CSE 4215: Network Security

Riyad Morshed Shoeb
2022

Introduction

What is Network security?

Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources[a].

[a] https://en.wikipedia.org/wiki/Network_security

What is Policy?

A Policy is a written document with a set of guidelines and principles that will be followed by an employee of an organization. It helps to take a decision.

What is Security Policy?

A security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, and how to handle situations when they do occur. A security policy must identify all of a company's assets as well as all the potential threats to those assets. Company employees need to be kept updated on the company's security policies. The policies should be updated regularly as well.

Network Security Policies, Strategies and Guidelines

Acceptable Use Policy (AUP) specifies the constraints and practices that an employee using organizational IT assets must agree to in order to access the corporate network or the internet. Examples: Which site can I visit? Can I use my ID to use other staff? Can I print my own doc?

Access Control Policy (ACP) outlines the access available to employees in regards to an organization's data and information systems. Other items covered in this policy are standards for user access, network access controls, operating system software controls, and the complexity of corporate systems passwords. Additional supplementary items often outlined include methods for monitoring how corporate systems are accessed and used, how unattended workstations are secured, and how access is removed when an employee leaves the organization. Examples: Only admin can enter the server room. A faculty can access the data of students. A student access a certain level of data.

Change Management Policy (CMP) refers to a formal process for making changes to IT, software development and security services/operations. The goal of a change management program is to increase the awareness and understanding of proposed changes across an organization, and to ensure that all changes are conducted methodically to minimize any adverse impact on services and customers. Example: Who can change what? Who is responsible for upgrading the software?

Information Security Policy (ISP) is a set of rules and guidelines that dictate how IT assets and resources should be used, managed, and protected.

Incident Response Policy (IRP) is an organized approach to how the company will manage an incident and remediate the impact to operations. The goal of this policy is to describe the process of handling an incident with respect to limiting the damage to business operations, customers and reducing recovery time and costs. Example: Handle Cyber Attack.

Remote Access Policy (RAP) is a document which outlines and defines acceptable methods of remotely connecting to an organization's internal networks. Example: Who should be given remote access? What information can be accessed remotely?

Email/Communication Policy (ECP) is a document that is used to formally outline how employees can use the business' chosen electronic communication medium. The primary goal of this policy is to provide guidelines to employees on what is considered the acceptable and unacceptable use of any corporate communication technology. An **email security policy** is an official company's document that details acceptable use of your organization's email system. It indicates to whom and from whom emails can be sent or received and defines what constitutes appropriate content for work emails.

Protect the organization from liabilities: When all employees read and sign an email policy, it proves they are aware and agree to the information contained in that policy. Should an email be sent that is not considered appropriate content according to the email policy, the employee, not the business, would bear the brunt of liability for any damages or suits brought as a result of their sending an inappropriate email.

Promote a professional environment: If email is used only in a professional manner in the workplace, you can be sure that embarrassing mistakes will not occur. For example, if staff are using work email to communicate with friends, the content in those emails are likely to be sloppy, unprofessional, and informal. If those emails accidentally get sent to clients or other professionals, the company image may become damaged. If an email policy does not allow for personal use of the work email system, your staff will remain in a professional mindset and eliminate the potential of personal emails going out to customers.

Increase productivity: Email tends to be a distraction for employees who are using it for non-professional reasons. If an email policy prohibits the use of work email for personal use, your employees will stay on task more and avoid the distractions that come from sending and receiving personal emails during work hours.

Establish systems for email: If the email policy outlines appropriate content for an email sent during work hours over the company email system, it can also help establish systems to ensure all staff members are contributing to the brand or image of the company. Have each staff member use a template for email responses and set up signature lines that appear in all outgoing emails to further establish the company's professionalism and image in the eyes of individuals who may receive email from your staff. Setting guidelines for content and use of email creates a single, comprehensive image of the company that helps keep the organization aligned with its mission.

Disaster Recovery Policy/Plan (DRP) generally includes both cyber-security and IT teams' input and is developed as part of the larger business continuity plan. The CISO (chief information security officer) and teams will manage an incident through the incident response policy. If the event has a significant business impact, the Business Continuity Plan will be activated. Example: Continue the business if one branch goes down due to disaster using other branch.

