**Revision**

**Topic 1**

**Four criteria that necessary for an encryption scheme to be considered computationally secure.**

Confidentiality: Unauthorized parties shouldn't be able to read the ciphertext's plaintext due to the encryption scheme.

Integrity: This scheme should make sure that any ciphertext alteration is detectable.

Authentication: In order to make sure that the sender and the recipient are who they claim they are, the scheme should verify the identities of the parties involved in the communication.

Non-repudiation: Sender denials of message transmission should be prevented by the scheme. This makes sure that the sender cannot pretend that they never sent the communication, which is important in situations where auditability and accountability are required.

**What is hash function**

A hash function is a mathematical function that converts a large, possibly variable amount of data to a single, small item. To ensure the integrity of the file, the contents might be bound together through hashing.

**Cryptography hashing function common example**

MD5 and SHA1

SHA-224, SHA-256, SHA-512, KECCAK-256, Whirlpool

**Symmetric and Asymmetric**

The same key is used for both encryption and decryption in symmetric encryption.

Much faster encryption is symmetric encryption.

Asymmetric

A public key is used for encryption in asymmetric encryption, and a separate private key is used for decryption.

One key cannot be derived from the other in asymmetric encryption.

The private key does not need to be distributed when using asymmetric encryption.

**Symmetric and asymmetric picture**

**Topic 2**

**Digital Certificate**

A digital document that binds the identity that the Certification Authority (CA) is ready to certify with your public key.

**Digital Certificate Usage**

A digital certificate issued by one of the public CAs will contain information in the key usage field of the certificate.

This means that the private key may be used for specific purposes such as:

* digital signatures
* certificate signing
* encipher or decipher only
* key encipherment
* data encipherment

**Certificate Standards**

The data in a certificate usually conforms to the ITU (IETF) standard X.509.

Includes information about:

* the identity of the owner of the corresponding private key
* the length of the key
* the algorithm used by the key
* the associated hashing algorithm
* dates of validity of the certificate
* the actions that the key can be used for

**Two (2) common methods that can be used to generates digital certificates.**

Certification Authority (CA)

Self-signed certificates.

**Topic 3**

**What is IPsec**

Provides IP-layer security services to other TCP/IP protocols and applications to use.

Provides devices connected to a TCP/IP network a way to safely communicate with one another.

In order for two devices to communicate safely, they create a safe path that can pass over numerous insecure intermediary systems.

**IPsec Applications**

Securing a company’s Virtual Private Network (VPN) over the Internet

Securing remote access over the internet.

Establishing connections with partners via an extranet.

Enhancing eCommerce security by adding to the security mechanism in the application layer.

**HTTP and HTTPS major different**

**HTTP**

Data is not encrypted.

URL begins with http://

Typically uses port 80 for communication.

Since the data is not encrypted, it can be modified during transmission without detection.

**HTTPS**

Data is encrypted using SSL/TLS

URL begins with https//:

Typically uses port 443 for communication.

Provides data integrity by ensuring that the data cannot be altered during transmission without being detected.

**How to see browser uses protocol**

**Topic 4**

**Use or used of cryptography in email communication**

Cryptography can be used in email to:

To sign an email in order to verify the sender's integrity and ensure the message's integrity.

To protect the confidentiality of an email message by encrypting its body.

To encrypt mail server communications in order to protect the confidentiality of the message header and body.

**Threat of email**

Viruses

Viruses are very sophisticated and often appear to be harmless correspondence.

Spam

Phishing

Spyware

**Potential drawbacks of email**

Email could potentially cause information overload.

Email lacks a personal touch.

Email can be disruptive.

Email cannot be ignored for a long time.

Email can cause misunderstandings.

Email messages can contain viruses.

**Describe 3 methods that a hacker can use to obtain or crack a weak password.**

Dictionary Attack

Brute Force Attack

Phishing

**Describes two (2) methods that an organization can use to identify existing security vulnerabilities in its network.**

Vulnerability Scanning

Penetration Testing

**What data is of interest?**

Payment Systems

Research and development information

Where a company is trying to develop things that require patents or copyright.

Software that can be downloaded for free rather than paid for.

Commercially sensitive information, such as salary details, marketing plans, etc…

Information about individuals.

**Protecting your data**

Back up data: allows for data recovery in the event that data is deleted or corrupted.

Have strong access control mechanisms.

Password protect documents.

Encrypt files.

Encrypt disks.

**Security Vulnerability**

A security vulnerability is a flaw or weakness in a network or system that makes it possible for an attack to negatively impact the network or system, including:

* enabling unauthorized access to a network or system
* causing the system's or network's performance to decrease
* destroying or changing data stored on a network or system

It's possible that the system is inherently vulnerable.

For example, even when installed and used properly, new software has a vulnerability when it is deployed.

The implementation of a system could be the cause of the vulnerability.

For example, setting up new software

The vulnerability could arise from how a system is run and maintained.

For example, Bad security protocols

**Causes**

Software-flaws in new software, not tested sufficiently before deployment

Hardware - dust

Organization procedures - poor password policy, lack of audits

Personnel - not training staff properly

Physical environment - no physical access controls, risks from flooding

Combinations of the above

**Complex System**

Large companies typically have large and complex computer networks.

Security flaws are more likely to exist in larger systems.

Security flaws are more likely to exist in complicated systems.

Large, complex networks require a great deal of effort and time to thoroughly test.

**Common Components**

Modern networks will use common components:

Software used by many others (sometimes open-source)

Hardware used by many others

Operating systems used by many others

Attackers will have access to these components and be familiar with any security flaws they have.

The Internet rapidly spreads the knowledge of these flaws and increases the likelihood of them being quickly exploited

**Verifying user identity**

User authentication has two steps:

Identification: introducing the user to the security system.

Verification: supplying data that connects the object and the identification.

The process through which a user claims their identity is known as identification.

The method used for verifying such claim is verification.

**Biometric**

Automated methods used to recognize the unique characteristics of humans.

Physical traits and behavioral traits

The aim of biometric authentication is to provide a non-transferable form of authentication.

Someone else could use your ATM card.

Can Someone else use your finger?

Example

Physical characteristics:

Fingerprint

Retinas

Irises

Facial patterns

Hand measurements

Behavioral characteristics

Signature

Typing patterns

Voice recognition

**Stateful filtering**

Also know as dynamic packer filtering.

Uses a stable table that stores detail of legitimate traffic requests:

IP address

Ports

Handshake status

Route/time

Compare packets with previous valid traffic.

Allows traffic based upon connections.

**Network Address Translation**

NAT provides a way to use a single IP address to connect multiple computers to an IP networking.

There reasons this useful

Shortage of IP address

Security

Flexible network administration.

**Different between Hardware firewall and software firewall.**

Usually found in routers, which distribute incoming data from an Internet connection to computers, are hardware firewalls.

Software firewalls are installed on each individual computer.

**What is VPN**

A private network that communicates through open communication channels like the Internet rather than leased lines.

Internet-based remote network communication.

Used by businesses or organizations wanting quiet communication.

• Two parts:

Protected or "inside" network

"Outside" network or segment (less trustworthy)

**SSL VPNs**

Connect securely via a standard Web browser

No special software required on client computers

Traffic between Web browser and the SSL VPN device is encrypted with the SSL protocol

Support access control by:

User

Device

Location

**SSL VPN 2 main types**

SSL tunnel VPN and Portal VPN

**WEP weakness**

There is a 50% chance that the same IV will repeat after 5000 packets as the 24 bit IV is too short and repeats after some time.

Replaying packets allows the access point to broadcast Ivs.

In a few of minutes at most, WEP can be packetized with the right hardware.