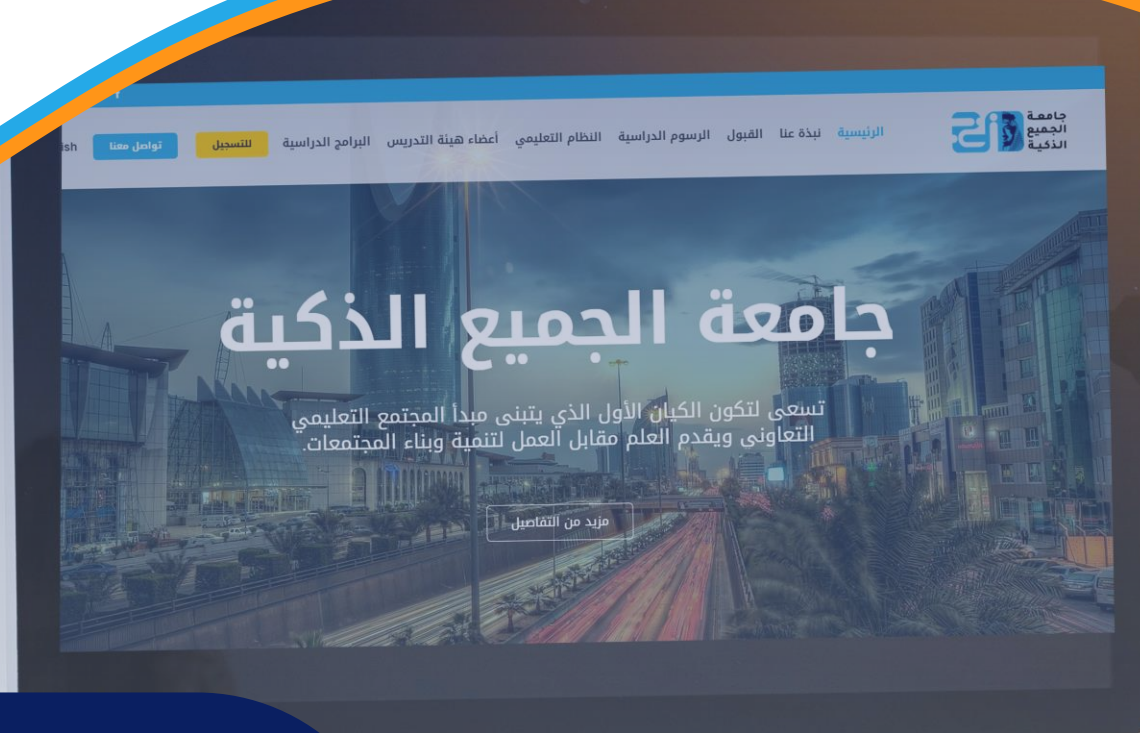




جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



IoT Security
Prepared by Dr. Abdelrhman Ahmed
Lecture 5

IoT Network security protocol

The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) open standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. IP Sec is developed as an integral element of Network VPN solutions. It also defines the encrypted, decrypted, and authenticated packets. The protocols needed for secure key exchange and key management are defined in it. IP Sec provides cryptography-based protection of all data at the IP layer of the communications stack. It provides secure communications transparently, with no changes required to existing applications. IP Sec is the IETF-chosen industry-standard network security framework for use in both the IP Versions 4 and 6 environments.



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.



