer system and/or computer network before hacking.
- **Protect the privacy of the organization** been hacked.
- **Transparently report** all the identified weaknesses in the computer system to the organization.
- **Inform** hardware and software vendors of the **identified weaknesses**.

Why Ethical Hacking?

- Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization’s image and save an organization a lot of money.
- Fake hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

Legality of Ethical Hacking:

Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking. The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests an individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

Summary

- Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks.
- Cybercrime is committing a crime with the aid of computers and information technology infrastructure.
- Ethical Hacking is about improving the security of computer systems and/or computer networks.
- Ethical Hacking is legal.

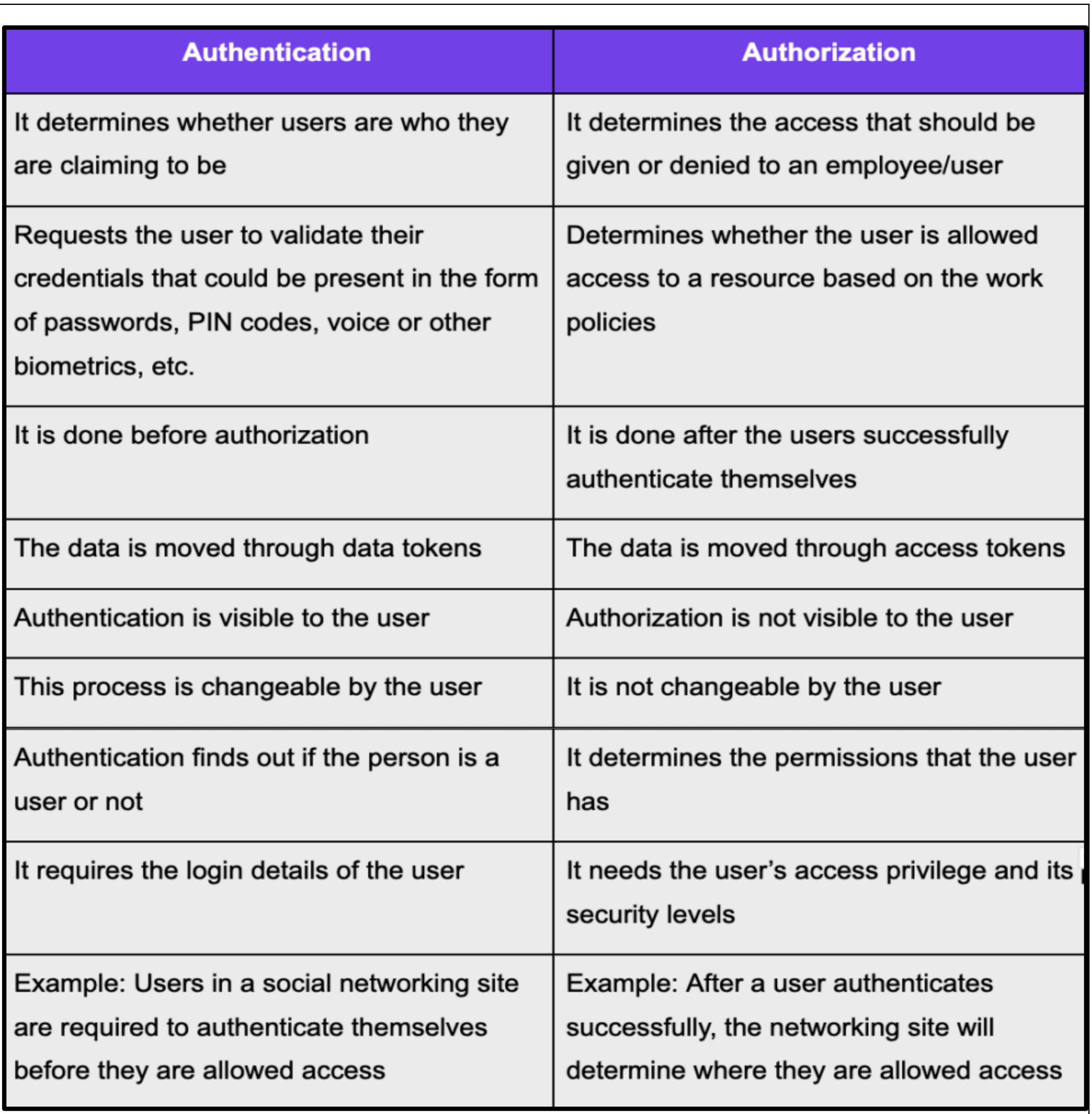
3.5 Security algorithms:

Data encryption is a common and effective security method—a sound choice for protecting an organization’s information. However, there are a handful of different encryption methods available, so how do you choose?

