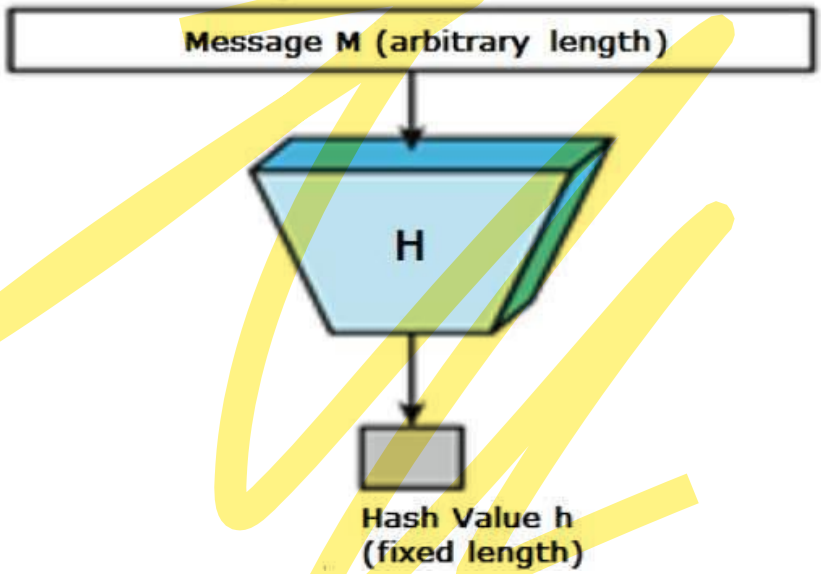
Hash Function

- 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.
- Values returned by a hash function are called **message digest** or simply **hash values**. The following picture illustrated hash function −



Features of Hash Functions

- The typical features of hash functions are −
- **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**.
  - Since a hash is a smaller representation of a larger data, it is also referred to as a **digest**.
  - Hash function with n bit output is referred to as an **n-bit hash function**. Popular hash functions generate values between 160 and 512 bits.
- **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.

• Properties of Hash Functions

- In order to be an effective cryptographic tool, the hash function is desired to possess following 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).
  - This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.

- **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.
  - Also, if a hash function is collision-resistant **then it is second pre-image resistant.**

•Popular Hash Functions

- Let us briefly see some popular hash functions −
- **Message Digest (MD)**
- MD5 was most popular and widely used hash function for quite some years.
- The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was adopted as Internet Standard RFC 1321. It is a 128-bit hash function.
- MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file. For example, file servers often provide a pre-computed MD5 checksum for the files, so that a user can compare the checksum of the downloaded file to it.
- 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.

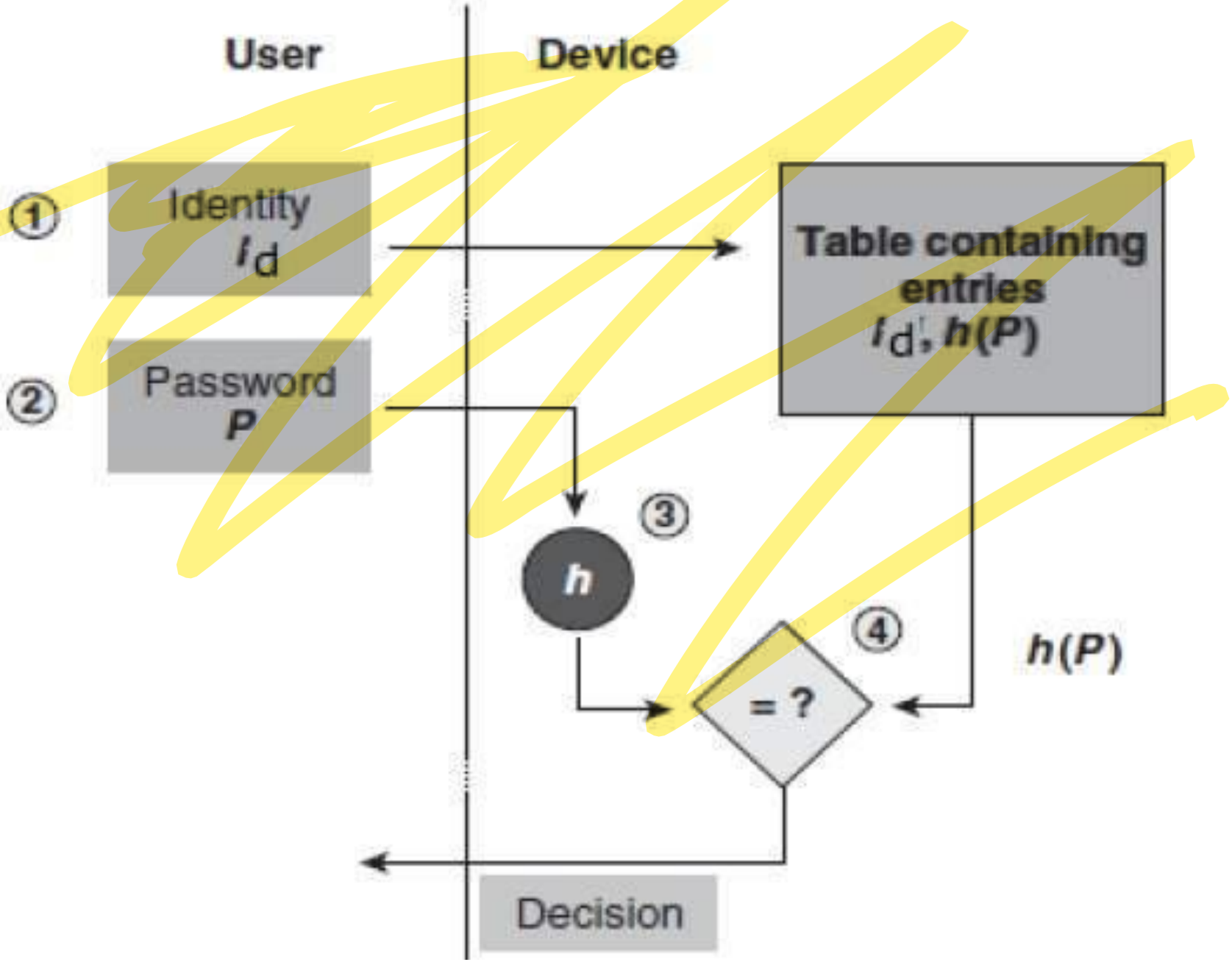
- **Secure Hash Function (SHA)**
- Family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. Though from same family, there are structurally different.
- The original version is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology (NIST) in 1993. It had few weaknesses and did not become very popular. Later in 1995, SHA-1 was designed to correct alleged weaknesses of SHA-0.
- 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.
- In 2005, a method was found for uncovering collisions for SHA-1 within practical time frame making long-term employability of SHA-1 doubtful.
- SHA-2 family has four further SHA variants, SHA-224, SHA-256, SHA-384, and SHA-512 depending up on number of bits in their hash value. No successful attacks have yet been reported on SHA-2 hash function.
- Though SHA-2 is a strong hash function. Though significantly different, its basic design is still follows design of SHA-1. Hence, NIST called for new competitive hash function designs.
- In October 2012, the NIST chose the Keccak algorithm as the new SHA-3 standard. Keccak offers many benefits, such as efficient performance and good resistance for attacks.