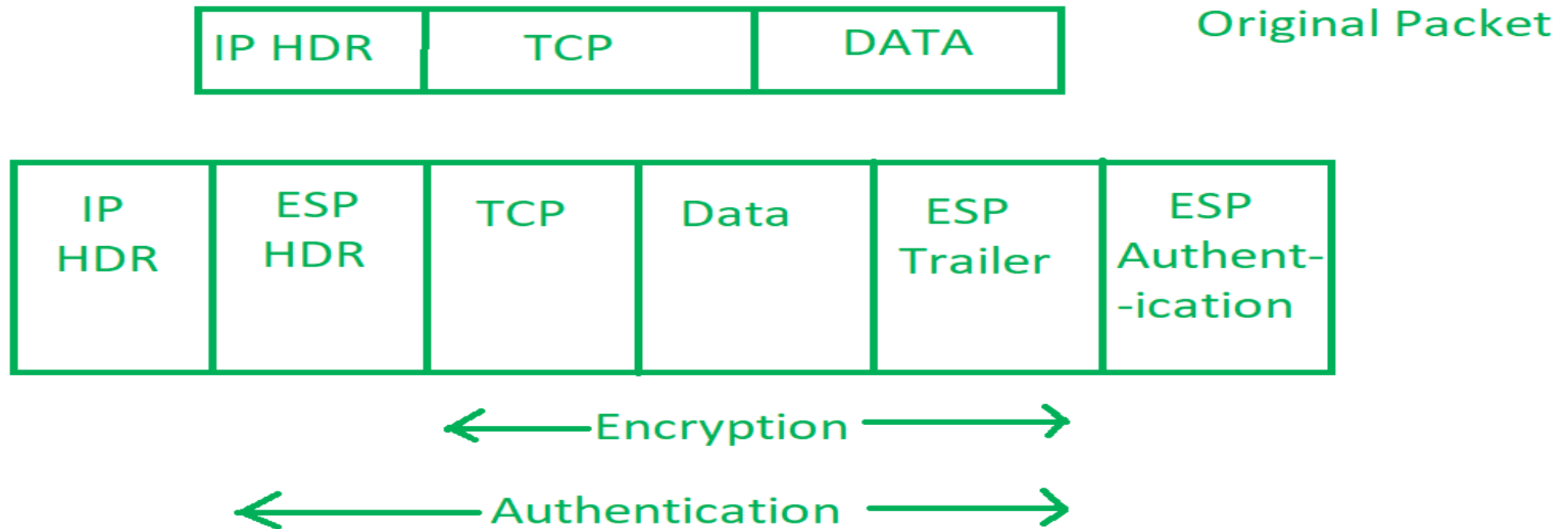
1. **Encapsulating Security Payload (ES)** :– It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.
2. **Authentication Header (AH)** :–It also provides data integrity, authentication, and anti-replay and it does not provide encryption.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



3. Internet Key Exchange (IKE) :- It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts are using IPsec.

Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produce a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets that are not authorized are discarded and not given to the receiver.



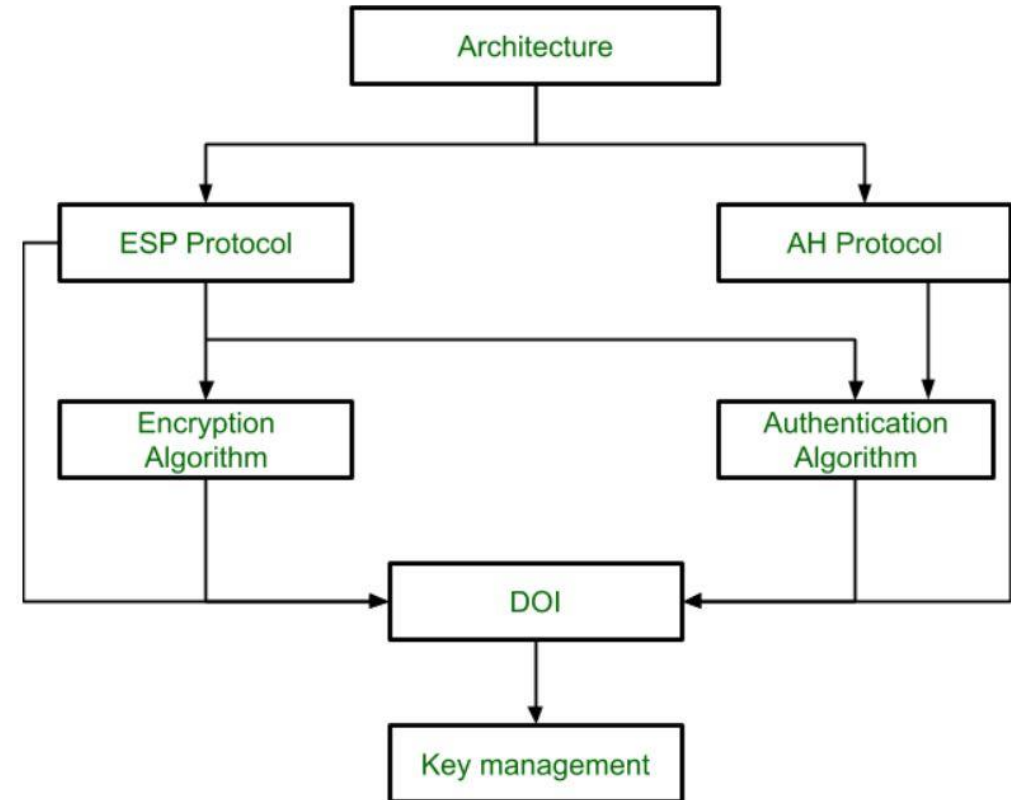


1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet applies appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
2. Then the **IKE Phase 1** starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The **Main mode** provides greater security and the **Aggressive mode** which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.