In a world where cybercrimes are on the rise, it’s comforting to know that there are as many methods available to protect network security as there are ways of trying to penetrate it. The real challenge is deciding which techniques an internet security expert should employ that best suits their organization’s specific situation.

Data encryption is a method of protecting data by encoding it in such a way that it can only be decrypted or accessed by an individual who holds the correct encryption key. When a person or entity accesses encrypted data without permission, it appears scrambled or unreadable.Data encryption is the process of converting data from a readable format to a scrambled piece of information. This is done to prevent prying eyes from reading confidential data in transit. Encryption can be applied to documents, files, messages, or any other form of communication over a network.

3.6 Authorization and authentication :

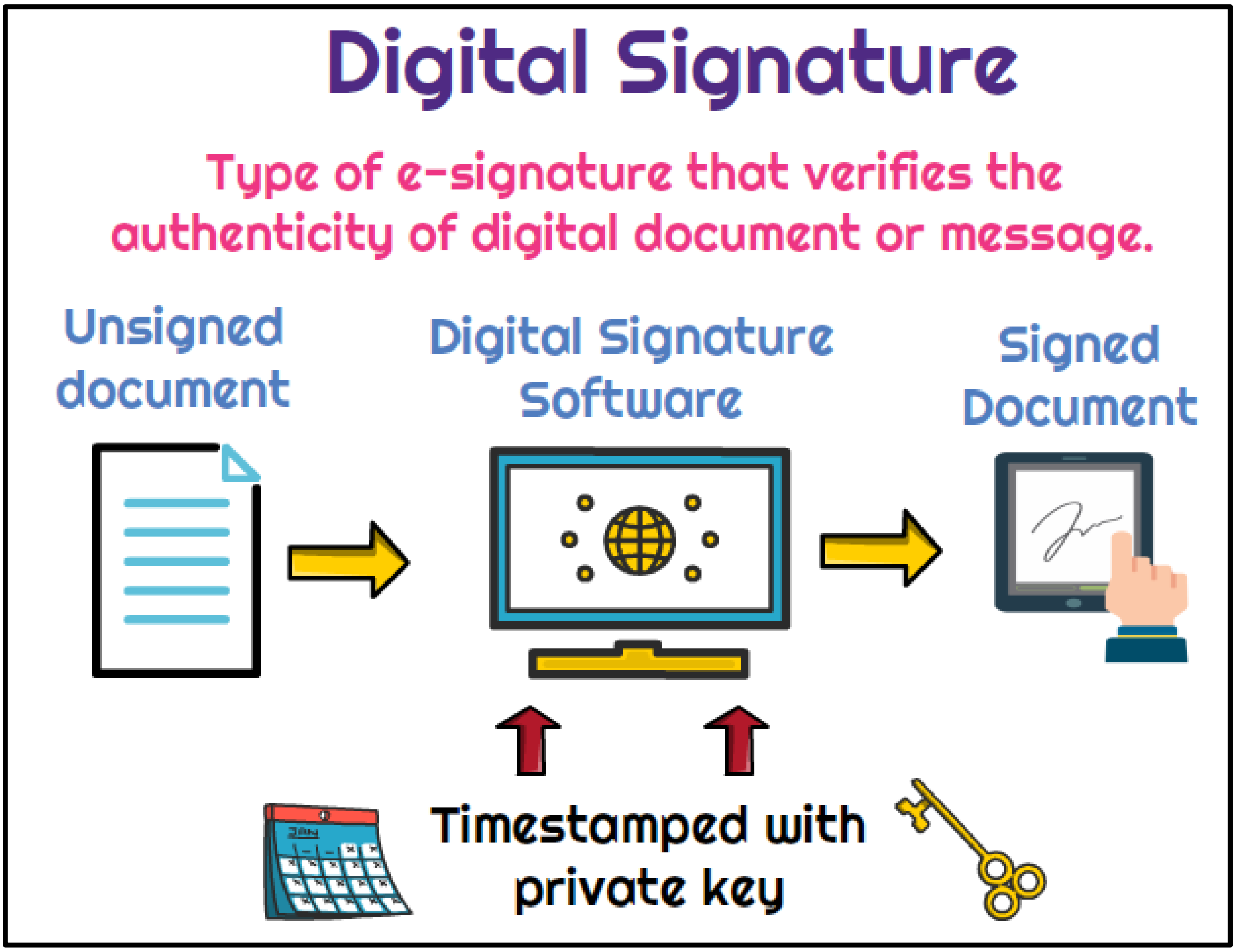


Authentication	Authorization
It determines whether users are who they are claiming to be	It determines the access that should be given or denied to an employee/user
Requests the user to validate their credentials that could be present in the form of passwords, PIN codes, voice or other biometrics, etc.	Determines whether the user is allowed access to a resource based on the work policies
It is done before authorization	It is done after the users successfully authenticate themselves
The data is moved through data tokens	The data is moved through access tokens
Authentication is visible to the user	Authorization is not visible to the user
This process is changeable by the user	It is not changeable by the user
Authentication finds out if the person is a user or not	It determines the permissions that the user has