Applications of Hash Functions

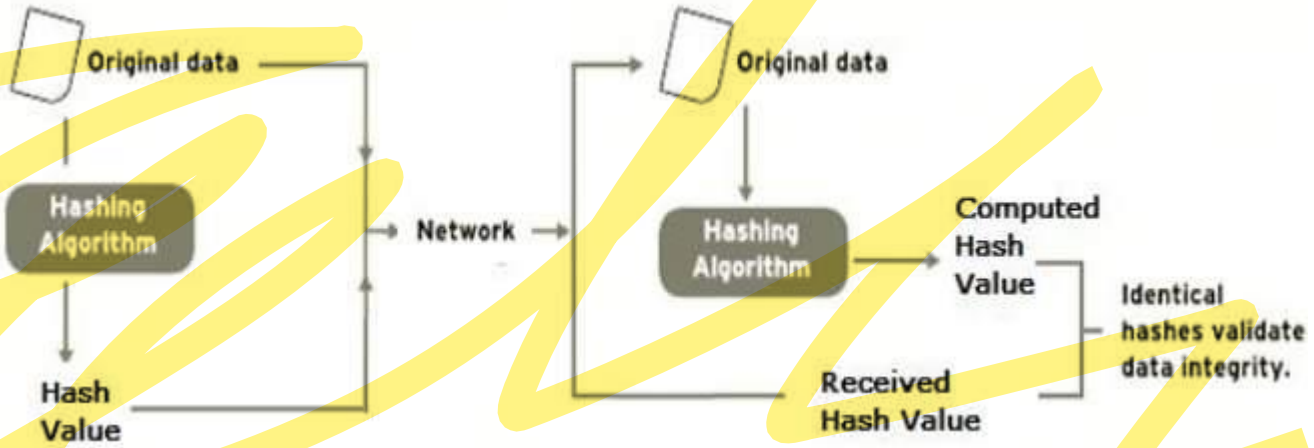
- There are two direct applications of hash function based on its cryptographic properties.

Password Storage

- Hash functions provide protection to password storage.
- Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file.
- The Password file consists of a table of pairs which are in the form (user id, h(P)).
- The process of logon is depicted in the following illustration –
- An intruder can only see the hashes of passwords, even if he accessed the password. He can neither logon using hash nor can he derive the password from hash value since hash function possesses the property of pre-image resistance.


User
Device
①
Identity
I_d
②
Password
P
Table containing entries
I_d, $h(P)$
③
h
④
= ?
$h(P)$
Decision

- **Data Integrity Check**
- Data integrity check is a most common application of the hash functions. It is used to generate the checksums on data files. This application provides assurance to the user about correctness of the data.
- The process is depicted in the following illustration –
- The integrity check helps the user to detect any changes made to original file. It however, does not provide any assurance about originality. The attacker, instead of modifying file data, can change the entire file and compute all together new hash and send to the receiver. This integrity check application is useful only if the user is sure about the originality of file.