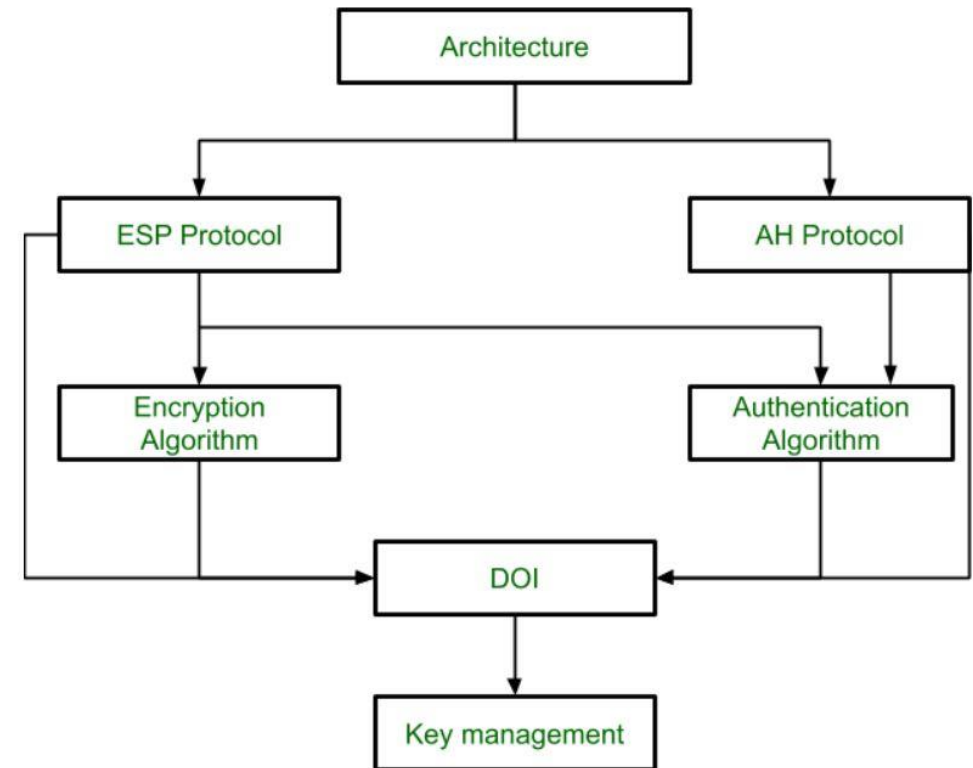
1. Now, the **IKE Phase 2** is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.
2. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
3. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both hosts.

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture includes protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality
- Authentication
- Integrity



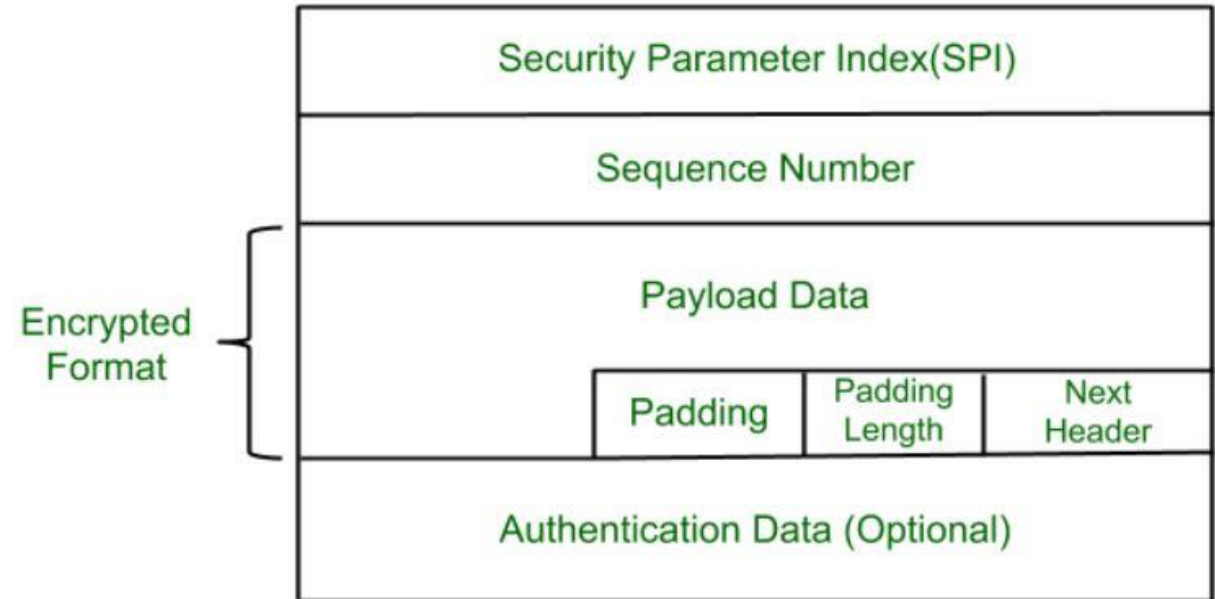
1. **Architecture:** Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms, and security requirements of IP Security technology.



