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

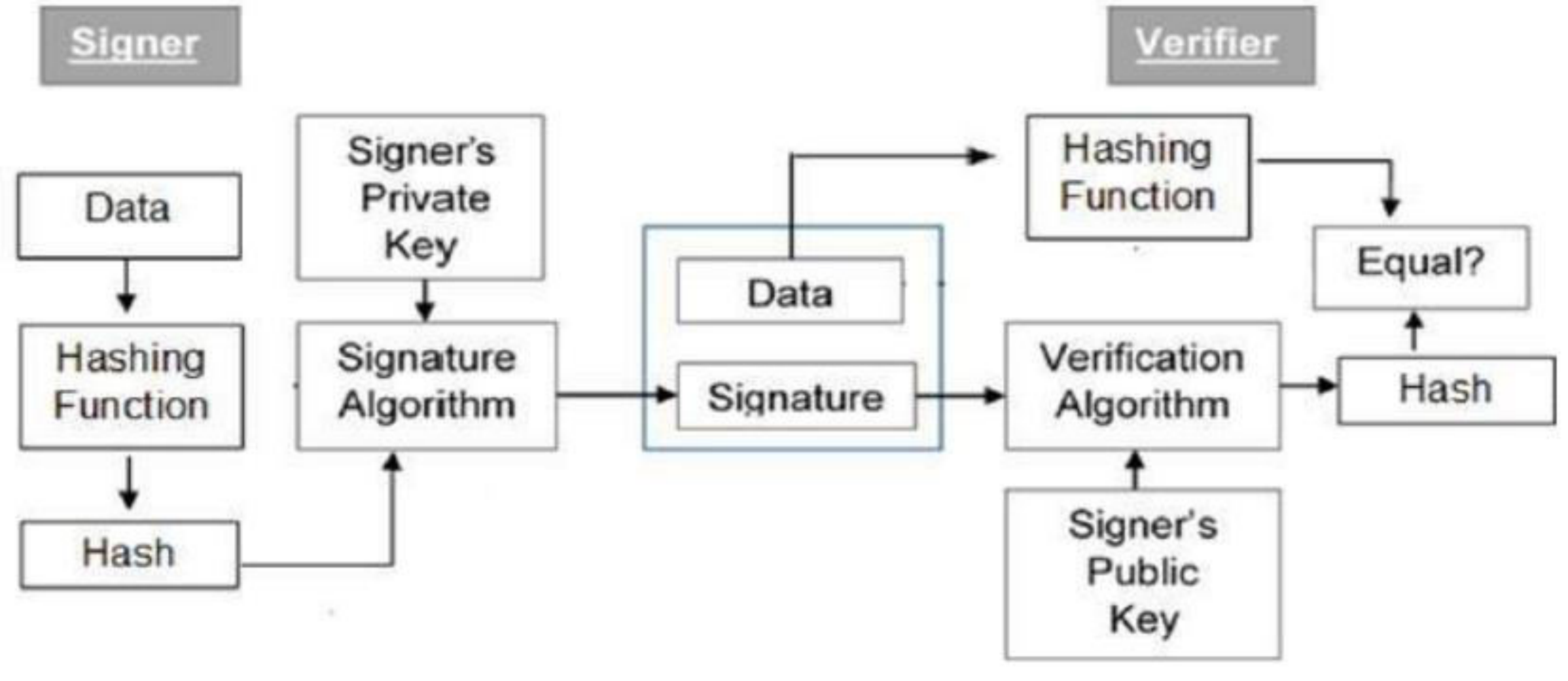
Ganesh Khatri
kh6ganesh@gmail.com

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.