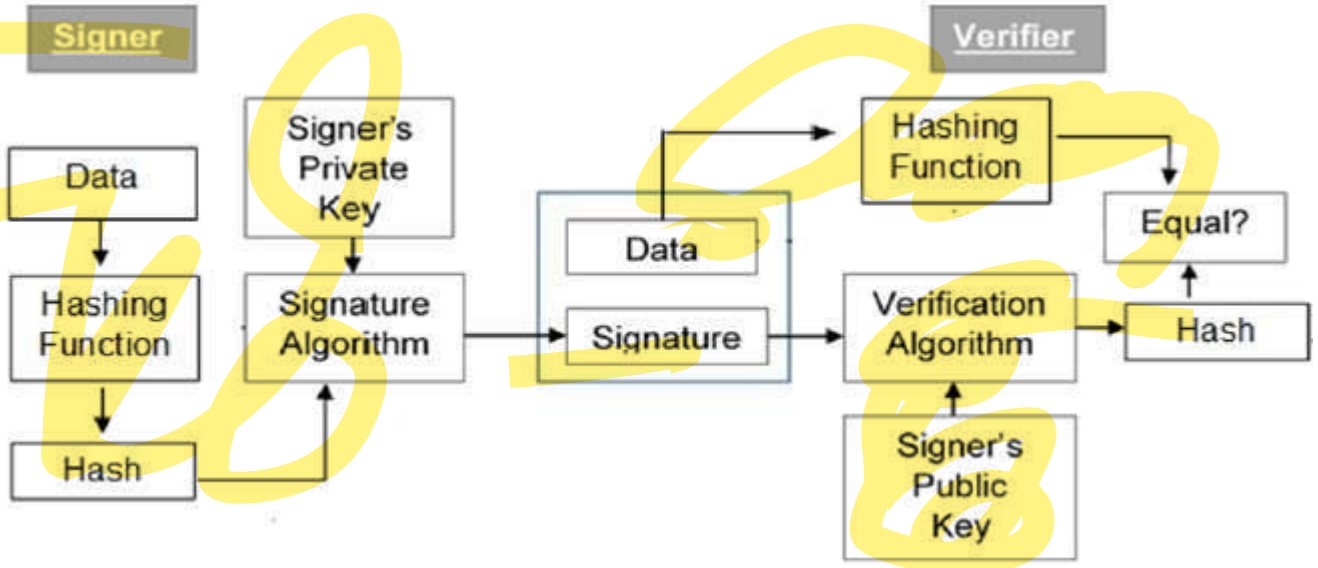


Digital Signatures

- Digital signatures are the public-key primitives of message authentication. 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.
- Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.
- In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Model of Digital Signature

- As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration −



- The following points explain the entire process in detail –
- 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.

- It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.
- Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.
- Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence **signing a hash is more efficient than signing the entire data**.

- **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.
- Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −
- **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.
- **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.

SSL/TLS

- SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details.
- The two systems can be a server and a client (for example, a shopping website and browser) or server to server (for example, an application with personal identifiable information or with payroll information).
- It does this by making sure that any data transferred between users and sites, or between two systems remain impossible to read.
- It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection. This information could be anything sensitive or personal which can include credit card numbers and other financial information, names and addresses.
- TLS (Transport Layer Security) is just an updated, more secure, version of SSL.

TLS

- **What is Transport Layer Security (TLS)?**
- Transport layer security (TLS) is another security protocol designed for privacy and data security among Internet communications. It encrypts communication between web apps and servers and is also used to encrypt email, messaging, and voice over IP (VoIP).
- It was introduced by the **Internet Technology Task Force (IETF)** of the **International Standards Organization (ISO)**, which launched the primary protocol in **1999**. In **2018**, the latest version was released and contained TLS 1.3.

SSL

- What is SSL?
- Secure Sockets Layer (SSL) is an encryption-based security protocol that ensures privacy, authentication, and data integrity in Internet communications. Its implementation is via hypertext transfer protocol secure (HTTPS) instead of the unencrypted hypertext transfer protocol (HTTP), creating a secure communication tunnel.
- **Secure Socket Layer (SSL)** is the most used internet security cryptographic protocol before the **Transport Layer Security (TLS)** was released in **1990**. However, the SSL protocol has been discontinued, but the TLS has now adopted it. Most people call it SSL. SSL provides a secure link between two devices or computers linked to the internet or the internal network.

- **The Difference Between TLS vs SSL**
- TLS is the updated version of the SSL protocol. The differences between TLS vs SSL lie in the iterations or updates to the protocols themselves. Updated versions, new features, and patches to vulnerabilities allow improved security and encryption.
- Even though TLS operates similarly to SSL, the certificate is still referred to as an SSL certificate to distinguish the encryption type from the credentials.
- The main differences between Secure Socket Layer and Transport Layer Security is that. In SSL (Secure Socket Layer), Message digest is used to create master secret and It provides the basic security services which are **Authentication** and **confidentiality**. while In TLS (Transport Layer Security), Pseudo-random function is used to create master secret.

S.NO	SSL	TLS
1.	SSL stands for Secure Socket Layer.	TLS stands for Transport Layer Security.
2.	SSL (Secure Socket Layer) supports **Fortezza** algorithm.	TLS (Transport Layer Security) does not supports **Fortezza** algorithm.
3.	SSL (Secure Socket Layer) is the 3.0 version.	TLS (Transport Layer Security) is the 1.0 version.
4.	In SSL(Secure Socket Layer), Message digest is used to create master secret.	In TLS(Transport Layer Security), Pseudo-random function is used to create master secret.

5.	In SSL(Secure Socket Layer), Message Authentication Code protocol is used.	In TLS(Transport Layer Security), Hashed Message Authentication Code protocol is used.
6.	SSL (Secure Socket Layer) is complex than TLS(Transport Layer Security).	TLS (Transport Layer Security) is simple.
7.	SSL (Secure Socket Layer) is less secured as compared to TLS(Transport Layer Security).	TLS (Transport Layer Security) provides high security.

IPSec

- The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.
- **Uses of IP Security –**
  IPsec can be used to do the following things:
- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

- **Components of IP Security –**
  It has the following components:

1. **Encapsulating Security Payload (ESP) –**
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH) –**
   It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

SSH

- SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network.
- SSH also refers to the suite of utilities that implement the SSH protocol. Secure Shell provides strong password authentication and public key authentication, as well as encrypted data communications between two computers connecting over an open network, such as the internet.
- In addition to providing strong encryption, SSH is widely used by network administrators to manage systems and applications remotely, enabling them to log in to another computer over a network, execute commands and move files from one computer to another.
- **How does SSH work?**
- Secure Shell was created to replace insecure terminal emulation or login programs, such as Telnet, rlogin (remote login) and rsh (remote shell). SSH enables the same functions -- logging in to and running terminal sessions on remote systems. SSH also replaces file transfer programs, such as File Transfer Protocol (FTP) and rcp (remote copy).

Email Security

- **Email security can be defined as the use of various techniques to keep sensitive information in email communication and accounts secure.**
- **These precautions are taken chiefly against unauthorized access, loss, or compromise. It allows an individual or an organization to protect the overall access to one or more email addresses or accounts.**
- Email security safeguards the content of an email account or service that generally serves as a popular medium for the spread of malware, spam, and phishing attacks.
- This is usually done using deceptive messages to entice recipients to divulge sensitive information, open attachments, or click on hyperlinks that install malware on the victim's device.