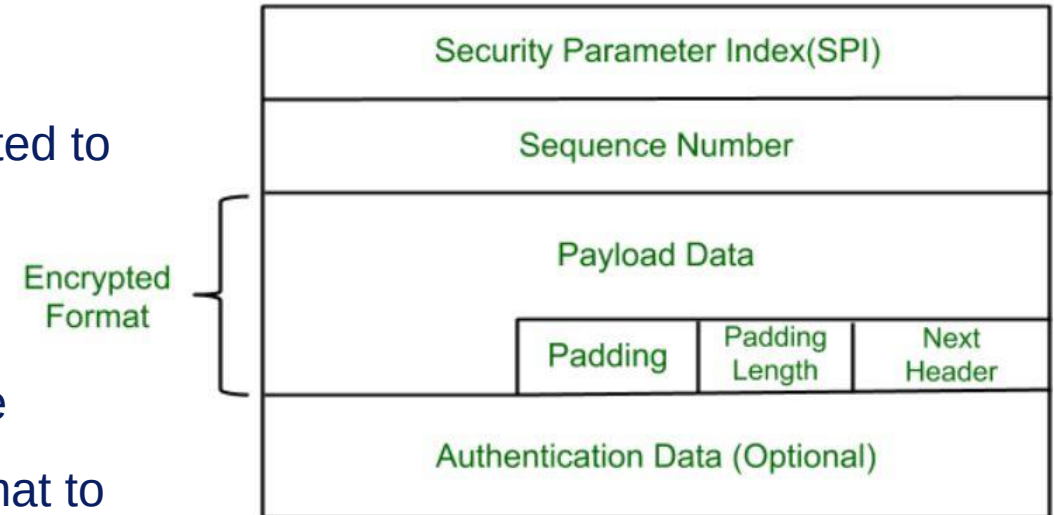
2. **ESP Protocol:** ESP(Encapsulation Security Payload) provides a confidentiality service. Encapsulation Security Payload is implemented in two ways:

- ESP with optional Authentication.
- ESP with Authentication.

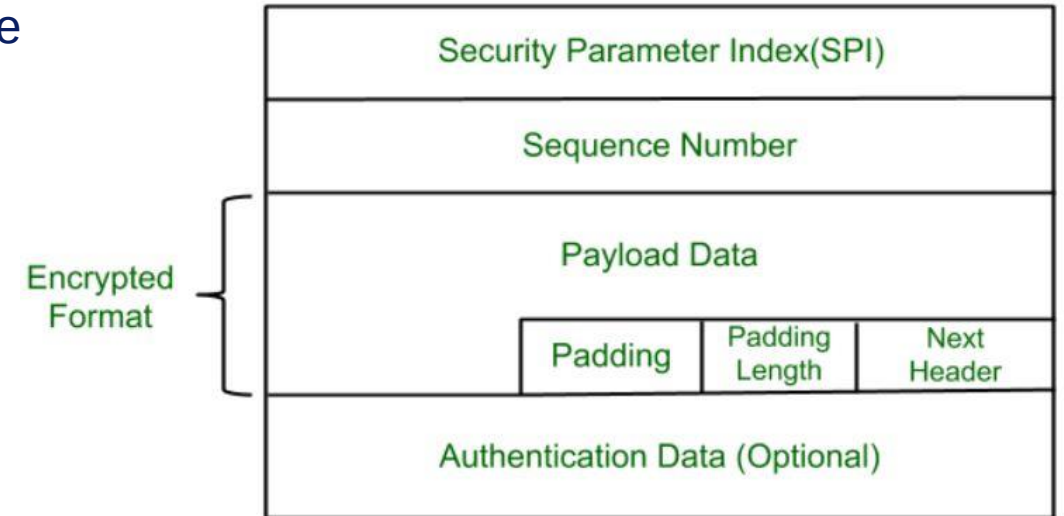
Packet Format:



- **Security Parameter Index(SPI):** This parameter is used by Security Association. It is used to give a unique number to the connection built between the Client and Server.
- **Sequence Number:** Unique Sequence numbers are allotted to every packet so that on the receiver side packets can be arranged properly.
- **Payload Data:** Payload data means the actual data or the actual message. The Payload data is in an encrypted format to achieve confidentiality.



- **Padding:** Extra bits of space are added to the original message in order to ensure confidentiality. **Padding length** is the size of the added bits of space in the original message.
- **Next Header:** Next header means the next payload or next actual data.
- **Authentication Data:** This field is optional in ESP protocol packet format.



3. **Encryption algorithm:** The encryption algorithm is the document that describes various encryption algorithms used for Encapsulation Security Payload.