Business Continuity Policy (BCP) coordinates efforts across the organization and uses the disaster recovery plan to restore hardware, applications and data deemed essential for business continuity. BCP's are unique to each business because they describe how the organization will operate in an emergency. Example: Fire in one branch but still continue the business using other options.

Network Security Assessments and Matrices

Risk Assessment is a systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking.

$$Risk = Likelihood \times Consequence = Probability \times Severability$$

Vulnerability A weakness that can be exploited.

Threat one who exploits a vulnerability.

Risk damage caused by exploiting

Asset which needs to be accessed

Bug error, fault or flaw in computer

Hacker Gains access with or without

Cracker gains access to damage assets.

Risk Assessments Elements

Risk Identify To identify risk we need the know assets (*e.g.* Hardware, software, people), threats (*e.g.* virus, experts leaving job, disaster, fire), vulnerability (*e.g.* No anti-virus, No fire extinguisher).

Risk Owner Who is responsible for what risk *e.g.* the software risk owner might be the admin.

Risk Assessment

- Determine the impact of risk
- Determine likelihood of risk

Table 1: Data for Risk Assessment Table

Asset	Owner	Threat	Vulnerability	Impact	Likelihood	Risk
Server	Admin	Electricity failure	No UPS/IPS	4	1	4
Contract	MD	Unauthorized access	It is in table	4	4	16

Network Security Threats and Attackers

Threats and Attackers

Intruders are the attackers who attempt to breach the security of a network. They attack the network in order to get unauthorized access.

Malicious Software, in short Malware, is computer programs designed to infiltrate and damage computers without the users consent. It is the general term covering all the different types of threats to your computer safety such as viruses, spyware, worms, trojans, rootkits and so on. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission. Types of Malware:

Virus (Vital Information Resources Under Seize) is a type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be **infected** with a computer virus. Affected files are document or text files, image files, videos files, audio files etc.

Worms are malicious, self-replicating program that can spread throughout a network without human assistance. It comes from downloading, internet surfing, email etc. Worms consume large volumes of memory, as well as bandwidth. This results in servers, individual systems, and networks getting overloaded and malfunctioning. To protect a computer against worm, making sure that the computer has all the latest updates installed is the best defence.

Trojan Horse or Trojan, is a type of malicious code or software that looks legitimate but can take control of a computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on the data or network. When you install a fake software, then Trojan horse can be installed. Probable symptom of Trojan virus are system errors, strange pop-ups, slow computer, strange behavior etc. How harmful Trojan virus is:

- Steal confidential files
- Steal pin/password
- Illicit Activities using hacked machine (as a result, hacked user can get arrested)

How to Remove Trojan virus?

- Run MS Defender Scan[a]
- Delete Temporary Files[b]
- Remove System Restore Point[c]
- Reset Browser Settings[d]
- Scan PC with Anti-Malware (*e.g.* MalwareFox).

Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an onscreen alert. How to Remove ransomwares? First, identify the type of attack and file extension, https://www.nomoreransom.org/en/index.html can help in this purpose. Secondly, use the following application to decrypt infected files

Spyware is any software that installs itself on your computer and starts covertly monitoring your online behavior without your knowledge or permission. It secretly gathers information about a person or organization and relays this data to other parties.

Adware is a form of malware that hides on your device and serves you advertisements. Some adware also monitors your behavior online so it can target you with specific ads.

How to prevent malware?

- Keep your computer and software updated.
- Use a non-administrator account whenever possible.
- Think twice before clicking links or downloading anything.
- Be careful about opening email attachments or images.
- Don't trust pop-up windows that ask you to download software.
- Limit your file-sharing.

See live Cyber Threat https://threatmap.checkpoint.com/

[a] Start->MS Defender Scan>Virus & Protection->Full Scan
[b] Start->Disk Cleanup>Select Temp Files
[c] Start->Create Restore Point->Configure->Delete
[d] Google Chrome Menu->Settings->Advanced->Reset and Cleanup->Restore Default Settings

Security Standards

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. Some Basic Terminology:

Plaintext original message

Ciphertext coded message

Cipher algorithm for transforming plaintext to ciphertext

Key info used in cipher; known only to sender/receiver, independent of the plaintext

Private key known only to the particular person

Public key known to everyone

Encipher (encrypt) converting plaintext to ciphertext

Decipher (decrypt) recovering plaintext from ciphertext

Cryptography study of encryption principles/methods

Cryptanalysis (code breaking) study of principles/methods of deciphering ciphertext without knowing key