TOOLBOX™

BEST PRACTICES FOR EMAIL SECURITY

01

Back up critical files

02

Educate employees

03

Automate email encryption

04

Implement multifactor authentication

05

Secure the email gateway

Wireless Network Security

- Wireless network security is the process of designing, implementing and ensuring security on a wireless computer network. It is a subset of network security that adds protection for a wireless computer network.
- Wireless network security is also known as wireless security.
- Wireless network security primarily protects a wireless network from unauthorized and malicious access attempts. Typically, wireless network security is delivered through wireless devices (usually a wireless router/switch) that encrypts and secures all wireless communication by default. Even if the wireless network security is compromised, the hacker is not able to view the content of the traffic/packet in transit. Moreover, wireless intrusion detection and prevention systems also enable protection of a wireless network by alerting the wireless network administrator in case of a security breach.
- Some of the common algorithms and standards to ensure wireless network security are Wired Equivalent Policy (WEP) and Wireless Protected Access (WPA).

- **5 SOLUTIONS TO WIRELESS SECURITY THREATS**
- 1. FIREWALLS
- With a quality firewall, your company can establish a strong security foundation to prevent unidentified access and offer secure network availability for your on-site and remote staff, business partners and customers. Firewalls are a security staple in all secure networking environments, wired and wireless.
- 2. INTRUSION DETECTION
- Intrusion detection and prevention software, also found in wired and wireless networks, provides your network with the software intelligence to immediately identify and halt attacks, threats, worms, viruses and more.
- 3. CONTENT FILTERING
- Content filtering is just as important as the first two solutions in all network environments because it helps protect you from internal activity. Filtering and monitoring software prevents your employees from accessing content via the Internet that could potentially be harmful to your operations.
- 4. AUTHENTICATION
- Authentication and identification methods protect the secure data on your network. In addition to password protection, solutions such as key fobs and biometric authentication ensure that only those with proper authority to access your secure data can do so, keeping your wireless network safe.
- 5. DATA ENCRYPTION
- Today's business climate relies upon collecting, analyzing and (more importantly) sharing vital information about your business and its customers. Data encryption can be used to secure the wireless networks, Virtual Private Networks and Secure Socket Layers your data is shared on.

S/MIME

- What is S/MIME?
- S/MIME is an acronym for Secure/Multipurpose Internet Mail Extensions. It references a type of public encryption and signing of MIME data (a.k.a. email messages) to verify a sender's identity. With S/MIME, it is possible to send and receive encrypted emails.
- S/MIME is a type of "end-to-end" encryption solution used for email messages. To be more specific, it uses asymmetric cryptography to protect emails from being read by a third party.

- S/MIME provides the following cryptographic security services for electronic messaging applications:

➢ Authentication

➢ Message integrity

➢ Non-repudiation of origin (using digital signatures)

➢ Privacy

➢ Data security (using encryption)

PGP

- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation.
- PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

There are, essentially, three main uses of PGP:

- Sending and receiving encrypted emails.
- Verifying the identity of the person who has sent you this message.
- Encrypting files stored on your devices or in the cloud.

UNIT 4

Access Control

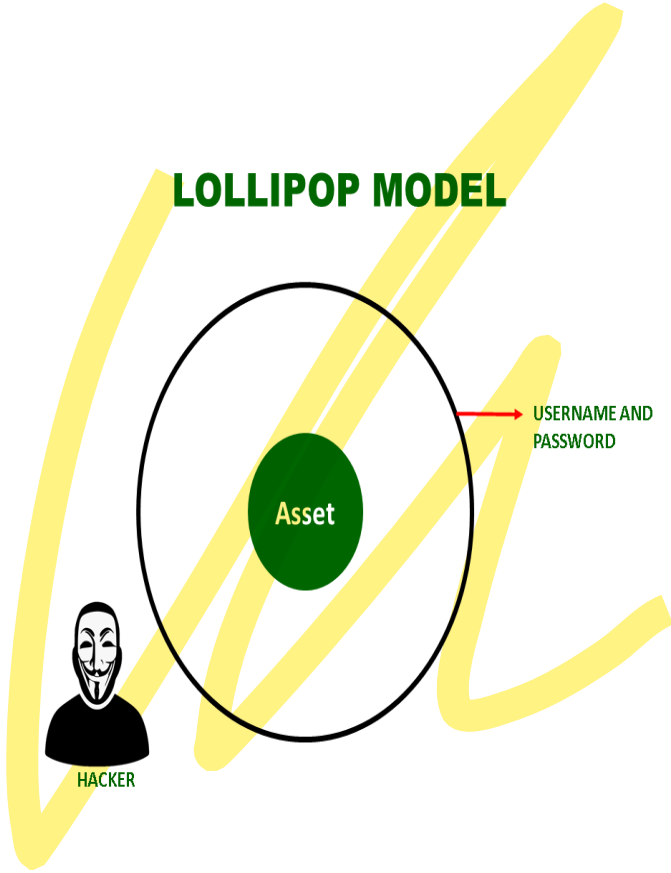
- Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data.
- At a high level, access control is a selective restriction of access to data. It consists of two main components: authentication and authorization
- Authentication is a technique used to verify that someone is who they claim to be. Authentication isn't sufficient by itself to protect data, Crowley notes. What's needed is an additional layer, authorization, which determines whether a user should be allowed to access the data or make the transaction they're attempting.
- Without authentication and authorization, there is no data security

- Access control can be split into two groups designed to improve physical security or cybersecurity:
- **Physical access control:** limits access to campuses, building and other physical assets, e.g. a proximity card to unlock a door.
- **Logical access control:** limits access to computers, networks, files and other sensitive data, e.g. a username and password.