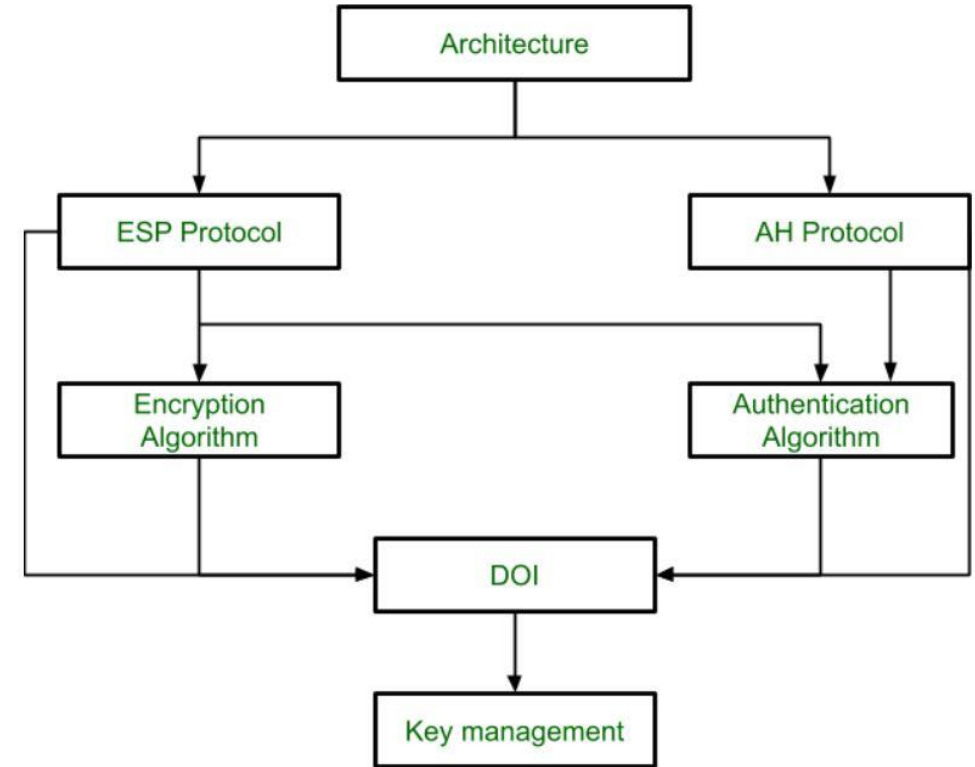
4. **AH Protocol:** AH (Authentication Header) Protocol provides both Authentication and Integrity service. The authentication Header is implemented in one way only: Authentication along with Integrity. The authentication Header covers the packet format and general issues related to the use of AH for packet authentication and integrity.

Next Header	Payload Length	Reserved
Security Parameter Index		
Sequence Number		
Authentication Data (Integrity Checksum)		

5. **Authentication Algorithm:** The authentication Algorithm contains the set of documents that describe the authentication algorithm used for AH and for the authentication option of ESP.

6. **DOI (Domain of Interpretation):** DOI is the identifier that supports both AH and ESP protocols. It contains values needed for documentation related to each other.