Cryptology field of both cryptography and cryptanalysis

Types of Cryptography:

- **Symmetric Cryptography** is simplest type of encryption technique when one key (private k1) used to encrypt and decrypt. It is less complex, faster and used for bulk data transfer. But it is not safe as the same key is used at both ends. The most popular symmetric encryption technique is DES (Data Encryption System).
  1. **Substitution Technique/cipher** is the one in which the letters of the plain text are replaced by other letter or number or symbol, *e.g.* Name->IWPX.
     (a) **Shift cipher**. When $k = 3$, it is Caesar cipher. Simple and easy to implement. Cons? The encryption and decryption algorithms are known. There are only 25 keys to try, vulnerable to brute-force attack. The language of the plaintext is known and easily recognizable.
     (b) **Monoalphabetic cipher** The most commonly used letters of the English language are **e, t, a, i, o, n, s, h,** and **r**.

2. **Transposition Technique/cipher** performs some sort of permutation on the plaintext letters *i.e.* it reorders the symbols, *e.g.* NAME->EAMN or AEMN or MENA etc (total 4!=24 permutations).
3. **Data Encryption Standard (DES)**
   - https://www.youtube.com/watch?v=cVhlCzmb-v0
   - Triple-DES
4. **Advanced Encryption Standard (AES)**
   - **Prerequisites:** Fields (5.3 [2]), Galois Finite Field (5.4 [2]), Polynomial Arithmetic (5.5, 5.6 [2])
   - Chapter-6 [2]
   - Key expansion and AES algorithm
   - Difference between DES, Triple-DES and AES
5. **Kerberos** 15.3 [2]

- **Asymmetric Cryptography** is the type of encryption technique when two keys (one private key and one public key) used to encrypt and decrypt. A message encrypted using public key must be decrypted by private key while a message encrypted using private key must be decrypted by public key. The popular asymmetric algorithms are RSA, DSA, Elliptic curve etc.
  1. **RSA**
  2. **Digital Signature Algorithm (DSA)**
  3. **Diffie–Hellman Key Exchange**
- **Hash Function:** No usage of key concept. When a variable length message passed to a Hash function then a fixed value is found known as Hash value/code. Many OS uses it to encrypt passwords.
  1. **Secured Hash Algorithm (SHA)-1/224/256/384/512**
  2. **Message Digest 5 (MD5)**
     - https://youtu.be/r6GlzIWiMD0?t=220

Attacks on Conventional Encryption Scheme, general approaches:

1. **Cryptanalysis**
2. **Brute-force attack:** Trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.
   - Guessing
   - Exhaustive key search
   - Software Tools that can perform brute-force attack

Security At Transport Layer

Secure Socket Layer (SSL) and **Transport Layer Security (TLS)** are protocols for establishing authenticated and encrypted links between networked computers. Although the SSL protocol was deprecated with the release of TLS 1.0 in 1999, it is still common to refer to these related technologies as SSL or SSL/TLS. [4]

SSL is 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 is just an updated, more secure, version of SSL. [3]

What is an SSL certificate? An SSL certificate (also known as a TLS or SSL/TLS certificate) is a digital document that binds the identity of a website to a cryptographic key pair consisting of a public key and a private key. The public key, included in the certificate, allows a web browser to initiate an encrypted communication session with a web server via the TLS and HTTPS protocols. The private key is kept secure on the server, and is used to digitally sign web pages and

other documents (such as images and JavaScript files). An SSL certificate also includes identifying information about a website, including its domain name and, optionally, identifying information about the site's owner. If the web server's SSL certificate is signed by a publicly trusted certificate authority (CA), like SSL.com, digitally signed content from the server will be trusted by end users' web browsers and operating systems as authentic. [4]

HTTPS (Hyper Text Transfer Protocol Secure) appears in the URL when a website is secured by an SSL certificate. The details of the certificate, including the issuing authority and the corporate name of the website owner, can be viewed by clicking on the lock symbol on the browser bar.

