Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Acknowledgement

- *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

Network Protection for Energy Control Systems

Overview

- Topic-1: Introduction to Energy Control Network Protection
- Topic-2: Common Security Weaknesses and Attacks in Energy Control Networks
- Topic-3: Essential Protection for Energy Control Networks
- Topic-4: Advanced Protection for Energy Control Networks

Agenda

01. Internet Security Problem

02. Ransomware Activities Impacting the Energy Sector

03. IP Security

04. Internet of Things (IoT) for Energy Sector

05. SSL/TLS for the IoT

What is TCP?

- Transmission Control Protocol (TCP) is a fundamental communications standard facilitating message exchange over networks, ensuring successful data delivery.
- TCP is a core internet protocol defined by the Internet Engineering Task Force (IETF) and is widely utilized in digital network communications for end-to-end data delivery.
- TCP establishes and maintains connections between sources and destinations, organizes data into packets, guarantees data integrity, and is widely employed by high-level protocols like FTP, SSH, IMAP, POP, SMTP, HTTP, among others.

What is TCP/IP in Networking? | Fortinet

What is IP?

- The **Internet Protocol** (**IP**) facilitates **data transmission** between **devices** across the **internet** by assigning each device a **unique IP address**. Today, it's considered the standard for **fast** and **secure communication** directly between **mobile devices**.

- IP is **responsible** for defining how **applications** and **devices** exchange data **packets**, **serving** as the principal **communications** protocol for **data exchange** between **computers** on **single** or **interconnected** networks.

- It does this through the **Internet Protocol Suite** (**TCP/IP**), a group of communications **protocols** that are split into **four abstraction** layers.

- IP is the main protocol within the **internet layer** of the **TCP/IP**, and it is **responsible** for delivering **data packets** between **source** and **destination** devices by incorporating **tags** such as address information within the **packets**.

The OSI model and TCP/IP model | Infosec (infosecinstitute.com)

How does TCP/IP work?

- **TCP/IP** works using the **client-server model**, where a client **requests** a **service** (e.g., sending a webpage) from a **server** in the network.
- The **TCP/IP** suite is classified as stateless overall, meaning each **client request** is considered new and unrelated to previous ones, allowing for **continuous** use of network **paths**.
- However, the **transport** layer within **TCP/IP** is **stateful**, maintaining a connection **until all packets** in a message are **received** and **reassembled** at the **destination**. This model slightly **differs** from the **OSI networking model**, which defines **communication** between **applications** over a network.

TCP/IP: What is TCP/IP and How Does it Work? (techtarget.com)

TCP vs. IP: What is the Difference?

- **TCP** and **IP** are separate **protocols** that collaborate to **ensure** data delivery within a network.
- **IP** assigns the **IP address**, defining the destination for the data, while **TCP transports** and **routes** the **data** to the designated **destination** and **ensures** it gets delivered to the destination application or device that IP has defined.
- Together, **TCP** and **IP** facilitate **communication** between **devices** over long **distances efficiently**.
- The **IP** address is like a **phone number** for a **smartphone**, while **TCP functions** similarly to the technology that enables the **phone** to ring and allows the **user to communicate** with the caller.
- **TCP/IP** refers to the combined use of **TCP** and **IP**, ensuring **safe** and **secure** data **transfer** between devices when **appropriate security protocols** are in place.

What is TCP/IP in Networking? | Fortinet

Why is TCP/IP important?

- **TCP/IP** is unrestricted and not controlled by any single company, allowing for easy **modification** of the IP suite.
- It is **compatible** with all **operating systems** (**OS**) and can communicate with any other system, computer **hardware,** and **networks**.
- **TCP/IP** is highly **scalable** and can **determine** the most **efficient** path through the network as a routable **protocol**, making it widely **used** in current **internet architecture**.

TCP/IP: What is TCP/IP and How Does it Work? (techtarget.com)

Four Layers of the TCP/IP model

1. The **application** layer **facilitates** standardized data exchange for **applications** and includes **protocols** such as HTTP, FTP, SMTP, POP3, and SNMP. It deals with the actual **application** data.

1. The **transport** layer ensures **end-to-end** communications across the network. **TCP** handles **communications** between **hosts** and **provides** flow control, multiplexing, and reliability.
   - The **transport protocols** include **TCP** and User Datagram Protocol (**UDP**), sometimes used instead of **TCP** for special purposes.