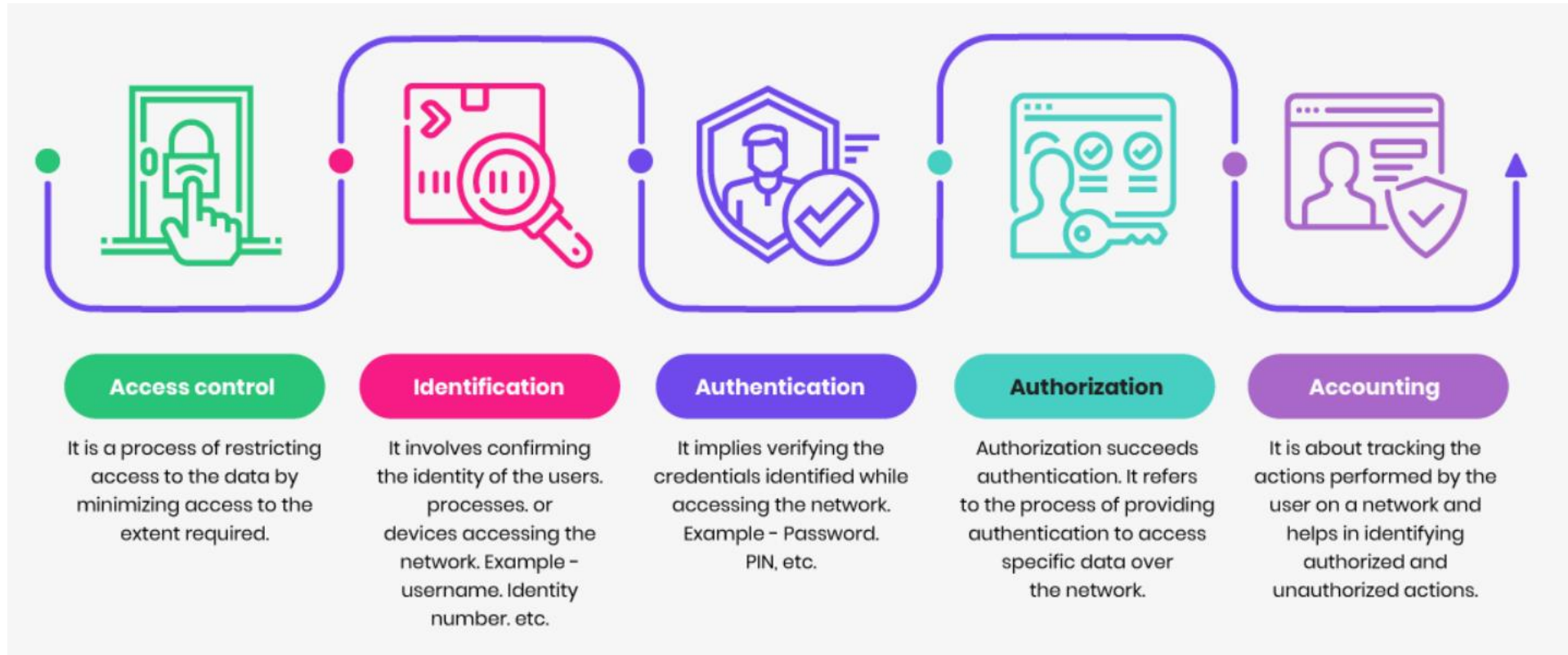
7. **Key Management:** Key Management contains the document that describes how the keys are exchanged between sender and receiver.



Foolproof network security is only possible through a detailed risk assessment process. The cybersecurity official should determine the nature and extent of existing and potential threats. Using the assessment, they'll suggest network security and firewalls to fix the vulnerabilities and counter any issue that may harm the system in the future.

Network security controls deliver the integrity and confidentiality of the network devices. Effective use of these tools reduces the risk of attacks and breaches. Proper security solutions allow organizations to implement strategies, as suggested by cybersecurity officials. Multiple control layers minimize the chances of attacks and ensures that the system will have active defensive measures. If one layer fails during a breach, another will take control to tackle the issue. This practice is known as defense in depth.





Network protocols allow communication between two or more network devices. In the absence of these protocols, devices lack the capability of understanding the electric signals they share. Different computer network protocols have specific purposes and scenarios.



Internet Protocol (IP): It is the address system of the internet with the core function of delivering information packets. IP is a primary key to network connections.

Transmission Control Protocol (TCP): TCP works with IP for exchanging data packets. TCP organizes data to ensure secure transmission between the client and the server.

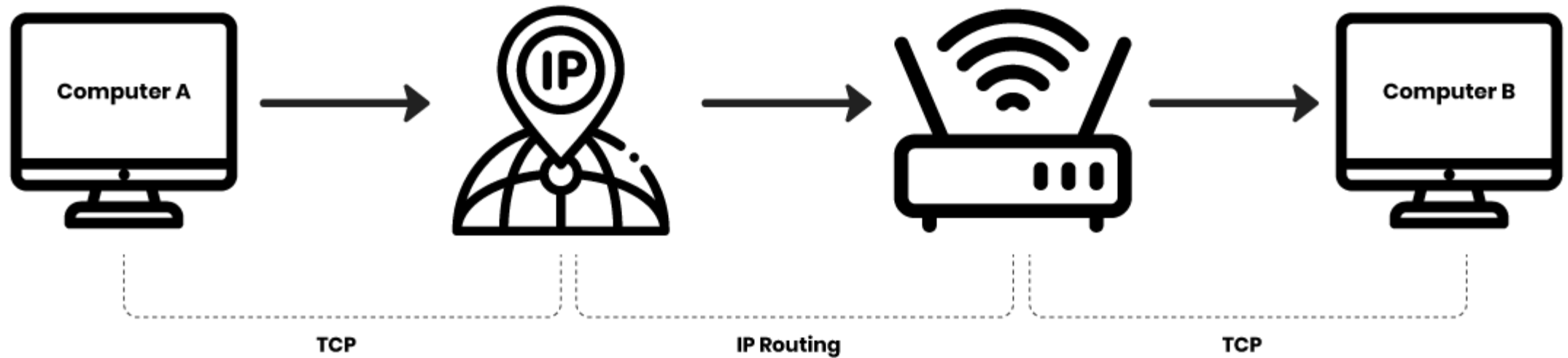
Components of network protocols:

Wireless Network Protocols: These protocols work on wireless networks, e.g., Wi-Fi, Bluetooth, and LTE. It proves useful for mobile and electronic devices that are not directly connected to a wire.