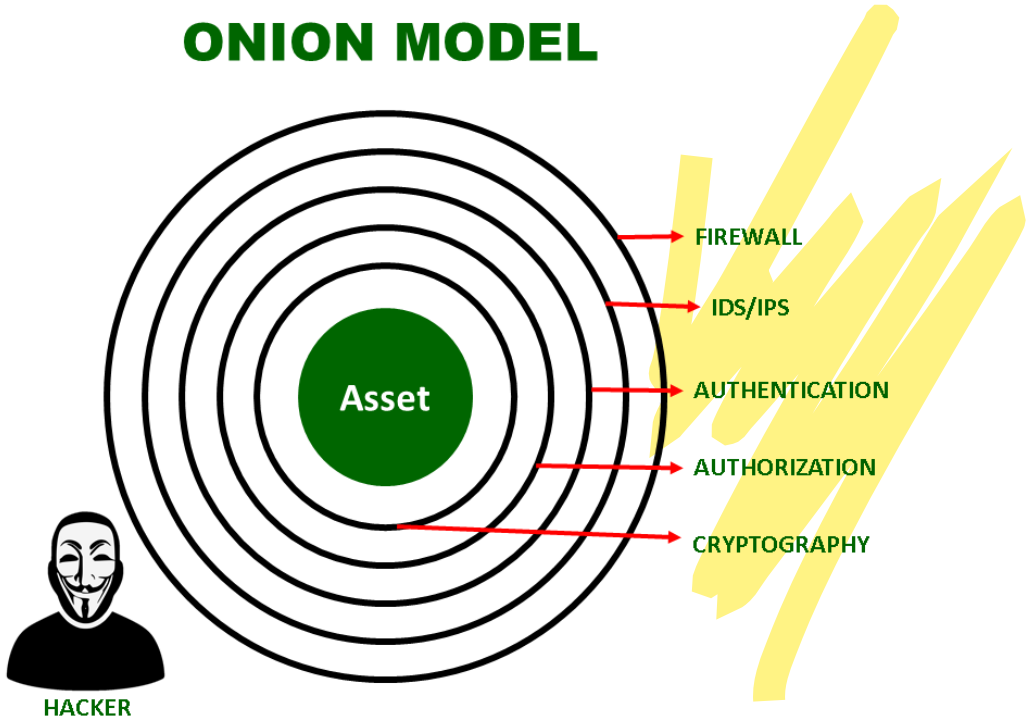
Defense Models

- These models are mainly used for Defense Purpose i.e., securing the data or the asset.
- There are 2 main types of Security Defense Models: Lollipop Model, and Onion Model. These are explained as following below.
- **1. Lollipop Model :**
  Lollipop Model is Defense Model associated with an analogy of a Lollipop. A lollipop is having a chocolate in the middle and around the chocolate, there is a layer of crust, mainly of sugar flavored syrup. A person licks and licks the lollipop and finally, the chocolate in the middle is exposed.

- Mapping this analogy of Lollipop to the Model, as shown in the above diagram, the hacker just needs to break that one layer of security to get hands on the asset, in this case, say it is Username and Password. Once it is done, the hacker can access the asset. So Lollipop Model is not a good model for Network Security.



- **2. Onion Model :**
  Onion Model is Defense Model associated with an analogy of an Onion. An Onion is a vegetable which is composed of layers. Only by peeling each layer, we can get to the center of the Onion. Also, while peeling, we get tears in our eyes.



- Mapping this analogy of Onion to the Model, as shown in the above diagram, the hacker needs to break all the layers of security to get access to the asset. Breaking each layer i.e., Firewall, IDS/IPS, Authentication, Authorisation, and Cryptography in this case, should bring tears to his eyes. In simple words, breaking each layer should be complex and extremely challenging for the hacker. So Onion Model is considered as a good model for Network Security.

Security Policies and Procedures

- A security policy is a set of standardized practices and procedures designed to protect a business's network from threat activity.
- Typically, the first part of the cybersecurity policy is focused on the general security expectations, roles, and responsibilities within the organization.
- The second part may include sections for several areas of cybersecurity, such as guidelines for antivirus software or the use of cloud applications.

- **6 examples of security policies**
- **1. Acceptable use policy (AUP)**
- An AUP is used to specify the restrictions and practices that an employee using organizational IT assets must agree to in order to access the corporate network or systems. It is a standard onboarding policy for new employees, ensuring that they have read and signed the AUP before being granted a network ID.
- **2. Data breach response policy**
- The goal of the **data breach response** policy is to describe the process of handling an incident and remediating the impact on business operations and customers. This policy typically defines staff roles and responsibilities in handling an incident, standards and metrics, incident reporting, remediation efforts, and feedback mechanisms.

- **3. Disaster recovery plan**
- A disaster recovery plan is developed as part of the larger business continuity plan, which includes both cybersecurity and IT teams' recommendations.
- **4. Business continuity plan**
- A business continuity plan (BCP) describes how the organization will operate in an emergency and coordinates efforts across the organization.
- **5. Remote access policy**
- Organizations can implement a remote access policy that outlines and defines procedures to remotely access the organization's internal networks.
- **6. Access control policy**
- An access control policy (ACP) defines the standards for user access, network access controls, and system software controls.

Firewalls

- A firewall is a **network security** device that monitors incoming and outgoing network traffic and permits or blocks data **packets** based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.
- How does a firewall work?
- Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."
- Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

- **Types of firewalls**
- Firewalls can either be software or hardware, though it's best to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between your network and gateway.
- Packet-filtering firewalls, the most common type of firewall, examine packets and prohibit them from passing through if they don't match an established security rule set. This type of firewall checks the packet's source and destination IP addresses. If packets match those of an "allowed" rule on the firewall, then it is trusted to enter the network.
- Packet-filtering firewalls are divided into two categories: stateful and stateless. Stateless firewalls examine packets independently of one another and lack context, making them easy targets for hackers. In contrast, stateful firewalls remember information about previously passed packets and are considered much more secure.

IDS

- An **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.
- Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Detection Method of IDS:

- **Signature-based Method:**
  Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.
- **Anomaly-based Method:**
  Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls:
IDS and firewall both are related to the network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it don't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

IPS

- Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.
- IPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IPS can also respond to a detected threat by attempting to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment or changing the attack's content.

- Intrusion prevention systems work by scanning all network traffic. There are a number of different threats that an IPS is designed to prevent, including:

✓Denial of Service (DoS) attack

✓Distributed Denial of Service (DDoS) attack

✓Various types of exploits

✓Worms

✓Viruses

- The IPS performs real-time packet inspection, deeply inspecting every packet that travels across the network. If any malicious or suspicious packets are detected, the IPS will carry out one of the following actions:

✓Terminate the TCP session that has been exploited and block the offending source IP address or user account from accessing any application, target hosts or other network resources unethically.

✓Reprogram or reconfigure the firewall to prevent a similar attack occurring in the future.

✓Remove or replace any malicious content that remains on the network following an attack. This is done by repackaging payloads, removing header information and removing any infected attachments from file or email servers.

- An intrusion prevention system is typically configured to use a number of different approaches to protect the network from unauthorised access. These include:
- Signature-Based - The signature-based approach uses predefined signatures of well-known network threats. When an attack is initiated that matches one of these signatures or patterns, the system takes necessary action.
- Anomaly-Based - The anomaly-based approach monitors for any abnormal or unexpected behavior on the network. If an anomaly is detected, the system blocks access to the target host immediately.
- Policy-Based - This approach requires administrators to configure security policies according to organizational security policies and the network infrastructure. When an activity occurs that violates a security policy, an alert is triggered and sent to the system administrators.

Log Files

- Log files record and track computing events. Log files are extremely valuable in computing as they provide a way for system admins to track the operation of the system in order to spot problems and make corrections.
- Why is logging important?
- Log files (also known as machine data) are important data points for security and surveillance, providing a full history of events over time. Beyond operating systems, log files are found in applications, web browsers, hardware, and even email.
- With proper log file tracking, businesses can either avoid or quickly rectify errors within their operating systems. Smart log tracking reduces downtime and minimizes the risk of lost data. Log data is typically sent to a secure host that acts as a common collection point before further processing by system admins.
- Server log files are raw data points that can be useful in a variety of ways. For example, on a web browser, log files can contain valuable information about user sessions, individual users, rendering times, and keyword data.
- In another way, log files are a trusted source of audit information by security professionals as they contain a full history of system activity such as access attempts, command line data, changes to sensitive information and more.

Honey Pots

- A honeypot is a computer or computer system intended to mimic likely targets of cyberattacks. It can be used to detect attacks or deflect them from a legitimate target. It can also be used to gain information about how cybercriminals operate.
- The principle behind them is simple: Don’t go looking for attackers. Prepare something that would attract their interest — the honeypot — and then wait for the attackers to show up.
- Like mice to cheese-baited mousetraps, cybercriminals are attracted to honeypots — not because they’re honeypots. The bad guys think the honeypot is a legitimate target, something worthy of their time. That’s because the bait includes applications and data that simulate a real computer system

How do honeypots work?

- If you, for instance, were in charge of IT security for a bank, you might set up a honeypot system that, to outsiders, looks like the bank's network. The same goes for those in charge of — or researching — other types of secure, internet-connected systems.
- By monitoring traffic to such systems, you can better understand where cybercriminals are coming from, how they operate, and what they want. More importantly, you can determine which security measures you have in place are working — and which ones may need improvement.

Honeypot example

- In 2015, internet security experts set up an online railway control system as honeypot bait. The goal was to study how criminals would attack projects where they could put the public at risk. In this case, the only damage done was to a model train set at a German technology conference. Over two weeks, the so-called "HoneyTrain" suffered 2.7 million attacks.

What could be at stake?

- Stealing personal information from online targets is one thing. Targeting public transportation systems is another. Beyond the IoT devices and the HoneyTrain, researchers have used honeypots to expose vulnerabilities with medical devices, gas stations, industrial control systems used for such things as electrical power grids, and more.
- Given all the attention that the bad guys get for their hacking and data breach efforts, it's good to know that the good guys have a few tricks up their sleeves to help protect against cyberattacks.
- As more and more devices and systems become internet-connected, the importance of battling back against those who use the internet as a weapon will only increase. Honeypots can help.

Network Admission Control

- NAC is a fantastic tool that makes sure all devices connecting to your network infrastructure are up to date. Imagine a scenario an employee goes on holiday, two weeks later, the same user goes back to work and connects their laptop into the network. Antivirus, OS updates, and Application updates will be out of date. NAC will make sure all updates are done before the user can take full advantage of the network. Up to date devices is less likely to be a victim of cyber-attack.
- **Network Admission Control (NAC)** solutions allow you to authenticate wired, wireless, and VPN users and devices to the network; evaluate and remediate a device for policy compliance before permitting access to the system; differentiate access based on roles, and then audit and report on who is on the network.

- **Features and Benefits**
- Prevents unauthorised network access to protect your information assets
- Helps proactively mitigate network threats such as viruses, worms, and spyware
- Addresses vulnerabilities on user machines through periodic evaluation and remediation
- Brings you significant cost savings by automatically tracking, repairing, and updating client machines
- Recognises and categorises users and their devices before malicious code can cause damage
- Evaluates security policy compliance based on user type, device type, and operating system
- Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention
- Applies posture assessment and remediation services to a variety of devices, operating systems, and device access methods including LAN, WLAN, WAN, and VPN
- Enforces policies for all operating scenarios without requiring separate products or additional modules
- Supports seamless single sign-on through an agent with automated remediation
- Provides clientless web authentication for guest users

Electronic Voting

- **electronic voting**, a form of computer-mediated voting in which voters make their selections with the aid of a computer. The voter usually chooses with the aid of a touch-screen display, although audio interfaces can be made available for voters with visual disabilities.
- To understand electronic voting, it is convenient to consider four basic steps in an election process: ballot composition, in which voters make choices; ballot casting, in which voters submit their ballots; ballot recording, in which a system records the submitted ballots; and tabulation, in which votes are counted.
- Ballot casting, recording, and tabulation are routinely done with computers even in voting systems that are not, strictly speaking, electronic.
- Electronic voting in the strict sense is a system where the first step, ballot composition (or choosing), is done with the aid of a computer.
- There are two quite different types of electronic voting technologies: those that use the Internet (I-voting) and those that do not (e-voting).

- Electronic voting and counting refers to the use of electronic technologies that assist or automate the voting and/or counting processes.
- In electronic voting, often called "e-voting," voters use an electronic device to make and record their ballot choices. Choices are recorded on the machine itself or the machine produces a token on which the choices are recorded, such as a magnetic card or a printout of the ballot choice. Electronic voting systems include electronic voting machines (EVMs) placed in polling stations, SMS voting and Internet voting.
- In electronic counting, part or all of the tabulation of results is automated. E-voting systems can be **remote** or **non-remote**, referring to whether the voters' ballot choices are transmitted to a central location (e.g. Internet or SMS voting) or recorded on a local medium (such as the EVM or a printed ballot).
- Systems will also be **supervised** or **unsupervised**, which relates to whether election staff are present to manage the voting process (e.g., if voting is done in a polling station) or not (such as Internet voting).
- The most common e-voting systems involve non-remote EVMs used in the supervised environment of the polling station. There are many key decisions that must be reached in adopting, designing, implementing and overseeing an e-voting system.

Security Awareness Training

- Security awareness training is a strategy used by IT and security professionals to prevent and mitigate user risk. These programs are designed to help users and employees understand the role they play in helping to combat information security breaches.
- Effective security awareness training helps employees understand proper cyber hygiene, the security risks associated with their actions and to identify cyber attacks they may encounter via email and the web.
- Research suggests that human error is involved in more than 90% of security breaches.
- Security awareness training helps to minimize risk thus preventing the loss of PII, IP, money or brand reputation.
- An effective awareness training program addresses the cybersecurity mistakes that employees may make when using email, the web and in the physical world such as tailgaiting or improper document disposal.

- Effective security awareness training focuses on engaging today's workforce to reduce user risk.
- Many security awareness training programs ignore education best practices, delivering training in one-off sessions that overwhelm users with information or worse, are forgettable.
- For training to stick, it needs to be persistent, delivered regularly in small doses, to fit employees' busy schedules.
- Most importantly, positive reinforcement and humor performs better than fear-based or boring messaging to improve retention of critical security topics.

Email and Internet use policies

- A computer and email usage policy, also known as an **internet usage policy**, is a document that you should ideally give to each employee upon hiring. Prospective employees should read the policy, sign it, and date it before they start work.
- You'll need to create a company computer, email, and internet use policy before you hire new employees. If you have a legal department, it can prepare this document for you; if not, you can work with an online provider or other professional to prepare one.
- How your employees will use the internet is an important decision for your company because there are many situations that will affect your business if there's no stated policy. Your written policy must take into account what type of business you have and whether internet and computer use is a significant part of the employee's job. If you have a marketing company, your employees may be actively promoting your business on all types of social media. You want to make sure your employees aren't texting, tweeting, or emailing friends and family, or downloading prohibited material, during working hours.

- An internet and email usage policy in the workplace usually states that your employees shouldn't expect anything they create on their business computers to be private, and that such data belongs to the company.
- Even though each state has different laws, many states allow companies to monitor employees' data, emails, downloads, and what the employees are doing on the computers. The written policy should specify what's allowed and what's prohibited, even if it appears to be common sense.
- While each company's internet usage policy is different, many contain similar clauses so that employees know in advance that they:
- Will be subject to monitoring, which could occur at any time
- Cannot download pornographic, sexual, or questionable content, nor may they send such material by email or other social media
- Cannot disparage the company, supervisors, or coworkers, but must promote the company in a professional manner
- Shall encrypt certain material to protect security, as further explained by the employer or IT department
- Cannot send emails or post on social media in a way that discriminates or ridicules anyone in any manner, including using language or other content that disparages groups based on age, race, color, religion, gender, sexual orientation, national origin, disability, weight, physical appearance, or other protected group

- Cannot harass, threaten, sexually harass, or send offensive, vulgar, or obscene material on company computers
- Are not allowed to use company computers for playing video or other games
- Cannot communicate company secrets—or confidential and privileged information—to anyone unless authorized to do so
- Cannot send emails to hundreds of addresses at once, which constitutes spam
- May not receive email or newsletters from private companies for personal use, personal causes, or purchases unrelated to company business
- Cannot download software, including music, without consulting the supervisor or IT department, so that spyware and viruses aren't transferred to the computer or network
- Cannot commit piracy, violate copyrights, discuss religion or politics, commit defamation, or use the internet for any unlawful purposes
- Cannot transmit chain letters, hate or incendiary mail, videos, or memes
- Will be denied access to company computers, and may be subject to disciplinary action or dismissal, if they do any of the above

Risk Management

- Cyber threats are constantly evolving. The most effective way to protect your organisation against cyber attacks is to adopt a risk-based approach to cyber security, where you regularly review your risks and whether your current measures are appropriate.
- A risk-based approach means the cyber security measures you implement are based on your organisation's unique risk profile, so you will not waste time, effort or expense addressing unlikely or irrelevant threats.

- Cyber risk management is the process of identifying, analysing, evaluating and addressing your organisation's cyber security threats.
- The first part of any cyber risk management programme is a cyber risk assessment. This will give you a snapshot of the threats that might compromise your organisation's cyber security and how severe they are.
- Based on your organisation's risk appetite, your cyber risk management programme then determines how to prioritise and respond to those risks.

A risk management programme typically follows these steps:

- Identify the risks that might compromise your cyber security. This usually involves identifying cyber security vulnerabilities in your system and the threats that might exploit them.
- Analyse the severity of each risk by assessing how likely it is to occur, and how significant the impact might be if it does.
- Evaluate how each risk fits within your risk appetite (your predetermined level of acceptable risk).
- Prioritise the risks.
- Decide how to respond to each risk. There are generally four options:
  - Treat – modify the likelihood and/or impact of the risk, typically by implementing security controls.
  - Tolerate – make an active decision to retain the risk (e.g. because it falls within the established risk acceptance criteria).
  - Terminate – avoid the risk entirely by ending or completely changing the activity causing the risk.
  - Transfer – share the risk with another party, usually by outsourcing or taking out insurance.
- Since cyber risk management is a continual process, monitor your risks to make sure they are still acceptable, review your controls to make sure they are still fit for purpose, and make changes as required. Remember that your risks are continually changing as the cyber threat landscape evolves, and your systems and activities change.

Copyright

- What Is Copyright?
- Copyright refers to the legal right of the owner of intellectual property. In simpler terms, copyright is the right to copy. This means that the original creators of products and anyone they give authorization to are the only ones with the exclusive right to reproduce the work.
- Copyright law protects creators of original material from unauthorized duplication or use.
- For an original work to be protected by copyright laws, it has to be in tangible form.
- In the U.S., the work of creators is protected by copyright laws until 70 years after their death.

- The primary objective of copyright is to induce and reward authors, through the provision of property rights, to create new works and to make those works available to the public to enjoy.
- The theory is that, by granting certain exclusive rights to creators, which allow them to protect their creative works against theft, they receive the benefit of economic rewards and the public receives the benefit of the creative works that might not otherwise be created or disseminated.
- **How Copyrighting Works**
- When someone creates a product that is viewed as original and that required significant mental activity to create, this product becomes an intellectual property that must be protected from unauthorized duplication.
- Examples of unique creations include computer software, art, poetry, graphic designs, musical lyrics and compositions, novels, film, original architectural designs, website content, etc. One safeguard that can be used to legally protect an original creation is copyright.

Software Licences

- What Is a Software License?
- A software license is a contract between the entity that created and supplied an application, underlying source code, or related product and its end user. The license is a text document designed to protect the intellectual property of the software developer and to limit any claims against them that may arise from its use.
- A software license also provides legally binding definitions for the distribution and use of the software. End-user rights, such as installation, warranties, and liabilities, are also often spelled out in the software license, including protection of the developer's intellectual property.
- Most software falls under one of two categories that have distinct differences in how they are viewed under copyright law:
- Proprietary – also referred to as "closed source"
- Free and open-source software (FOSS) – referred to as "open source"

- FOSS software licenses – give rights to the customer that include modification and reuse of the software code, providing the actual source code with the software product(s). This open-source type of licensing affords the user authority to modify the software functions and freedom to inspect the software code.
- Proprietary software licenses – provide no such authority for code modification or reuse and normally provide software with operational code only, and no source code. A proprietary software license often includes terms that prohibit "reverse engineering" of the object code with the intention of obtaining source code by the licensee.
- In both cases, the software license will most often specify limitations of liability from use of the software product, any mutual responsibilities such as support, and any warranties or disclaimer of warranty.
- Where software is not covered by any license, it is normally categorized as:
- Public domain software – freely available for use and not copyright protected
- Private unlicensed software – such as business applications that still falls under copyright protection

- Open source and proprietary software licensing may also specify additional restrictions and terms:

✓Transfer of ownership to the buyer or retention of ownership by the seller

✓Any authorization for copying, selling, or distributing the software

✓Definition of whether the license constitutes purchase or leasing of the software

IPR

- Intellectual property (IP) is a term referring to a brand, invention, design or other kind of creation, which a person or business has legal rights over. Almost all businesses own some form of IP, which could be a business asset.
- Common types of IP include:

➢ Copyright – this protects written or published works such as books, songs, films, web content and artistic works;

➢ Patents – this protects commercial inventions, for example, a new business product or process;

➢ Designs – this protects designs, such as drawings or computer models;

➢ Trade marks – this protects signs, symbols, logos, words or sounds that distinguish your products and services from those of your competitors.

- IP can be either registered or unregistered. With unregistered IP, you automatically have legal rights over your creation. Unregistered forms of IP include copyright, unregistered design rights, common law trade marks and database rights, confidential information and trade secrets. With registered IP, you will have to apply to an authority, such as the Intellectual Property Office in the UK, to have your rights recognised. If you do not do this, others are free to exploit your creations. Registered forms of IP include patents, registered trade marks and registered design rights. Copyright is also registerable.
- intellectual property rights are a common type of legal IP protection for those who create. These rights, however, have actually contributed enormously to the world, in particular economically.
- Many companies in a variety of industries rely on the enforcement of their patents, trademarks, and copyrights, while consumers can also be assured of quality when they purchasing IP-backed products.

- The purpose of intellectual property rights is to encourage new creations, including technology, artwork, and inventions, that might increase economic growth. Intellectual property rights increase the incentives for individuals to continue to produce things that further create job opportunities and new technologies, while enabling our world to improve and evolve even faster.
- Intellectual property rights are legal rights that provide creators protection for original works, inventions, or the appearance of products, artistic works, scientific developments, and so on.
- There are four types of intellectual property rights (IP): patents, trademarks, copyrights, and trade secrets.

Types of Intellectual Property Rights

- Patent
- A patent is used to prevent an invention from being created, sold, or used by another party without permission. Patents are the most common type of intellectual property rights that come to people's minds when they think of intellectual property rights protection. A Patent Owner has every right to commercialize his/her/its patent, including buying and selling the patent or granting a license to the invention to any third party under mutually agreed terms.

- Trademarks are another familiar type of intellectual property rights protection. A trademark is a distinctive sign which allows consumers to easily identify the particular goods or services that a company provides. Some examples include McDonald's golden arch, the Facebook logo, and so on. A trademark can come in the form of text, a phrase, symbol, sound, smell, and/or color scheme. Unlike patents, a trademark can protect a set or class of products or services, instead of just one product or process.

Copyright

- Copyright does not protect ideas. Rather, it only covers "tangible" forms of creations and original work–for example, art, music, architectural drawings, or even software codes. The copyright owner has the exclusive right to sell, publish, and/or reproduce any literary, musical, dramatic, artistic, or architectural work created by the author.

Trade Secret

- Trade secrets are the secrets of a business. They are proprietary systems, formulas, strategies, or other information that is confidential and is not meant for unauthorized commercial use by others. This is a critical form of protection that can help businesses to gain a competitive advantage.