Difference between HTTP and HTTPS

Security on Network Layer

Internet Protocol Security (IPSec)

Internet Security is normally applied at three layers:

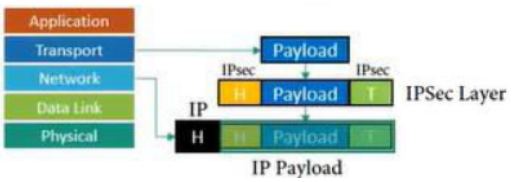
- Network Layer
- Transport Layer
- Application Layer

At network layer, security can be applied between

- Two hosts
- Two Routers
- A host and a router

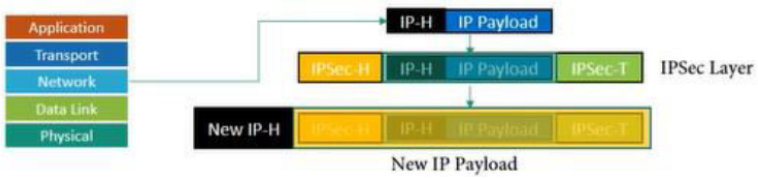
To provide the security at network layer, **IETF** (Internet Engineering Task Force) designed a set of protocol, known as IP Security (IPSec). VPN (Virtual Private Network) is one application of IPSec. Two modes of IPSec:

1. **Transport Mode:** IPSec protects what is delivered from the transport layer to the network layer, *i.e.* transport mode protects the payload to be encapsulated in the network layer. It does not protect the IP header. It only protects the packet from the transport layer (the IP-layer payload). This mode is used when we need host-to-host (end-to-end) protection. The IPSec layer in this case exists between Transport and Network layer.



2. **Tunnel Mode:** IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IP security methods to the entire packet, and then adds a new IP header. Normally used between:
   - two routers
   - a host and a router
   - a router and a host

   Here IPSec layer is the part of Network layer.



Two version of Protocol:

1. **AH (Authentication Header)** protocol is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet. The protocol uses a hash function and a symmetric (secret) key to create a message digest. The digest is inserted in the authentication header. The AH is then placed in the appropriate

location, based on the mode (transport or tunnel).

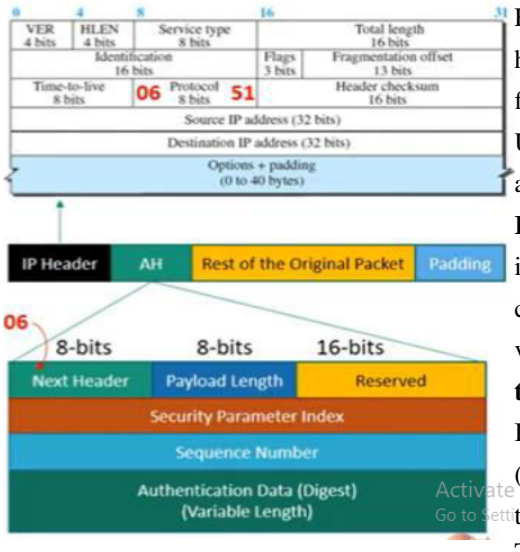
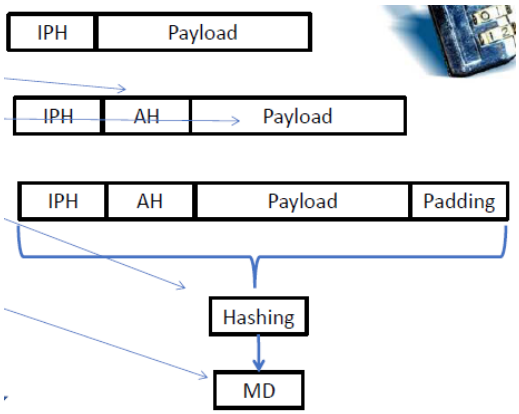


Figure shows the fields and the position of the authentication header in transport mode. **Next Header** is an 8-bit field that defines the type of payload carried by the IP datagram (such as TCP, UDP, ICMP, or OSPF). **Payload Length** defines the length of the authentication header in 4-byte multiples. **Security Parameter Index (SPI)** is a 32-bit field that plays the role of a virtual circuit identifier and is the same for all packets sent during a connection, called a **Security Association**. A 32-bit **sequence number** provides ordering information for a sequence of datagrams. **Authentication Data** is the result of applying a hash function to the entire IP datagram except for the fields that are changed during transit (*e.g.*, time-to-live). The AH protocol provides source authentication and data integrity, but not privacy/confidentiality.



The protocol works as follows:

(a) An authentication header is added to the payload with the authentication data field set to 0.