Network Routing Protocols: A routing protocol defines the route path to carry network messages and dynamic routing decisions. OSPF, BGP, and EIGRP are some examples of routing protocols.

Chapter 05

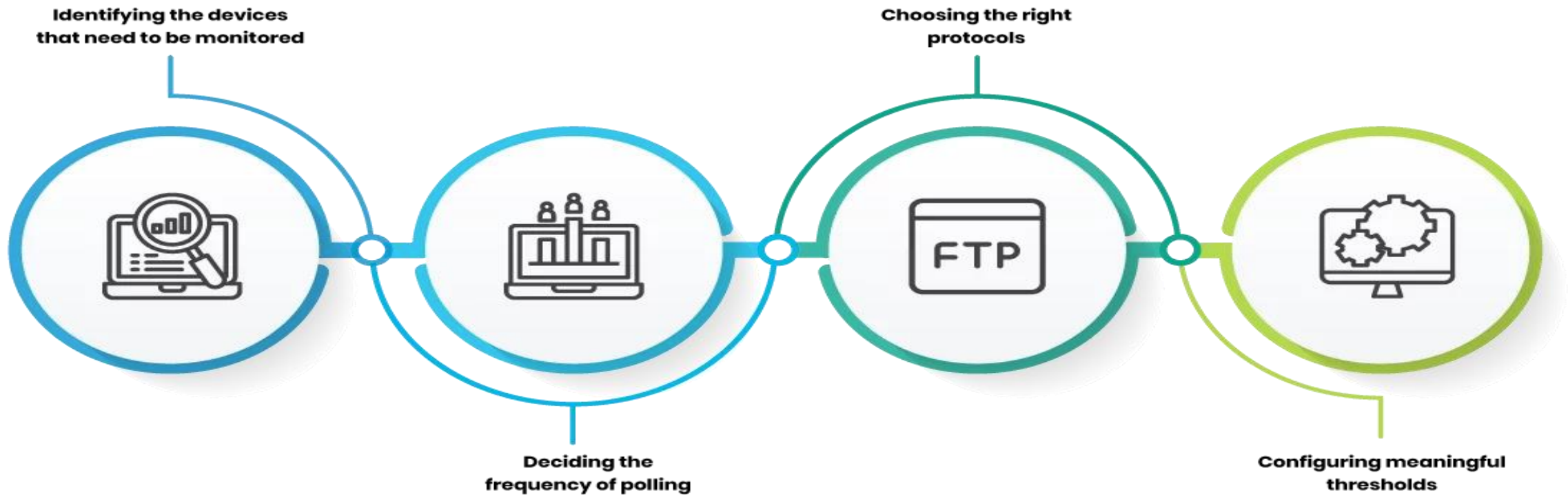
Components of Network Protocols



Network security is monitored to ensure the safety of the internal systems and the data that is generated during the process. This data is helpful in various IT operations and case studies. Network traffic monitoring tools are broadly classified into two types. There are deep packet inspection tools and flow-based tools. These tools are gaining popularity in the cybersecurity community as companies are relying on mechanics like cloud and VOIP. Network monitoring software is helpful in monitoring network traffic whenever the stress on the network increases.

Chapter 05

Ensure Security of Wireless Network



Security Techniques:-

No network is safe in an environment where hackers continuously find ways to exploit the system. A threat can cause problems at any moment. A foolproof network security system will ensure these problems won't occur. Here are some of the must-have network security tools that help you protect your internal systems from intrusions.

Access control: in network security allows you to improve defense by limiting user access and resources to certain parts of the network for which they are responsible.

Anti-malware: is one of the security essentials that identifies viruses, worms, Trojans, etc., and prevents them from infecting the network.

Behavioral Analytics: Security personnel establishes guidelines for what is considered normal behavior for customers as well as users. Behavioral analytics software keeps an eye on any suspected activity to identify abnormal behavior.

Application security: helps establish security guidelines for applications that are relevant to network security. This process blocks any suspicious application from entering the system as well as for closing gaps in security coverage.

Data Loss Prevention: Humans are considered the weakest security link. Data loss prevention (DLP) technologies protect staff and anyone who uses the network from misusing and possibly compromising sensitive data.

Firewalls: are an important part of the network security system as they act as a barrier between the network's trusted zone and everything beyond it.

Email Security: Phishing allows intruders to access an insecure network illegally. Email security blocks phishing attempts and outbound messages carrying sensitive data.