It requires the login details of the user	It needs the user's access privilege and its security levels
Example: Users in a social networking site are required to authenticate themselves before they are allowed access	Example: After a user authenticates successfully, the networking site will determine where they are allowed access

3.7 Digital signature:

A digital signature is a type of electronic signature (e-signature) that verifies the authenticity of a digital document or message. Before digital signatures, you could sign a document and then the document owner could modify or change the document after you signed.

However, with a digital signature, the signature is timestamped and a private key is inserted to the specific document. So if the document changes, your signature will no longer be valid and the document will need to be re-signed.



Digital Signature

Type of e-signature that verifies the authenticity of digital document or message.

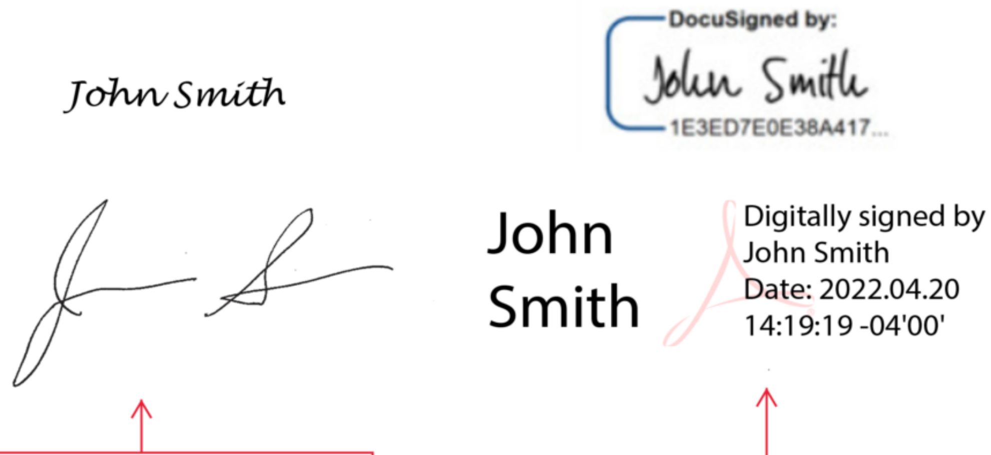
Unsigned document

Digital Signature Software

Signed Document

Timestamped with private key

Types of digital signature software included DocuSign, Hello Sign, Adobe Sign, etc. The private key is retained by the signor and anyone else will receive the public key which allows anyone to review the signed document.


John Smith
DocuSigned by:
John Smith
1E3ED7E0E38A417...
John Smith
Digitally signed by John Smith Date: 2022.04.20 14:19:19 -04'00'

The top example considered a "Typed" signature the lower example is a "Wet" signature. The NIH has been returning Other Support pages that include a "Typed" or "Wet" signatures.

The two examples above (DocuSigned and Adobe) are allowable as the electronic signature on an NIH Other Support document.

Unit -4 Electronic Data Interchange