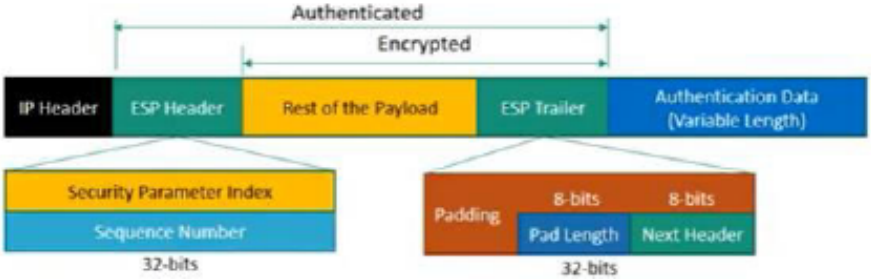
(b) Padding may be added to make the total length appropriate for a particular hashing algorithm.

(c) Hashing is based on the total packet. However, only those fields of the IP header that do not change during transmission are included in the calculation of the message digest (authentication data).

(d) The authentication data are inserted in the authentication header.

(e) The IP header is added after changing the value of the protocol field to 51.

2. **ESP (Encapsulating Security Payload)** provides source authentication, integrity, confidentiality. ESP adds a header and trailer. When an IP datagram carries an ESP header and trailer, the value of the protocol field in the IP header is 50. A field inside the ESP trailer (the next-header field) holds the original value of the protocol field (the type of payload being carried by the IP datagram, such as TCP or UDP). The ESP procedure follows these steps:
   (a) An ESP trailer is added to the payload.
   (b) The payload and the trailer are encrypted.
   (c) The ESP header is added.
   (d) The ESP header, payload, and ESP trailer are used to create the authentication data.
   (e) The authentication data are added to the end of the ESP trailer.
   (f) The IP header is added after changing the protocol value to 50.



Security Association is a technique that changes the connectionless service of the network layer to a connection-oriented service for the purpose of applying security measures. It is a contract between two parties; it creates a secure channel between them. If a peer relationship is needed for two-way secure exchange, then two security associations are required.

1. one outbound SA

2. one inbound SA

The Security Association can be more involved if the two parties need message integrity and authentication. Each association needs other data such as the algorithm for message integrity, the key, and other parameters. A security association is uniquely identified by three parameters:

1. **Security parameter index:** A 32-bit unsigned integer assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
2. **Destination address:** This is the address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router.
3. **Protocol (AH or ESP):** This field from the outer IP header indicates whether the association is an AH or ESP security association.

Think about the scenario: S.node wants to send messages to many people and R.node needs to receive messages from many people. Each site needs to have both inbound and outbound SAs to allow bidirectional communication. That means we need set of SAs. Hence, we need to store all these SAs in a database and that database is called **Security Association Database (SAD)**. SAD is a two dimensional table. Each row defining a single SA. Normally, there are two SADs, one inbound and one outbound. When a host needs to send a packet that must carry an IPSec header, the host needs to find the corresponding entry in the outbound SAD to find the information for applying security to the packet. Similarly, when a host receives a packet that carries an IPSec header, the host needs to find the corresponding entry in the inbound SAD to find the information for checking the security of the packet. SAD contains the following entry: Security Parameter Index, Sequence Number Counter, Sequence Counter Overflow, Anti-Replay Window, AH Information, ESP Information, Lifetime of this Security Association, IPsec Protocol Mode, Path MTU.

Security Policy Database defines the type of security applied to a packet when it is to be sent or when it has arrived. Each host that is using the IPSec protocol needs to keep a Security Policy Database (SPD). Here also there is a need for an inbound SPD and an outbound SPD. Each entry in the SPD can be accessed using a six tuple index: source address, destination address, Name, Protocol, source port, destination port.

Outbound SPD When a packet is to be sent out, the outbound SPD is consulted. The input to the outbound SPD is the six tuple index. The output is one of the three following cases:

- drop (packet cannot be sent)
- bypass (bypassing security header)
- apply (applying the security according to the SAD; if there is no SAD, create one).

Inbound SPD When a packet arrives, the inbound SPD is consulted. Each entry in the inbound SPD is also accessed using the same six tuple index. The output is one of the three following cases:

- discard (drop the packet)
- bypass (bypassing the security and delivering the packet to the transport layer)
- apply (applying the policy using the SAD).

Internet Key Exchange (IKE) is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. It provides message content protection and also an open frame for implementing standard algorithms. The Internet Key Exchange (IKE) is a protocol designed to create both inbound and outbound Security Associations. When a peer needs to send an IP packet, it consults the Security Policy Database (SPD) to see if there is an SA for that type of traffic. If there is no SA, IKE is called to establish one. IKE is a complex protocol based on three other protocols: Oakley, SKEME, ISAKMP.

Network Security Applications

AAA (Authentication Authorization Accounting) Standards

Authentication involves checking the identity being used, is being used by the correct owner of the identity. Types of authentication:

- **something a person knows**: commonly referred to as authentication by knowledge. Examples: a password,

a PIN, combination numbers (*e.g.* for a lock), secret answers (*e.g.* mother's maiden name).

- **something a person has**: commonly referred to as authentication by ownership. Examples: Swipe cards, Unique tokens, Keys.
- **something a person is**: commonly referred to as authentication by characteristic. The characteristic is a physical characteristic which is unique to the person, that way. Example: Fingerprints, Retinal scans, Face Identification (Face Id on smartphones).

Authorization checks what the identity has permissions (access rights) to.

Accounting records what the identity does.

Benefits of AAA: For big network, there are several router/switches, it is difficult to store authentication data to every device. For example, for a new user John, admin should enter login/password to every device, which is troublesome. Suppose an user wants access to router 2, At first user sends request to R2, then R2 sends the request to the server to check, if it is valid then user can get access to R2. To add a new user, admin just insert authentication data in AAA server.

Email Securities

- **Email Security Requirement**
  1. Confidentiality: protection from disclosure
  2. Authentication: of sender of message
  3. Integrity: protection from modification
  4. Non-repudiation: protection from deniel by sender
- **Protocols of Email**
  - Simple Mail Transfer Protocol (SMTP)
  - Post Office Protocol (PoP)
  - Internet Mail Access Protocol (IMAP)
  - Multipurpose Internet Mail Extension (MIME)

Pretty Good Service (PGP) is invented by Phil Zimmermann. It was designed to provide all four aspects of security in the sending of email. It uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. It 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. It 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. PGP Steps to secure e-mail at the sender site:

1. The e-mail message is hashed by using a hashing function to create a digest.
2. The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
3. The original message and signed digest are encrypted by using a one-time secret key created by the sender.
4. The secret key is encrypted by using a receiver's public key.
5. Both the encrypted secret key and the encrypted combination of message and digest are sent together.

PGP Steps to receive e-mail at the receiver site:

1. The receiver receives the combination of encrypted secret key and message digest.
2. The encrypted secret key is decrypted by using the receiver's private key to get the one-time secret key.
3. The secret key is then used to decrypt the combination of message and digest.
4. The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
5. Both the digests are compared if both of them are equal, means that all the aspects of security are preserved.

Sandboxing

It is a security mechanism that allows you to run software in isolated space. Sandboxing creates a virtual machine inside the machine. For example, creates Windows 10 inside Windows 10. Helpful for executing untrusted applications. Prevents programs from making permanent changes to system. Secure web browsing, *e.g.* malware downloaded from websites can't infect your system. Popular tool that implements sandboxing: Sandboxie.

To setup Sandbox:

1. First Check whether the machine is virtually enabled or not
2. To check it go to `Task Manager->Performance->CPU` and check virtualization. It should be enabled.
3. If NOT enabled then choose advance start up from start `/run` button. From `Recovery->advance startup->Restart now->Troubleshoot->advance option->UEFI Firmware Settings`
4. If Virtualization Enabled then from windows `Start->Turn on/off windows features->windows sandbox`
5. If still no windows sandbox feature exist then install Tool Sandboxie from Internet.
6. After installation open Sandboxie and `sandbox->new box->right click and proceed`

Firewalls and Proxy Server

Security for Wireless Network Protocols

What is Wireless Network? With the help of wireless technology we can transfer data from one device to another without using wires or cables. Using this technology we can establish network which is more flexible, intangible and easy to access. It supports communication via RF (Radio Frequency). Wireless communication is the transfer of information or power between two or more points that are not connected by an electrical conductor.

Need of Wireless Network

- Mobile communication
- Communication must take place in a terrain that makes wired communication difficult or impossible.
- A communication system must be deployed quickly.
- Communication facilities must be installed at low initial cost.
- The same information must be broadcast to many locations.

Requirements of Wireless Network

- Network Interface Card (NIC) used for wireless networks. NIC uses antenna, unlike the RJ45.
- Access Point for generating signal and establish connection between devices.
- Devices which has wireless signal adapter.

Types of Wireless Network: Based on the size, wireless networks are divided into 4 categories

1. **Wireless LAN** is a network where two or more computers are connected that covers only a limited area. The NIC used in this connection has a small range to cover. We often call this **peer to peer network**. This is also called **Ad Hoc Network** which is being set up for temporary purposes. Unlike switch in a wired network, a special device is used in WLAN, which is called **Access Point**. WLAN which uses access point are called **BSS (Basic Service Set)**. This acts as a coordinator between different devices. **Wi-Fi (Wireless Fidelity)** uses RF signal (Frequency: 2.4 GHz or 5 GHz). Wi-Fi technology is only used in WLAN. Range: About 100 Meters. Wi-Fi products are certified and tested by Wi-Fi alliance. We can see their trademarks in most of the Wi-Fi devices.
2. **Wireless MAN** is a collected unit of many WLANs located at various locations. It uses WIMAX (Worldwide Interoperability for Microwave Access) which is controlled by WiMAX Forum. Maximum Speed 1 Gbits/sec. IEEE 802.16
3. **Wireless WAN (WWAN)** is a very large network which is spread over a very large area. It connects many cities together. Mobile Phones use WWAN to make communication possible. The technology in WWAN are subdivided in many generations - 2G, 3G and 4G. The communication system which was used before the emergence of 2G is called 1G used in 1980. This technology is used in most of the Analog devices.

4. **Wireless PAN:** The Wireless Networks that are used in smaller distances are known as WPAN. The communication between a mobile phone and its Bluetooth headset is a typical example of WPAN. Two kinds of Wireless technologies are used for WPAN:
    - **Bluetooth** is used to connect devices in personal area without using cables. Use ISM band 2.4 GHz. Speed up to 721Kbps. Range 10 to 100 meters.
    - Infrared Data Association.

WEP (Wired Equivalent Privacy) was developed for wireless networks and approved as a Wi-Fi security standard in September 1999. WEP was supposed to offer the same security level as wired networks. The keys used by WEP are 64-bit & 128 bit. WEP was officially abandoned by the Wi-Fi Alliance in 2004. WEP keys lost public favor when people began to realize that they are easy to crack, which leaves your network potentially open to hackers.
WPA (Wi-Fi Protected Access) became available in 2003. It is more secure than WEP. It Uses TKIP (Temporal Key Integrity Protocol). The keys used by WPA are 256-bit. WPA, just like WEP, after being put through proof-of-concept and applied public demonstrations turned out to be pretty vulnerable to intrusion.
WPA2 (Wi-Fi Protected Access Version 2) support or use Advanced Encryption Standard (AES), became available in 2006. AES is approved by the U.S. government for encrypting the information classified as top secret, so it must be good enough to protect home networks.
WPA3 (Wi-Fi Protected Access Version 3) is the next generation of WiFi security. Protecting Wi-Fi from hackers is one of the most important tasks in cybersecurity. Which is why the arrival of next-generation wireless security protocol WPA3.

Security Protocols for Ad-Hoc Network

Security Protocols for Sensor Network

Security for Communication Protocols

Security for Operating System and Mobile Agents

Security for E-Commerce

Security for LAN and WAN

Switching and Routing Security

other State-OfThe-Art Related Topics

REFERENCES

[1] *10. System Security - Express Learning: Cryptography and Network Security [Book]*. en. URL: https://www.oreilly.com/library/view/express-learning-cryptography/9788131764527/chap10.xhtml (visited on 09/07/2022).

[2] William Stallings. *Cryptography and network security: principles and practice*. eng. Seventh edition, global edition. Pearson, 2017. ISBN: 9781292158587.

[3] *What is an SSL Certificate?* en-US. URL: https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https (visited on 09/10/2022).

[4] *What is SSL?* en-US. URL: https://www.ssl.com/faqs/faq-what-is-ssl/ (visited on 09/10/2022).

If you want to upgrade this shit, copy the project from Overleaf.