Mobile and Wireless Security: Mobile and wireless devices are vulnerable to possible network breaches and therefore require extra scrutiny.

Intrusion Detection and Prevention: Intrusion detection and prevention systems AKA intrusion detection system analyze network traffic/packets to identify different types of attacks and respond quickly. Intrusion detection systems create a database of known attack methods to identify patterns and thwart any similar incidents in the future.

Security Information and Event Management (SIEM): SIEM collects data from various network tools. This information helps in identifying and responding to threats accordingly.

VPN: A virtual private network authenticates safer communication between a network and a device.



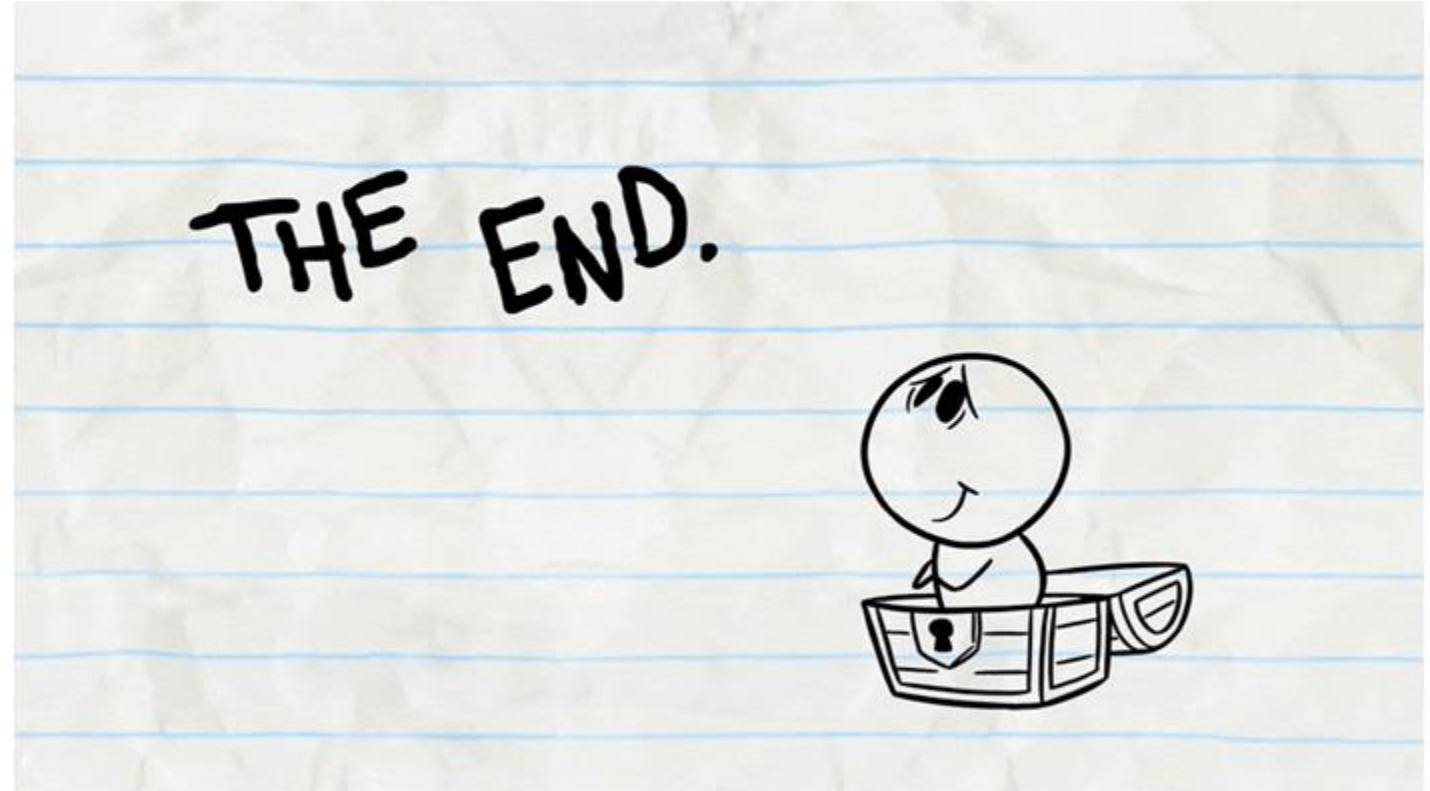
VPN: A virtual private network is an extension of an enterprise's private intranet across a public network such as the Internet. It creates a secure private connection through what is essentially a private tunnel. VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners/suppliers into an extended corporate network. Internet service providers (ISPs) offer cost-effective access to the Internet through direct lines or local telephone numbers. Therefore, companies can eliminate their current networking options that use more expensive leased lines, long-distance calls, and toll-free telephone numbers.



The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY