CSC-370
E - Commerce
(BSc CSIT, TU)

Ganesh Khatri
kh6ganesh@gmail.com

Security in e-Commerce

- E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.
- 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
- Recent research indicates that cybercrime is on the rise for some major companies like Equifax, Yahoo, Facebook, etc, who find themselves as a victim of cyber-attacks

Dimensions of e-Commerce Security

- The most common security breaches for the ecommerce website are concerned with following six dimensions.
  - Integrity
  - Availability
  - Confidentiality
  - Non-repudiation
  - Authenticity
  - Privacy

Dimensions of e-Commerce Security

- **Integrity :**
  - We all have the one common question, whether we have received the same data that the sender has sent.
  - Now it is the duty for integrity for the correctness of the information that has been transmitted or received or displayed on a website over the internet
  - Integrity can ensure that information on the internet has not been altered in any way by an unauthorized party.
  - It maintains the consistency, accuracy, and trustworthiness of the information over its entire life cycle.
  - **Example :** The most common threat will be "would any unauthorized person will intercept and redirect payment into a different account" since ecommerce sites prefer online transfer mostly
  - Let us consider a subscription model, where you will give credit card details for a bill payment to the merchant. If someone added extra cost on your credit card bill without both yours or merchant's knowledge, then you need to pay extra money for something you haven't purchased

Dimensions of e-Commerce Security

- **Availability :**
  - Continuous availability of the data is the key to provide a better customer experience in ecommerce.
  - The continuous availability of the ecommerce website/app increases online visibility, search engine rankings, and site traffic.
  - Data which is present on the website/app must be secured and available 24 x 7 x 365 for the customer without downtime.
  - If it is not, it will be difficult to gain a competitive edge and survive in the digital world
  - **Customer perspective :** Can I access the site at any time from anywhere?
  - **Merchant perspective :** Whether my site is operating without any downtime?
  - **Example :** An ecommerce website can be flooded with useless traffic that causes to shut down your site, making impossible for the user to access the site

Dimensions of e-Commerce Security

- **Confidentiality :**
  - Confidentiality refers to protecting information from being accessed by an unauthorized person on the internet.
  - In other words, only the people who are authorized can gain access to view or modify or use the sensitive data of any customer or merchants
  - According to Juniper Research, nearly 146 billion records will be exposed by criminal data breaches between 2018 and 2023
  - **Customer perspective :** Can someone other than the intended recipient or a person read my message?
  - **Merchant perspective :** Whether information on my site can be accessed by the unauthorized person without knowledge?
  - **Example :** Ecommerce uses a user name and password to login to their account. Let's consider this case for resetting the password, where an ecommerce site sends a one-time password to their customer in email or phone number if someone else reads it

Dimensions of e-Commerce Security

- **Non-repudiation / Non-rejection :**
  - Good business depends on both buyers and sellers. They must not deny any facts or rules once they accept that there should not be any repudiation
  - Non-repudiation confirms whether the information sent between the two parties was received or not. It ensures that the purchase cannot be denied by the person who completed the transaction. In other words, it's an assurance that anyone cannot deny the validity of transaction
  - Mostly non-repudiation uses a digital signature for online transactions because no one can deny the authenticity of their signature on a document
  - Sometimes, customers claim that they haven't ordered the product from a particular merchant if they disliked the product later

Dimensions of e-Commerce Security

- **Authenticity :**
  - In ecommerce, since both the customer and seller need to trust each other, they must remain as who they are in real. Both the seller and buyer must provide proof of their original identity so that the ecommerce transaction can happen securely between them
  - Every ecommerce site uses authenticity as a tool to ensure the identity of the person over the internet. In ecommerce, fraudulent identity and authentication are also possible, which makes identity a difficult process.
  - Some common ways to ensure a person's identity are customer log in using a password
  - **Example :** Some users can use a fake email address to access any of the ecommerce services, so customer details should be analyzed and verified before giving them the access to the e-Commerce

Dimensions of e-Commerce Security

- **Privacy :**
  - Where confidentiality is a concern about the information present during communication, privacy is concerned with personal details
  - In general, privacy is used to control the usage of information by the customers that they have given to the merchant
  - According to Fortune, 1.16 billion email address and passwords are exposed in 2019 through security breaches
  - Privacy is a major threat to any online transaction or internet user since personal information has been revealed and there is no way back to disclose them
  - **Customer perspective :** Can I control the usage of information about myself that I have transmitted to the ecommerce site?
  - **Merchant perspective :** What if anyone else uses personal data collected as part of the ecommerce transaction? Is there any unauthorized person to access a customer's personal data?
  - **Example :** If a hacker breaks into the ecommerce site, they can gain access to the customer credit card details or any other customer information. This also violates information confidentiality and personal privacy.

Security Threats in E-commerce

- There's no doubt that the online retail market is booming.
- However, this success often attracts unwanted attention, and cyber-criminals have an ever-more sophisticated collection of methods to exploit gaps in online store security.
- As online stores become more advanced, it's important to keep up with the significant security risks that come with it.
- Let’s explore the different types of threats in eCommerce and best methods to avoid them.

Security Threats in E-commerce

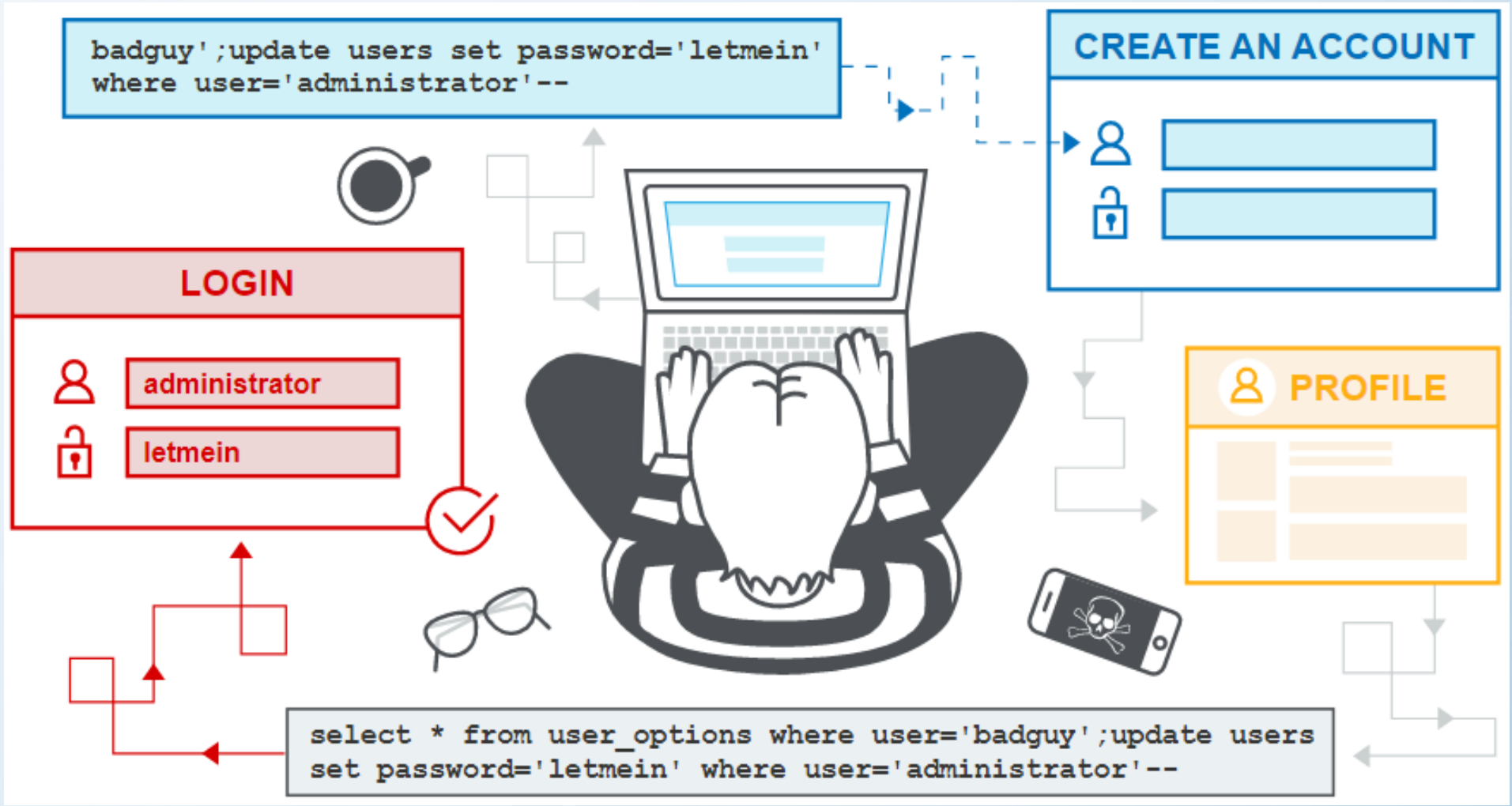
- Various security threats in eCommerce are :
  1. Vulnerabilities in eCommerce application
  2. Adware
  3. Spyware
  4. Social engineering
  5. Phishing
  6. Credit card fraud and Identity theft
  7. Spoofing and Pharming
  8. Client and Server Security
  9. Data Transaction Security

1. Vulnerabilities in eCommerce application

- These types of threats are due to different weaknesses or weak coding of applications. Different types of vulnerabilities are :
- **SQL Injection :**
  - SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.
  - It generally allows an attacker to view data that they are not normally able to retrieve.
  - This might include data belonging to other users, or any other data that the application itself is able to access.
  - In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

1. Vulnerabilities in eCommerce application

- **SQL Injection :**



1. Vulnerabilities in eCommerce application

- **SQL Injection :**
  - A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information
  - The majority of SQL injection vulnerabilities can be found quickly and reliably using different web vulnerability scanners like Burp Suite.
  - SQL injection can be detected manually by using a systematic set of tests against every entry point in the application.
  - SQL Injection can be prevented by avoiding the quotes(‘ ’) from SQL queries. Normally it can be done using prepared statements.
  - Eg : $stmt = $pdo->prepare(“SQL query”);
  - There are various other techniques to avoid it depending upon different languages.
  - One more popular method is “Parse Tree Validation Method to avoid SQL Injection”

1. Vulnerabilities in eCommerce application

- **Buffer Overflows :**
  - Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another.
  - A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer.
  - As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations
  - Attackers exploit buffer overflow issues by overwriting the memory of an application.
  - This changes the execution path of the program, triggering a response that damages files or exposes private information.
  - For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems

1. Vulnerabilities in eCommerce application

- **Buffer Overflows :**
  - Developers can protect against buffer overflow vulnerabilities via security measures in their code, or by using languages that offer built-in protection
  - modern operating systems have runtime protections as well like data execution prevention, Address space randomization etc
  - Security measures in code and operating system protection are not enough.
  - When an organization discovers a buffer overflow vulnerability, it must react quickly to patch the affected software and make sure that users of the software can access the patch

1. Vulnerabilities in eCommerce application

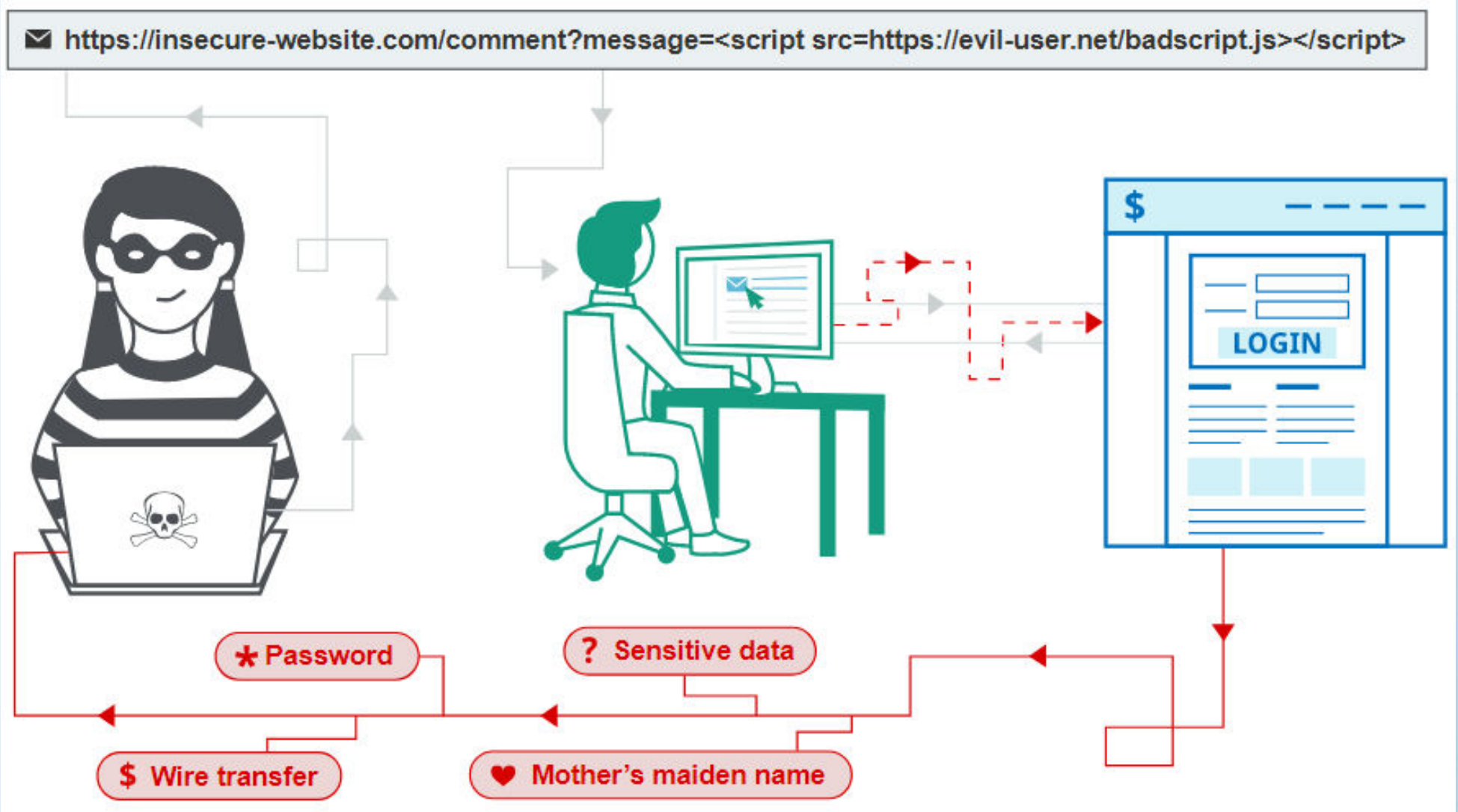
- **Remote Command Execution :**
  - Remote code execution is always performed by an automated tool. These attacks are typically written into an automated script
  - Remote arbitrary code execution is most often aimed at giving a remote user administrative access on a vulnerable system.
  - The attack is usually prefaced by an information gathering attack, in which the attacker uses some means such as an automated scanning tool to identify the vulnerable version of software.
  - Once identified, the attacker executes the script against the program with hopes of gaining local administrative access on the host
  - This is usually through the lack of proper input validation or verification.
  - For ecommerce platforms, this remains the most prevailing weakness that anyone can experience

1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**
  - Cross-site scripting (XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application.
  - It allows an attacker to circumvent the same origin policy, which is designed to separate different websites from each other
  - Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data.
  - If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.
  - Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript to users.
  - When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the application

1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**



1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**
  - There are 3 types of XSS attacks.
  1. **Reflected XSS :**
     - is the simplest variety of cross-site scripting.
     - It arises when an application receives data in an HTTP request and includes that data within the immediate response in an unsafe way.
     - If your website has URL of type https://insecure-website.com/status?message=All+is+well then an attacker can easily construct an attack like this : https://insecure-website.com/status?message=<script>/* Bad Stuff */</script>
     - If the user visits the URL constructed by the attacker, then the attacker's script executes in the user's browser, in the context of that user's session with the application.
     - At that point, the script can carry out any action, and retrieve any data, to which the user has access.

1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**
  - There are 3 types of XSS attacks.
  2. **Stored XSS :**
     - Stored XSS (also known as persistent or second-order XSS) arises when an application receives data from an untrusted source and includes that data within its later HTTP responses in an unsafe way
     - Suppose a website allows users to submit comments on blog posts, which are displayed to other users.
     - Users submit comments using an HTTP request like the following

       http://vulnerable-website.com/postId=3&comment=This+post+was+extremely+helpful.&name=Carlos+Montoya&email=carlos%40normal-user.net
     - After this comment has been submitted, any user who visits the blog post will receive the following within the application's response
       This post was extremely helpful.

1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**
  - There are 3 types of XSS attacks.

  2. Stored XSS :

  - Assuming the application doesn't perform any other processing of the data, an attacker can submit a malicious comment like this:
    <script>/* Bad stuff here... */</script>
  - Within the attacker's request, this comment would be URL-encoded as
    comment=%3Cscript%3E%2F*%2BBad%2Bstuff%2Bhere...%2B*%2F%3C%2Fscript%3E
  - Any user who visits the blog post will now receive the following within the application's response:
    <script>/* Bad stuff here... */</script>

1. Vulnerabilities in eCommerce application

- **Cross-site Scripting :**
  - There are 3 types of XSS attacks.
  2. **DOM-based XSS :**
     - DOM-based XSS arises when an application contains some client-side JavaScript that processes data from an untrusted source in an unsafe way, usually by writing the data back to the DOM

2. Adware

- Adware, often called advertising-supported software by its developers, is software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user.
- Some security professionals view it as the forerunner of the modern-day PUP (potentially unwanted program).
- Typically, it uses a method to either disguise itself as legitimate, or piggyback on another program to trick you into installing it on your PC, tablet, or mobile device

3. Spyware

- Spyware is a type of malicious software or malware that is installed on a computing device without the end user's knowledge.
- It invades the device, steals sensitive information and internet usage data, and relays it to advertisers, data firms or external users.
- Any software can be classified as spyware if it is downloaded without the user's authorization.
- Spyware is controversial because, even when it is installed for relatively innocuous reasons, it can violate the end user's privacy and has the potential to be abused
- Spyware is one of the most common threats to internet users.
- Once installed, it monitors internet activity, tracks login credentials and spies on sensitive information.
- The primary goal of spyware is usually to obtain credit card numbers, banking information and passwords.

3. Spyware : How to prevent?

- Maintaining strict cybersecurity practices is the best way to prevent spyware. Some best practices include the following
  - only downloading software from trusted sources
  - reading all disclosures when installing software
  - avoiding interaction with pop-up ads
  - staying current with updates and patches for browser, OS and application software

4. Social engineering

- Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.
- In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.
- Attacks can happen online, in-person, and via other interactions
- Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user's behavior.
- Once an attacker understands what motivates a user's actions, they can deceive and manipulate the user effectively.
- Social engineering attacks rely on actual communication between attackers and victims. The attacker tends to motivate the user into compromising themselves, rather than using brute force methods to breach your data

4. Social engineering : How does it work?

- The attack cycle gives these criminals a reliable process for deceiving you. Steps for the social engineering attack cycle are usually as follows :
  - **Prepare :** by gathering background information on you or a larger group you are a part of
  - **Infiltrate :** by establishing a relationship or initiating an interaction, started by building trust.
  - **Exploit the victim :** once trust and a weakness are established to advance the attack
  - **Disengage :** once the user has taken the desired action
- This process can take place in a single email or over months in a series of social media chats.
- It could even be a face-to-face interaction but it ultimately concludes with an action you take, like sharing your information or exposing yourself to malware

5. Phishing

- Phishing is a kind of social engineering attack.
- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords
- The information is then used to access important accounts and can result in identity theft and financial loss

5. Phishing : Common Features of Phishing Emails

- **Too Good To Be True :**
  - Attractive offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems to good to be true
- **Sense of Urgency :** -
  - A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just
- **Hyperlinks :** -
  - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different or it could be a popular website with a misspelling.

5. Phishing : Common Features of Phishing Emails

- **Attachments :**
  - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file.
- **Unusual Sender :** Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it!

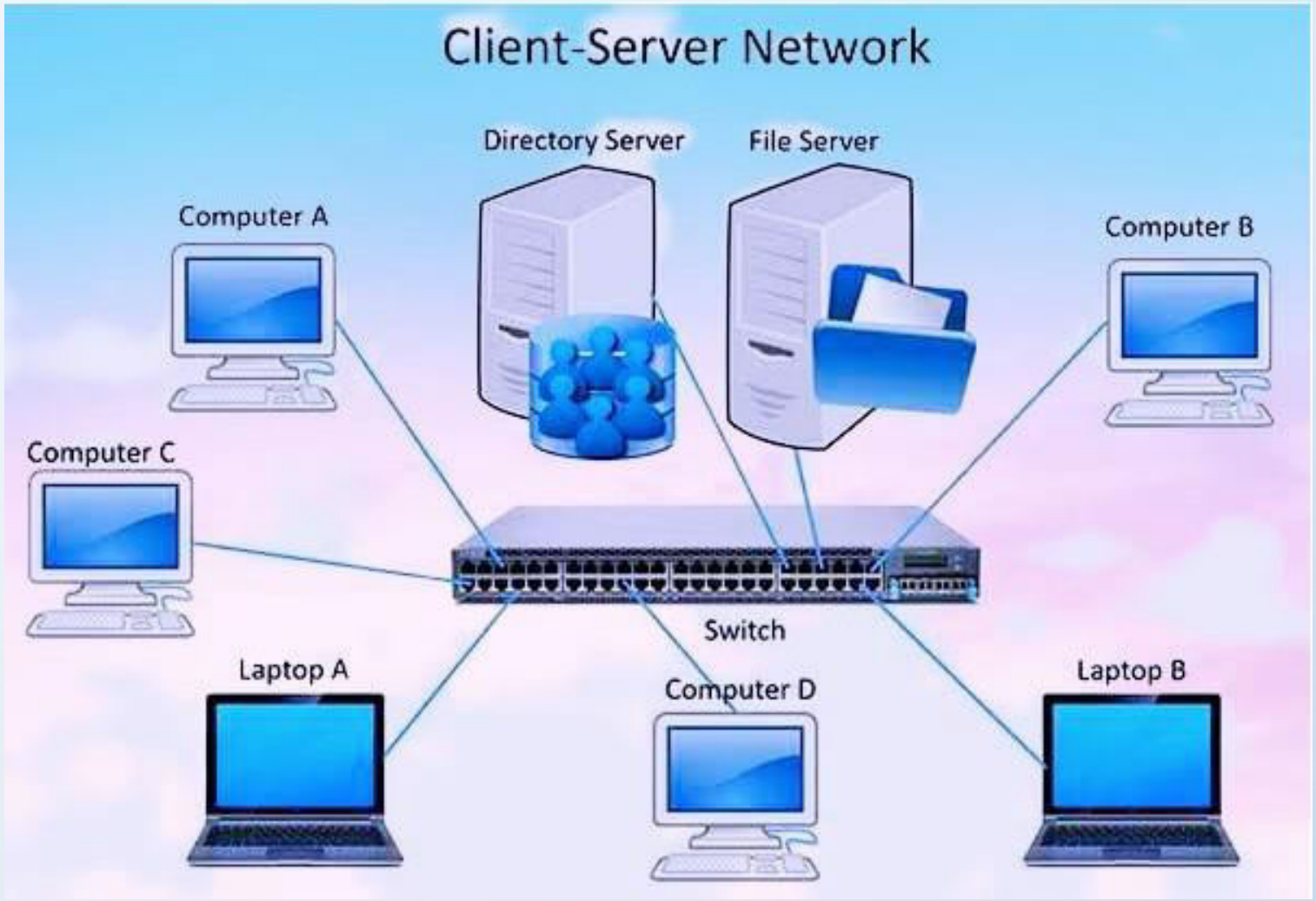
6. Credit card fraud and Identity theft

- **Credit card fraud** :
  - is a potential consequence of identity theft.
  - Here, a thief steals your credit card information and then makes purchases in a store or online.
  - Suppose, most credit card companies have a liability limit of $50.
  - This means that even if a thief has charged thousands of dollars to your card, you'd likely only have to pay $50.
  - More often than not, credit card companies simply wipe out any charges that are the result of fraud
- **identity theft :**
  - involves much more than a few fraudulent charges.
  - Identity thieves can steal your personal information to open a new line of credit, open a new credit card, or obtain a false ID in your name.
  - Unlike credit card fraud, there's no liability limit. That means you might end up paying for all the damage caused by an identity thief.

7. Spoofing and Pharming

- **Spoofing**
  - describes a criminal who impersonates another individual or organization, with the intent to gather personal or business information
- **Pharming**
  - is a malicious website that resembles a legitimate website, used to gather usernames and passwords
  - pharming is a advance technique to get users credentials by making effort to entering users into the website
  - In order words, it misdirects users to a fake website that appears to be official and victims gives their personal information by fault.
  - In pharming, fake website is created which appears to be official. Users then access the website and request is popped up regarding username and password and other credentials
- **Note :** Differences between Phishing and Farming : https://www.geeksforgeeks.org/difference-between-phishing-and-pharming

8. Client/Server Security

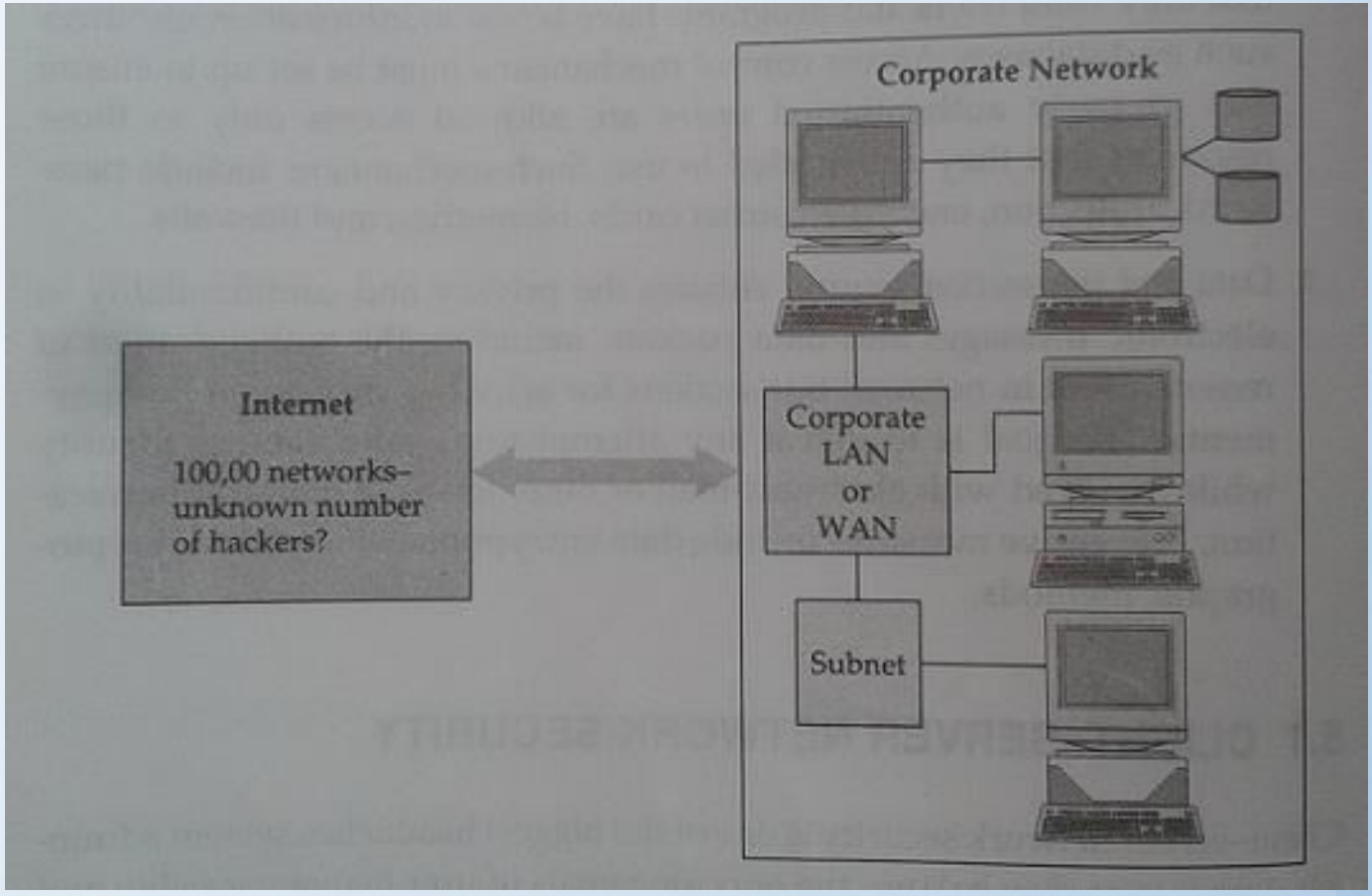


8. Client and Server Security

- A client-server network is a network consisting of a central computer, also known as a server, which hosts data and other forms of resources and clients such as laptops and desktop computers contact the server and request to use data or share its other resources with it
- A network security is defined as a circumstance, condition with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse
- uses various authorization methods to make sure that only valid user and programs have access to information resources such as databases.
- Access control mechanisms must be set up to ensure that properly authenticated users are allowed access only to those resources that they are entitled to use.
- Such mechanisms include password protection, encrypted smart cards, biometrics, and firewalls

8. Client and Server Security

- According to the National Center for Computer Crime Data, computer security violations cost U.S. businesses half a billion dollars each year
- Network security on the Internet is a major concern for commercial organizations, especially top management.
- Recently, the Internet has raised many new security concerns.
- By connecting to the Internet, a local network organization may be exposing itself to the entire population on the Internet.
- As given figure illustrates, an internet connection opens itself to access from other networks comprising the public Internet



unprotected internet connection

8. Client and Server Security

- Client/server network security problems manifest themselves in three ways
  - **Physical security holes**
  - **Software security holes**
  - **Inconsistent usage holes**
- **Physical Security Holes**
  - result when individuals gain unauthorized physical access to a computer.
  - A good example would be a public workstation room, where it would be easy for a hacker to reboot a machine into single-user mode and tamper with the files, if precautions are not taken.
  - On the network, this is also a common problem, as hackers gain access to network systems by guessing passwords of various users

8. Client and Server Security

- **Software Security Holes**
  - result when badly written programs or "privileged" software are "compromised" into doing things they shouldn’t.
  - The most famous example of this category is the "sendmail" hole, which brought the Internet to its knees in 1988.
  - A more recent problem was the "rlogin" hole in the IBM RS-6000 workstations, which enabled a cracker (a malicious hacker) to create a "root" shell or superuser access mode.
  - This is the highest level of access possible and could be used to delete the entire file system, or create a new account or password file etc.

8. Client and Server Security

- **Inconsistent Usage Holes**
  - result when a system administrator assembles a combination of hardware and software such that the system is seriously flawed from a security point of view.
  - The incompatibility of attempting two unconnected but useful things creates the security hole.
  - Problems like this are difficult to isolate once a system is set up and running, so it is better to carefully build the system with them in mind.
  - This type of problem is becoming common as software becomes more complex
- To reduce these security threats, various protection methods are used.
- At the file level, operating systems typically offer mechanisms such as access control lists that specify the resources various users and groups are entitled to access
- Protection, also called authorization or access control - grants privileges to the system or resource by checking user-specific information such as passwords.

8. Client and Server Security

- Over the years, several protection methods have been developed :
  - **Trust-Based Security**
  - **Security through Obscurity**
  - **Password Schemes**
  - **Biometric Systems** etc
- **Trust-Based Security :**
  - trust-based security means to trust everyone and do nothing extra for protection.
  - It is possible not to provide access restrictions of any kind and to assume that all users are trustworthy and competent in their use of the shared network.
  - This approach assumes that no one ever makes an expensive breach such as getting root access and deleting all files (a common hacker trick).
  - This approach worked in the past, when the system administrator had to worry about a limited threat. Today, this is no longer the case

8. Client and Server Security

- **Security through Obscurity :**
  - Most organizations in the mainframe era practiced a philosophy known as security through obscurity (STO) - the notion that any network can be secured as long as nobody outside its management group is allowed to find out anything about its operational details and users are provided information on a need-to-know basis.
  - Hiding account passwords in binary files or scripts with the presumption that "nobody will ever find them" is a prime case of STO (somewhat like hiding the housekey under the doormat and telling only family and friends).
  - In short, STO provides a false sense of security in computing systems by hiding information

8. Client and Server Security

- **Password Schemes :**
  - a password scheme, creates a first-level barrier to accidental intrusion.
  - In actuality, however, password schemes do little about deliberate attack, especially when common words or proper names are selected as passwords.
  - The simplest method used by most hackers is dictionary comparison - comparing a list of encrypted user passwords against a dictionary of encrypted common words.
  - This scheme often works because users tend to choose relatively simple or familiar words as passwords.
  - To beat the dictionary comparison method, experts often recommend using a minimum of eight-character length mixed-case passwords containing at least one non - alphanumeric character and changing passwords every 60 to 90 days

8. Client and Server Security

- **Biometric Systems :**
  - Biometric systems, the most secure level of authorization, involve some unique aspect of a person's body.
  - Past biometric authentication was based on comparisons of fingerprints, palm prints, retinal patterns, or on signature verification or voice recognition.
  - Biometric systems are very expensive to implement : At a cost of several thousand dollars per reader station, they may be better suited for controlling physical access where one biometric unit can serve for many workers than for network or workstation access.
  - Many biometric devices also carry a high price in terms of inconvenience; for example, some systems take 10 to 30 seconds to verify an access request

9. Data Transaction Security

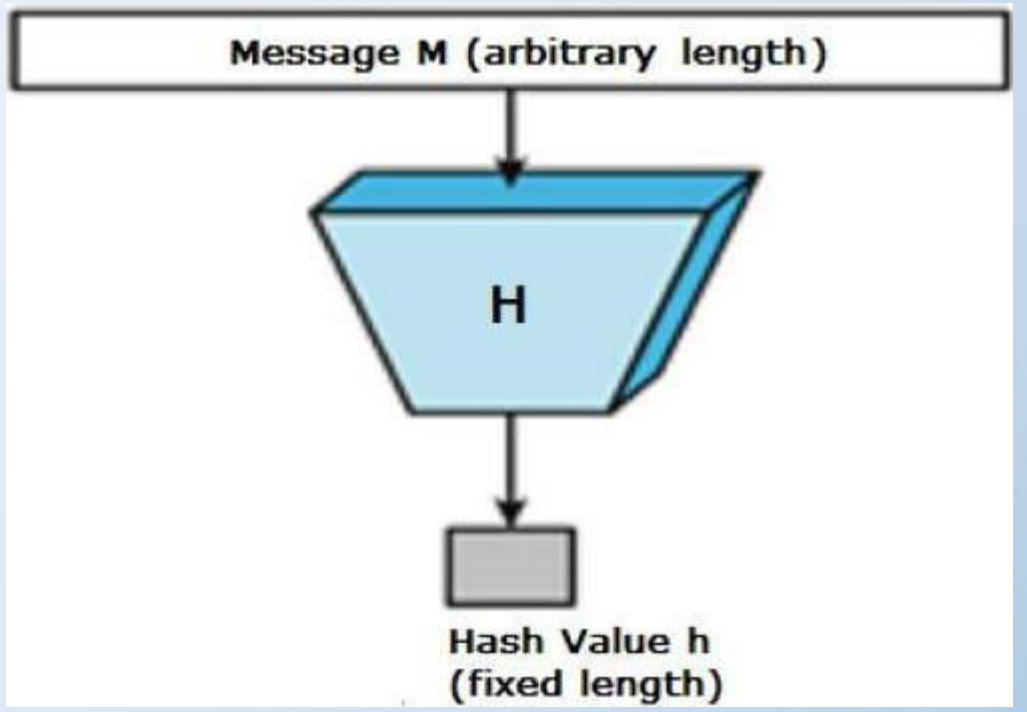
- Many people regularly bank and shop online with ease, confident that the millions of transactions that take place each day are secure.
- Good safeguards are in place, but as the internet is constantly susceptible to new threats, these best practices will help you keep your money and financial information safe
- Online buying presents challenges to keeping your money safe, but if you're smart, they're challenges that aren't too hard to overcome
- Different methods can be used to secure online transactions
  1. Picking a secure password
  2. Two-factor authentication
  3. Use of well known and secured payment gateway apps.
  4. Use of web browser privacy mode
  5. Keeping the browser up to date
  6. Disable Autocomplete/Password storage in-browser
  7. Passwords - make them complex, change them frequently etc.

9. Data Transaction Security

- is an algorithm that takes an arbitrary amount of data input - a credential - and produces a fixed-size output of enciphered text called a hash value, or just "hash." or message digest.
- That enciphered text can then be stored instead of the password itself, and later used to verify the user.
- hash functions are extremely useful and appear in almost all information security applications.
- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value.
- The input to the hash function is of arbitrary length but output is always of fixed length.

Security Mechanisms : Hash Functions

- **Features**
  - **Fixed Length Output (Hash Value) :** Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as hashing the data. In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions
  - **Efficiency of Operation :** Generally for any hash function h with input x, computation of h(x) is a fast operation. Computationally hash functions are much faster than a symmetric encryption



Security Mechanisms : Hash Functions

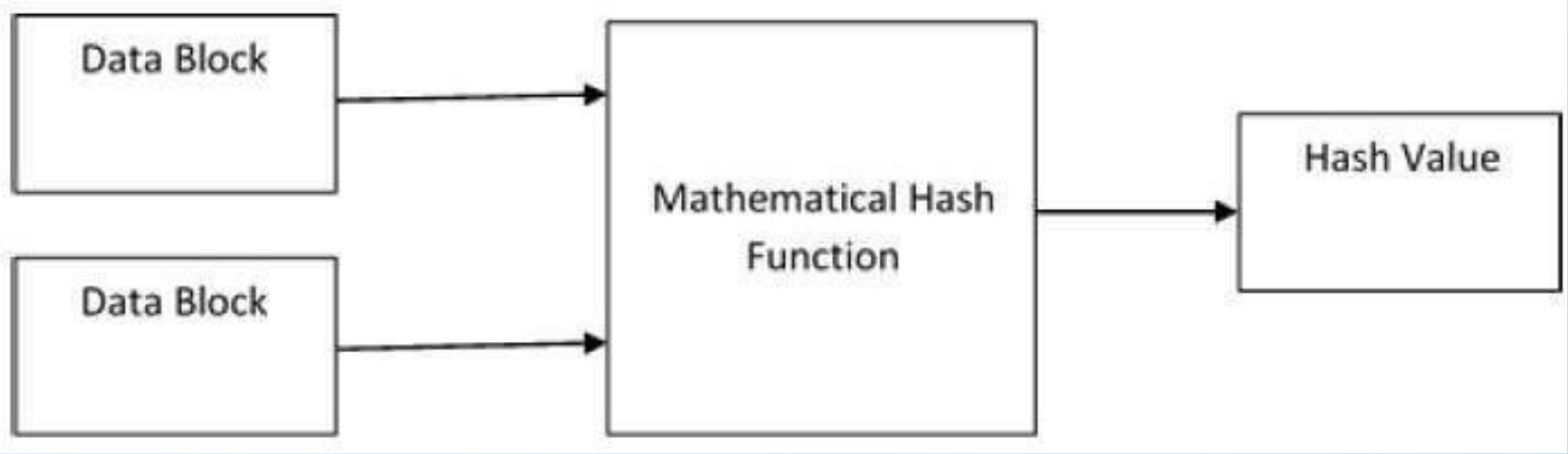
- **Properties :**
- **Pre-Image Resistance :**
  - This property means that it should be computationally hard to reverse a hash function.
  - In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
  - This property protects against an attacker who only has a hash value and is trying to find the input
- **Second Pre-Image Resistance :**
  - This property means given an input and its hash, it should be hard to find a different input with the same hash.
  - In other words, if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).

Security Mechanisms : Hash Functions

- **Properties :**
- **Collision Resistance :**
  - This property means it should be hard to find two different inputs of any length that result in the same hash.
  - This property is also referred to as collision free hash function.
  - In other words, for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y).
  - Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions.
  - This property of collision free only confirms that these collisions should be hard to find.
  - This property makes it very difficult for an attacker to find two input values with the same hash

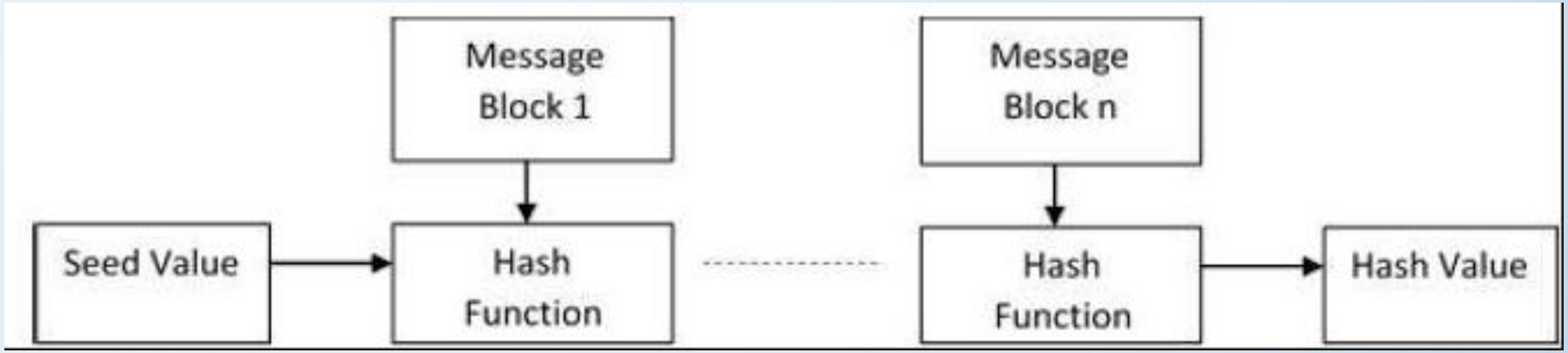
Security Mechanisms : Hash Functions

- **Design of Hashing Algorithms**
  - At the heart of a hashing is a mathematical function that operates on two fixed-size blocks of data to create a hash code.
  - This hash function forms the part of the hashing algorithm.
  - The size of each data block varies depending on the algorithm.
  - Typically the block sizes are from 128 bits to 512 bits.
  - The following illustration demonstrates hash function :



Security Mechanisms : Hash Functions

- **Design of Hashing Algorithms**
  - Hashing algorithm involves rounds of above hash function like a block cipher.
  - Each round takes an input of a fixed size, typically a combination of the most recent message block and the output of the last round.
  - this process is repeated for as many rounds as are required to hash the entire message.
  - Schematic of hashing algorithm is depicted in the following illustration



Security Mechanisms : Hash Functions

- **Design of Hashing Algorithms**
  - Since, the hash value of first message block becomes an input to the second hash operation, output of which alters the result of the third operation, and so on.
  - This effect, known as an avalanche effect of hashing
  - **Hash function** generates a hash code by operating on two blocks of fixed-length binary data
  - **Hashing algorithm** is a process for using the hash function, specifying how the message will be broken up and how the results from previous message blocks are chained together

Security Mechanisms : Hash Functions

- Examples of popular hash functions are :
- **Message Digest(MD) :**
  - It is a 128-bit hash function.
  - Different versions are MD2, MD4, MD5 and MD6
  - Most popular version is MD5.
  - In 2004, collisions were found in MD5. An analytical attack was reported to be successful only in an hour by using computer cluster.
  - This collision attack resulted in compromised MD5 and hence it is no longer recommended for use

Security Mechanisms : Hash Functions

- Examples of popular hash functions are :
- **Secure Hash Function (SHA) :**
  - Different versions are : SHA-0, SHA-1, SHA-2, and SHA-3
  - The original version is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology (NIST) in 1993.
  - SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security.
  - SHA-3 is the latest version developed in 2012.

Security Mechanisms : Hash Functions

- Examples of popular hash functions are :
- **RIPEMD :**
  - The RIPEMD is an acronym for RACE Integrity Primitives Evaluation Message Digest.
  - This set of hash functions was designed by open research community and generally known as a family of European hash functions.
  - Versions : RIPEMD, RIPEMD-128, and RIPEMD-160. There also exist 256, and 320-bit versions of this algorithm.

Security Mechanisms : Hash Functions

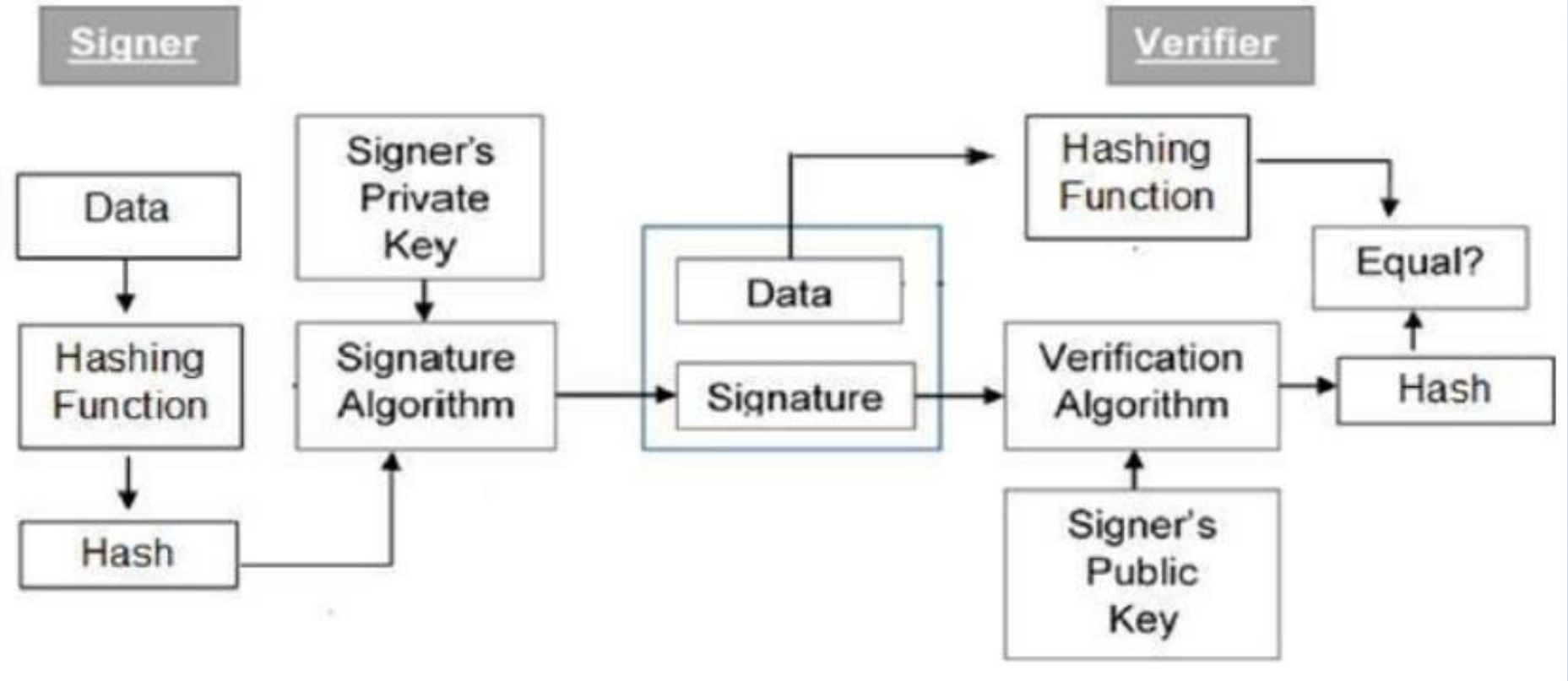
- Examples of popular hash functions are :
- **Whirlpool :**
  - This is a 512-bit hash function.
  - It is derived from the modified version of Advanced Encryption Standard (AES). One of the designer was Vincent Rijmen, a co-creator of the AES.
  - Three versions of Whirlpool have been released; namely WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL.

Security Mechanisms : Digital Signatures

- A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature.
- The Digital Signature Algorithm (DSA) was developed by the National Institute of Standards and Technology
- Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer
- In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message
- Similarly, a digital signature is a technique that binds a person/entity to the digital data.
- This binding can be independently verified by receiver as well as any third party

Security Mechanisms : Model of Digital Signature

- digital signature scheme is based on public key cryptography.
- The model of digital signature scheme is depicted in the following illustration



Security Mechanisms : Model of Digital Signature

- **Process :**
  - Each person adopting this scheme has a public-private key pair
  - Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key
  - Signer feeds data to the hash function and generates hash of data
  - Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier
  - Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output
  - Verifier also runs same hash function on received data to generate hash value
  - For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid
  - Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future

Security Mechanisms : Importance of Digital Signature

- Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security
- **Message Authentication :**
  - When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else
- **Data Integrity :**
  - In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails.
  - The hash of modified data and the output provided by the verification algorithm will not match.
  - Hence, receiver can safely deny the message assuming that data integrity has been breached.

Security Mechanisms : Importance of Digital Signature

- **Non-repudiation :**
  - Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data.
  - Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.
- By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely – Privacy, Authentication, Integrity, and Non-repudiation

Security Mechanisms : Digital Authentication

- is the process of verifying that users or devices are who or what they claim to be in order to enable access to sensitive applications, data and services.
- there are multiple ways to verify electronic authenticity. Here's an outline of the most popular digital authentication methods in the enterprise today.
  1. Unique passwords
  2. Preshared key (PSK)
  3. Biometric authentication
  4. Two-factor authentication (2FA)
  5. Behavioral authentication
  6. Device recognition etc

Security Mechanisms : Digital Authentication

1. **Unique passwords :**
   - In the enterprise, passwords remain the most common digital authentication method
   - User or devices typically have their own username that is not secret
   - This username is combined with a unique and secret password known only by the users or devices to access company data, applications and services
   - While the unique password authentication method works, it can become burdensome to end users due to the number of passwords they must manage.
   - This is one reason why technologies such as single sign-on(SSO) have become so popular.
   - With SSO, users must only remember a single secret password that will authenticate them and allow access to multiple corporate services

Security Mechanisms : Digital Authentication

2. Preshared key (PSK) :

- A PSK is a password that is only shared among users or devices that are authorized to access the same resources
- The most common example of PSK use within the enterprise is during Wi-Fi authentication
- A PSK is often used to allow employees to gain access to the corporate network.
- However, because the password is shared, it is considered less secure than individual password alternatives.

Security Mechanisms : Digital Authentication

3. **Biometric authentication :**
   - Look at lecture 3 for this.

Security Mechanisms : Digital Authentication

4. Two-factor authentication (2FA) :

- 2FA takes the process of a standard username and unique secret password and applies a second layer of verification.
- This second layer in 2FA may include a text message sent to a specific mobile phone number when access is granted, the use of software tokens/QR codes, biometric authentication or push notifications to the user

Security Mechanisms : Digital Authentication

5. Behavioral authentication :

- is a more complex method for verifying users.
- is commonly implemented in highly sensitive businesses deals.
- Behavioral biometric verification can involve analyzing keystroke dynamics or mouse-use characteristics.
- To verify a user or machine, AI analyzes user data or a device's typical computing behavior.
- If that behavior veers outside of predefined baselines, it triggers a lockdown of what that user or device is authorized to access
- Eg : google reCaptcha

Security Mechanisms : Digital Authentication

6. Device recognition :

- platforms can be implemented that recognize authorized hardware and immediately allow them access to certain network resources.
- This type of authentication is most used in companies with BYOD(Bring Your Own Devices) policies.
- It is an added precaution to ensure that only devices that are considered appropriate can connect to the network.

Security Mechanisms : Intrusion Detection System(IDS)

- is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.
- It is a software application that scans a network or a system for harmful activity or policy breaching.
- Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system.
- A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms

Security Mechanisms : IDS Types

1. **Network Intrusion Detection System (NIDS) :**
   - NIDS are set up at a planned point within the network to examine traffic from all devices on the network.
   - It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks.
   - Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator.
   - An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall

Security Mechanisms : IDS Types

2. Host Intrusion Detection System (HIDS) :

- HIDS run on independent hosts or devices on the network.
- HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.
- It takes a snapshot of existing system files and compares it with the previous snapshot.
- If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate.
- An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

Security Mechanisms : IDS Types

3. Protocol-based Intrusion Detection System (PIDS) :

- PIDS comprises of a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server.
- It tries to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol.

4. Application Protocol-based Intrusion Detection System (APIDS) :

- APIDS is a system or agent that generally resides within a group of servers.
- It identifies the intrusions by monitoring and interpreting the communication on application specific protocols.
- For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

Security Mechanisms : IDS Types

5. Hybrid Intrusion Detection System :

- is made by the combination of two or more approaches of the intrusion detection system.
- In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system.
- Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system.

Security Mechanisms : Secured Socket Layer (SSL)

- provides security to the data that is transferred between web browser and server.
- SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.
- SSL was the most widely deployed cryptographic protocol to provide security over internet communications.
- One common example is when SSL is used to secure communication between a web browser and a web server. This turns a website's address from HTTP to HTTPS, the ‘S’ standing for ‘secure’
- Technically, SSL is a transparent protocol which requires little interaction from the end user when establishing a secure session.

Security Mechanisms : Secured Socket Layer (SSL)

- With so much of our day to day transactions and communications happening online, there is very little reason for not using SSL.
- SSL supports the following information security principles :
  - **Encryption :** protects data transmissions (e.g. browser to server, server to server, application to server, etc.)
  - **Authentication :** ensures the server you're connected to is actually the correct server
  - **Data integrity :** ensures that the data that is requested or submitted is what is actually delivered.
- To adopt SSL in your business, you should purchase an SSL Certificate.

Security Mechanisms : Secured Socket Layer (SSL)

- SSL can be used to secure :
  - Online credit card transactions or other online payments.
  - Intranet-based traffic, such as internal networks, file sharing, extranets and database connections.
  - Webmail servers like Outlook Web Access, Exchange and Office Communications Server.
  - the connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange.
  - The transfer of files over HTTPS and FTP(s) services, such as website owners updating new pages to their websites or transferring large files.
  - System logins to applications and control panels like Parallels, cPanel and others.
  - Workflow and virtualization applications like cloud-based computing platforms.