2. The **network layer**, the **internet** layer, deals with **packets** and **connects** independent networks to **transport** the **packets** across network boundaries.
   - The **network layer** protocols are **IP** and **Internet Control Message Protocol**, used for error **reporting**.

3. The **physical layer**, the **network interface** or **data link layer**, operates at the link level, connecting nodes or hosts within a network.
   - **Protocols** in this layer include **Ethernet** and **Address Resolution Protocol**.

TCP/IP: What is TCP/IP and How Does it Work? (techtarget.com)

Internet Security Problem

- Today's Internet is primarily **comprised** of
  - Public
  - Un-trusted
  - Unreliable IP networks
- Because of this inherent lack of security, the Internet is subject to various types of **threats**

COMPSCI-726-IPSec.pdf (auckland.ac.nz)

Internet Security Problem

- **Unauthorised modification**
  - The contents of a **packet** can be accidentally or deliberately modified
- **Identity spoofing**
  - The origin of an IP packet can be **forged**
- Replay attacks
  - **Unauthorised** data can be retransmitted
- **Loss of privacy**
  - The contents of a packet can be **examined** in transit

COMPSCI-726-IPSec.pdf (auckland.ac.nz)

Most Common Types of Cyber Attacks?

1.Malware: Malware is malicious software that harms **computers**, **networks**, or **servers**. It includes **ransomware**, **trojans**, **spyware**, **viruses**, **worms**, **keyloggers**, **bots**, and **crypto-jacking**.

2.Denial-of-Service (**DoS**) **Attacks**: A Denial-of-Service (DoS) attack **floods** a network with **false requests**, disrupting business **operations**. Users can't access **email**, **websites**, or other **resources**, **costing time** and **resources** to restore **operations**. Unlike DoS attacks, **Distributed Denial of Service** (**DDoS**) attacks originate from multiple **systems**, making them harder to block. (According to the practical task in Topic 1)

3.Phishing: Phishing is a **cyberattack** method using **email**, **SMS**, **phone**, or **social media** to trick victims into sharing **sensitive** information or **downloading** malicious files.

4.Spoofing: Spoofing is when cybercriminals **disguise** as trusted **sources** to access systems or **devices**, aiming to steal information, extort money, or install malware. (According to the practical task in Topic 1)

5.Identity-Based Attacks: Identity-driven **attacks** are difficult to **detect** and involve **compromised** credentials, making it challenging to distinguish between **genuine** user behavior and a **hacker** using **traditional** security measures and tools.

10 Most Common Types of Cyber Attacks Today - CrowdStrike

Most Common Types of Cyber Attacks?

6. **Code Injection Attacks**: Code **injection** attacks involve **injecting malicious** code into vulnerable systems to alter their behavior.

6. **Supply Chain Attacks**: A **supply chain attack** targets trusted **third-party** vendors in the supply chain by **injecting malicious code** into **software** or **compromising** hardware components to **infect users**. Software supply **chains** are vulnerable due to their **reliance** on various **off-the-shelf components** like third-party **APIs**, **open-source** code, and proprietary software from vendors.

6. **Insider Threats**: IT teams must address **external** and **insider** threats for **comprehensive** security. Insider threats, like **current** or **former** employees, pose **significant** risks due to their access to **sensitive data** and knowledge of company **operations**. These **threats** could be **malicious**, driven by **financial gain** or **coercion**, or **non-malicious**, stemming from negligence. On the other hand, some **insider threats** are **not malicious** but negligent. To mitigate these risks, organizations should implement robust **cybersecurity training programs** to educate stakeholders about potential **threats**, including those from **insiders**.

6. **DNS Tunneling**: DNS Tunneling is a **cyberattack** using **DNS queries** to bypass security measures and transmit data within a network. Once compromised, **hackers** can **command** and **control activities**, **deploy malware**, and **extract sensitive data** using **DNS tunneling** by encoding information in DNS responses.

6. **IoT-Based Attacks**: IoT attacks target IoT devices or networks, enabling hackers to **control devices**, **steal data**, or form **botnets** for **DoS/DDoS** attacks. With connected devices on the rise, cybersecurity experts anticipate **increasing** IoT **infections**, particularly with the expansion of **5G networks**.

10 Most Common Types of Cyber Attacks Today - CrowdStrike

Homework: Code Injection

PRACTICAL TASK

Objective: To enhance your practical skills, it is crucial to engage in hands-on work. The aim of this exercise is to simulate a real-world network to see how an attacker can inject code into a victim's machine.

Guidelines: Follow the steps below to set up a controlled, simulation-based lab environment using virtual machines (a victim and an attacker). This setup will enable you to send code from the attacker's side to the victim, allowing the code to be injected whenever the victim visits a particular website.

1. Use the GNS3 network simulator to create a topology with a node (victim machine) and a Kali Linux machine acting as the attacker.
2. Ensure you install these machines on your preferred virtual machine software and integrate them with the GNS3 server.
3. Ensure the installation of the Bettercab tool on your Kali Linux.

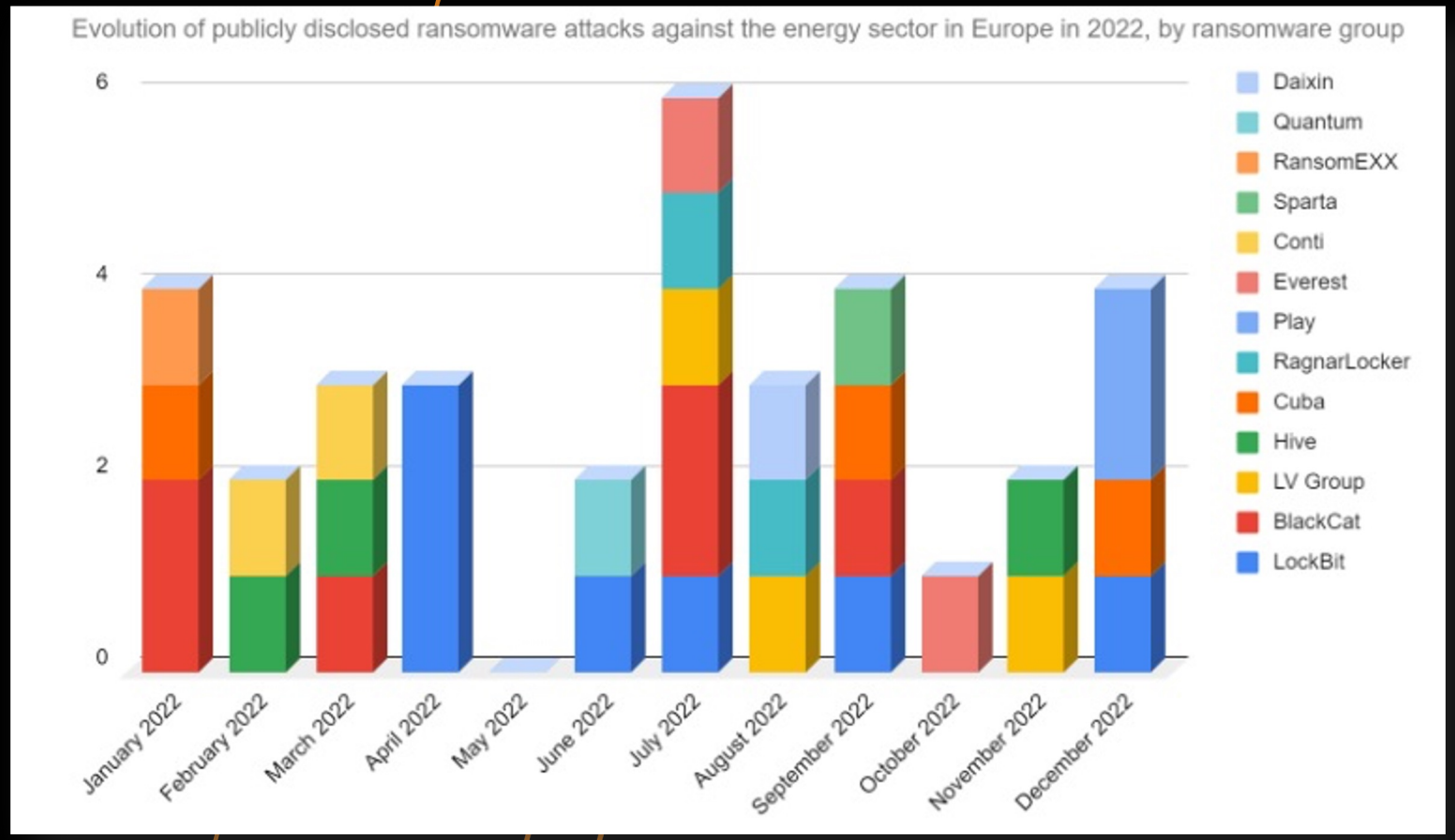
Task: Use Bettercap to position the attacker in the middle of the traffic between the victim machine and the gateway. This tool will enable you to perform ARP spoofing, misleading the gateway into believing that the attacker's device is the legitimate one, and deceiving the legitimate device into thinking that the attacker is the gateway. Create a simple JavaScript code (e.g., alert('Hello World');), which will be injected and executed when the victim visits a website. It is required to use a website developed solely for the educational purpose of describing security breaches; therefore, we require the use of the Acunetix Web Vulnerability Scanner. Ensure the code is injected when the victim visits the Vulnweb.com site. Report the results and demonstrate how the code is successfully injected into the victim's machine.

List of Large-Scale Cyber Attacks on Critical Infrastructure Facilities of Energy Sector

Year	Location	Attack Objects	Type	Impact
2014	International	**Energy companies**	NA	**250** US and **Western European companies** were infected for **espionage**.
2015	Ukraine	**Electricity operators**	DDoS	**30 substations** disconnected, **8 provinces** without power **for hours**.
2015	UAE	**Energy companies**	Trojan "Laziok"	**Espionage**, strategically important data theft
2017	Turkey	**Electric network in Istanbul**	Trojan	Power system **failure**, **blackout** in the city over **2 hours**
2019	Utah, USA	**Wind farms**	Trojan	**Power system failure**
2020	USA	**Energy department**	Trojan	**Power system failure**
2021	Denmark	**Wind turbines** of Vestas company	Trojan	Vestas, top wind turbine supplier, data **compromised** in suspected 22.11.21 cyberattack.
2022	Ukraine	**Ukranian electrical substations**	Industroyer2	**April 2022 virus targets Ukrainian high-voltage substations**, controls **switches** and **circuit breakers** using **Industrial control system** (ICS) protocols. Detected and **mitigated** before blackout.
2022	Austria	**Wind turbines of Enercon company**	NA	Around **5,800** wind **turbines in Europe**, generating **11,000 MW**, were **affected** by the **malfunction**. It took **weeks** to become controlled again
2022	Germany	**Wind turbines of Windtechnik company**	NA	Deutsche **Windtechnik** faced a **cyberattack on April 12, 2022**, after the **attack** was **detected**, **all remote data monitoring connections** to the **wind turbines** were **disconnected** for **security reasons**.
2022	Germany	**Wind Turbine Giant Nordex**	Bazar Loader TrickBot	The **cyber-attack was detected by IT security** team early. Nordex revealed that the **necessary response protocols** were taken and **IT systems** across multiple locations and business units were **shut down**

Fursov, Ihor, Klym Yamkovyi, and Oleksandr Shmatko. "Smart Grid and wind generators: an overview of cyber threats and vulnerabilities of power supply networks." *Radioelectronic and Computer Systems* 4 (2022): 50-63.

Ransomware Activities Impacting the Energy Sector in 2022



[The Energy sector 2022 cyber threat landscape - Sekoia.io Blog]

Main Internet Security Protocols

- Security protocols ensure **secure communication** between multiple **computers** by encrypting data to safeguard it from **unauthorized access**, allowing only **authorized** users to access it. Some standard security protocols include:
  - **Secure Sockets Layer (SSL):** Establishes a secure **connection** between **two computers** by **encrypting data transferred** over the **internet**, **preventing hackers** from **intercepting** sensitive information.
  - **IPsec (Internet Protocol Security)**: Encrypts all **data transmitted** over a network, providing **end-to-end security** for communications between **different networks**.
  - **Transport Layer Security (TLS)**: **Secures data** at the transport layer, where data is **sent** and **received** by applications. TLS **ensures** that **all messages** sent across the network are **authenticated**, **encrypted**, and **cannot be intercepted**.

3 Mains Types of Network Protocols | TradeWeb

IP Security

- **IP security** (**IPsec**) is a capability that can be **added** to either the **current** version of the **Internet Protocol** (**IPv4** or **IPv6**) by means of **additional** headers.
- **IPsec** encompasses **three functional areas**: **authentication**, **confidentiality**, and **key management**.
- **Authentication** makes use of the **Hash-based message authentication** code (or HMAC) message **authentication** code. **Authentication** can be **applied** to the **entire original** IP packet (**tunnel mode**) or to all of the packets except for the IP **header** (transport mode).
- **Confidentiality** is provided by an **encryption** format known as encapsulating security **payload**. Both **tunnel** and **transport** modes can be accommodated.

IP Security

- Have a range of **application-specific security mechanisms**
  - **Secure/Multipurpose Internet Mail Extensions** (S/MIME)
  - **Pretty Good Privacy** (PGP)
  - **Kerberos**,
  - **Secure Sockets Layer (**SSL)
  - **Hypertext transfer protocol secure** (HTTPS)
- Organizations can secure their **IP network** by blocking **links** to **untrusted sites**, **encrypting outgoing packets**, and **authenticating incoming** ones, ensuring **comprehensive** security even for **applications** lacking built-in **security measures**.
- Would like security **implemented** by the **network** for all applications

Benefits of IPsec

- **IPsec**, when integrated into a **firewall** or **router**, offers **robust security** for all **perimeter traffic** without imposing **additional processing** overhead on **internal network traffic**.
- **IPsec** in a **firewall** is difficult to **bypass** when all **external** traffic **must pass through** the **firewall** as the legitimate entry point from the Internet into the organization.
- **IPsec** below the **transport layer** (**TCP/UDP**), making it **transparent** to applications. Therefore, there's **no requirement** to modify **software** on **user** or **server** systems when implementing **IPsec** in the **firewall** or **router**.
- There is no need to **train users** on **security mechanisms**, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- **IPSec** can secure **individual users**, which is beneficial for remote **workers**, and create **secure virtual subnetworks** for **sensitive applications** within an organization.

How does IPsec work?

- IPsec connections involve the following steps:
  - **Key exchange**: Key exchange in **IPsec** involves **setting up keys** for encryption through a **secure exchange** between **connected devices**.
  - **Packet headers and trailers**: IPsec **adds headers** and **trailers** to data packets, providing **authentication** and **encryption** information. These additions help **ensure secure transmission** over the network.
  - **Authentication**: **IPsec** provides **authentication** for each **packet**, like a **stamp** of **authenticity** on a **collectible** item. That aims to **verify packets** are from trusted **sources**, **not attackers**.
  - **Encryption**: **IPsec encrypts** packet **payloads** and **IP headers**, ensuring **secure** and **private** data **transmission**.
  - **Transmission**: **Encrypted IPsec packets** travel across one or more networks to their destination using a **transport protocol**.
    - At this stage, IPsec traffic **differs** from **regular** IP traffic in that it most often **uses UDP** as its **transport protocol**, rather than **TCP**. TCP, the **Transmission Control Protocol**, sets up **dedicated connections** between devices and ensures that all **packets arrive**. **UDP**, the **User Datagram Protocol**, does not set up these dedicated connections. IPsec uses **UDP** because this allows IPsec packets to get through **firewalls**.
  - **Decryption**: At the other end of the **communication**, the packets are **decrypted**, and **applications** (e.g. a **browser**) can now use the delivered data.

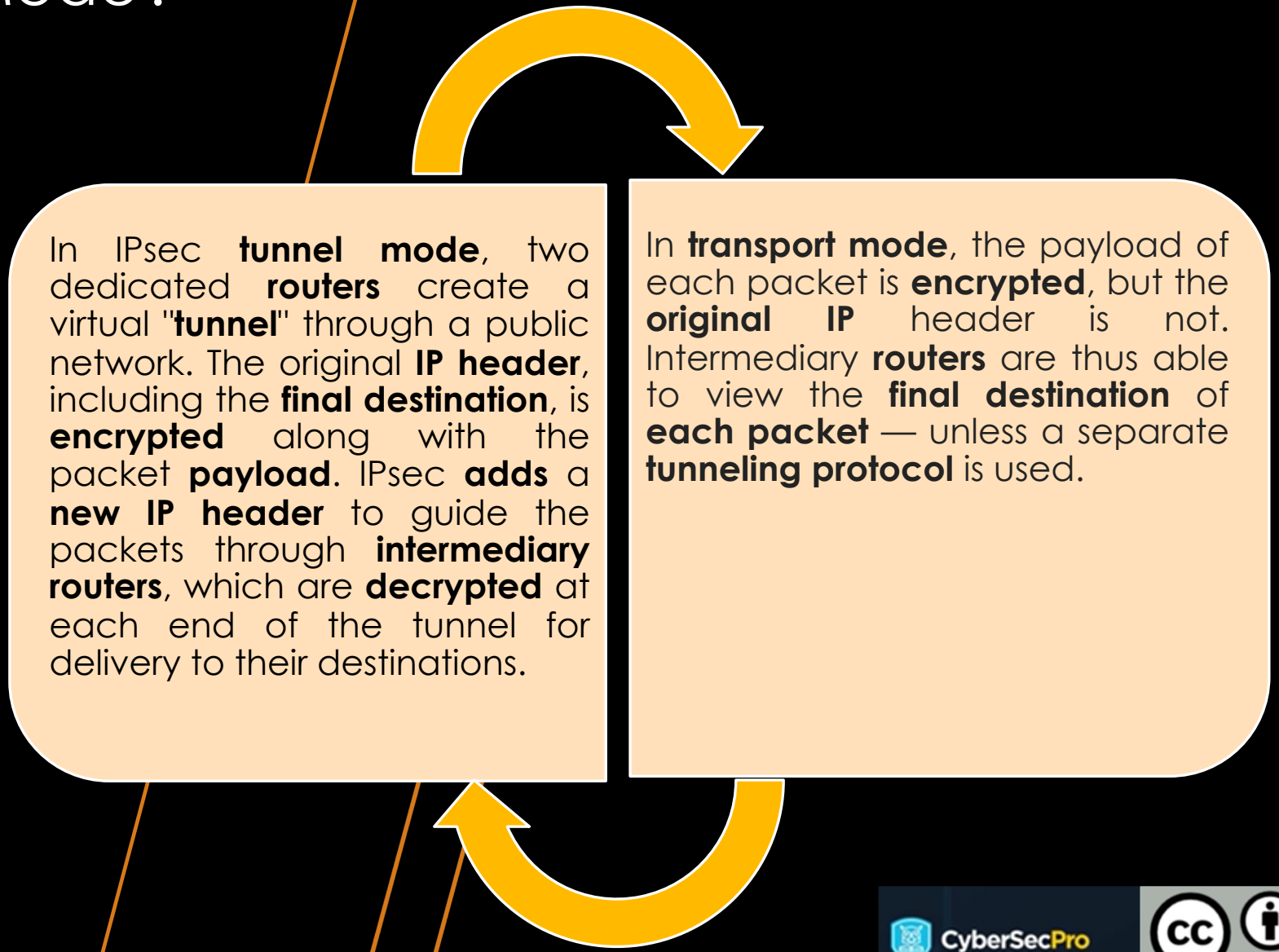
What is IPsec? | How IPsec VPNs work | Cloudflare

What Protocols are Used in IPsec?

- **IPsec** is a suite of **protocols** used in networking to **format data** for **interpretation** by networked computers.
  - **Authentication Header** (**AH**) **ensures data packets** are from trusted sources and haven't been tampered with, acting like a tamper-proof seal. However, **AH headers** don't **encrypt** data or hide it from attackers.
  - **Encapsulating Security Protocol** (**ESP**) **encrypts** both the **IP header** and **payload** in each packet, except in transport mode where only the payload is **encrypted**. Additionally, **ESP** adds its own header and trailer to each packet.
  - **Security Association** (**SA**) encompasses **protocols** for negotiating encryption keys and algorithms, with **Internet Key Exchange** (IKE) being a prominent example.

What is IPsec? | How IPsec VPNs work | Cloudflare

What is the Difference Between IPsec Tunnel Mode and IPsec Transport Mode?



In IPsec **tunnel mode**, two dedicated **routers** create a virtual "**tunnel**" through a public network. The original **IP header**, including the **final destination**, is **encrypted** along with the packet **payload**. IPsec **adds** a **new IP header** to guide the packets through **intermediary routers**, which are **decrypted** at each end of the tunnel for delivery to their destinations.

In **transport mode**, the payload of each packet is **encrypted**, but the **original IP** header is not. Intermediary **routers** are thus able to view the **final destination** of **each packet** — unless a separate **tunneling protocol** is used.

What is IPsec? | How IPsec VPNs work | Cloudflare

IPsec Services

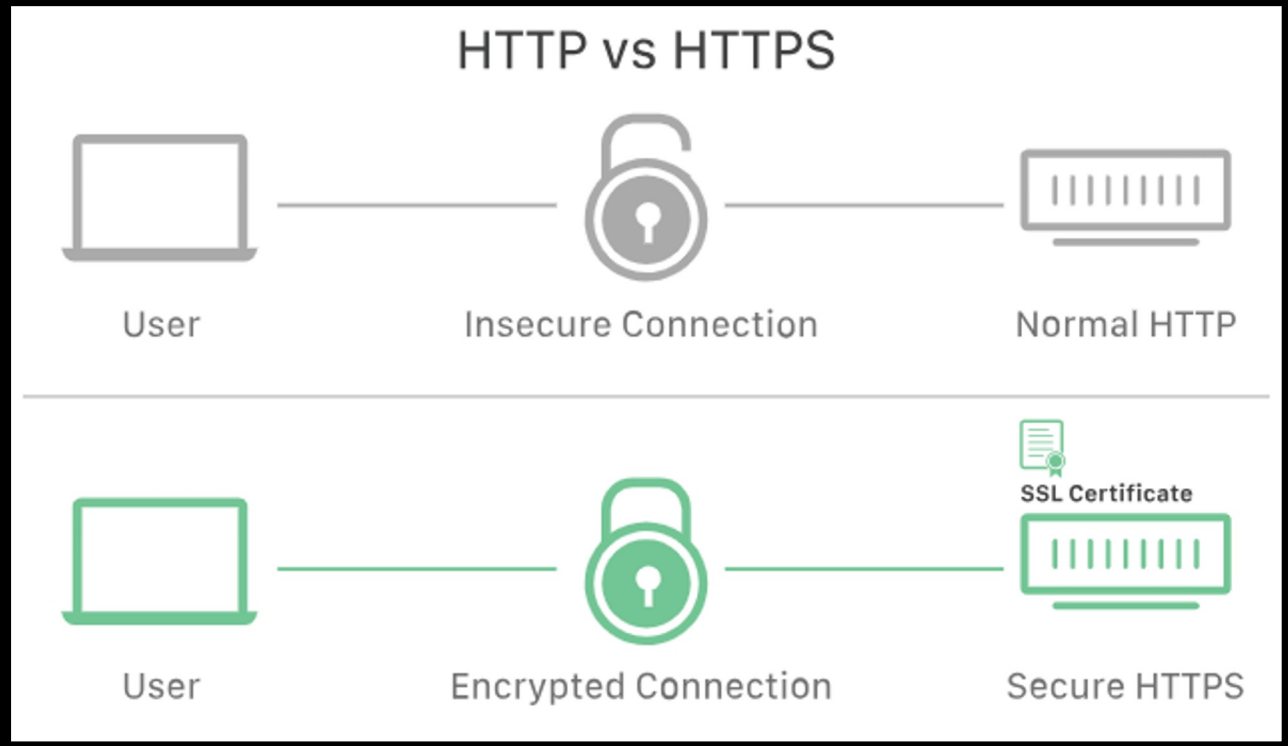
- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
  - a form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality

Applications of IPSec

- IPsec **ensures secure** communication over **LANs**, **private,** and **public** WANs, and the Internet:
  - **Secure branch office connectivity over the Internet**: allows **companies** to establish **secure virtual private networks** (VPNs) over the **Internet** or public WANs. This **reduces** reliance on **private** networks, leading to **cost savings** and **decreased** network management overhead.
  - **Secure remote access over the Internet**: allows **end users** to access their **company's network securely** via a local call to an ISP, **reducing** toll **charges** for traveling employees and telecommuters.
  - **Establishing extranet and intranet connectivity with partners**: enables **secure communication** with external **organizations** by **ensuring authentication** and **confidentiality** and providing a key **exchange mechanism**.
  - **Enhancing electronic commerce security**: **enhances security** even in **applications** with **built-in protocols**. IPsec **ensures** all designated traffic is **encrypted** and **authenticated**, adding an **extra layer** of security beyond the **application** layer.

SSL

SSL, or **Secure Sockets Layer**, is an **encryption** protocol **developed** by **Netscape in 1995** to secure **Internet communications**. It ensures **privacy**, **authentication**, and **data integrity**. SSL evolved into **TLS**, but websites using **SSL/TLS** display "**HTTPS**" in their URL instead of "**HTTP**."



Source: Cloudflare

What is SSL (Secure Sockets Layer)? | Cloudflare

Homework: Comparing HTTP and HTTPS with a Focus on SSL/TLS Importance

PRACTICAL TASK

Objective: To enhance your practical skills, it is crucial to engage in hands-on work. The aim of this exercise is to simulate real-world network interactions, compare the security of HTTP with that of HTTPS, and understand why SSL/TLS is essential.

Guidelines: Follow the steps below to set up a controlled, simulation-based lab environment using virtual machines (victims and an attacker). This setup will enable you to perform a Man-in-the-Middle (MitM) attack and capture all data transmitted from the victim machine in a safe and isolated setting.

1. Use the GNS3 network simulator to create a topology with a node (victim machine) and a Kali Linux machine acting as the attacker.

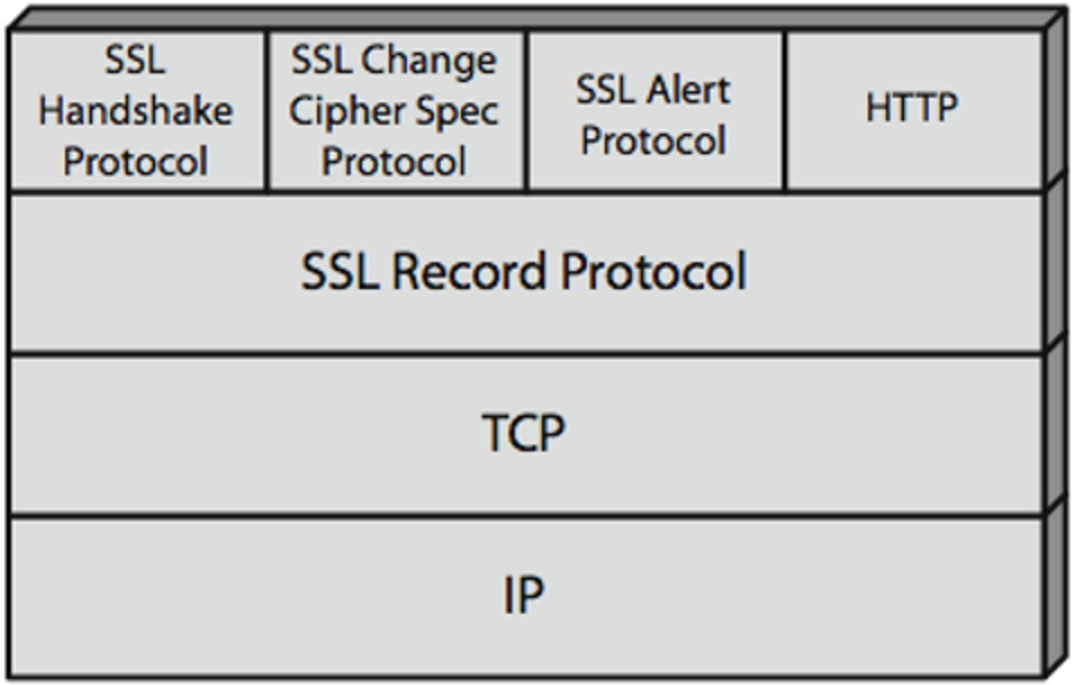
2. Ensure you install these machines on your preferred virtual machine software and integrate them with the GNS3 server.

3. Ensure the installation of the Bettercap tool on your Kali Linux.

Task: Use Bettercap to simulate a Man-in-the-Middle (MitM) attack. Once the attacker is successfully positioned in the middle of the traffic from the victim device, start sniffing all packets transmitting from that device. Test this on the victim machine by visiting an HTTP website. It is required to use a website developed solely for the educational purpose of describing security breaches; therefore, we require using vulnweb. Use any related web application on this website to provide a **username** and **password**, then check the collection of these credentials from the attacker's side. Report the results and show how all the target credentials are now available to the attacker.

SSL Architecture

- The **SSL Record Protocol** provides basic security services to various higher-layer protocols.
- In particular, the Hypertext Transfer Protocol (**HTTP**), which provides the **transfer service** for Web **client/server interaction**, can operate on top of **SSL**.
- Three higher-layer protocols are also defined as part of SSL: the **Handshake Protocol**, **Change Cipher Spec Protocol**, and **Alert Protocol**. These SSL-specific protocols are used in the management of **SSL exchanges**.



SSL Architecture

Two important SSL concepts are the SSL connection and the SSL session:

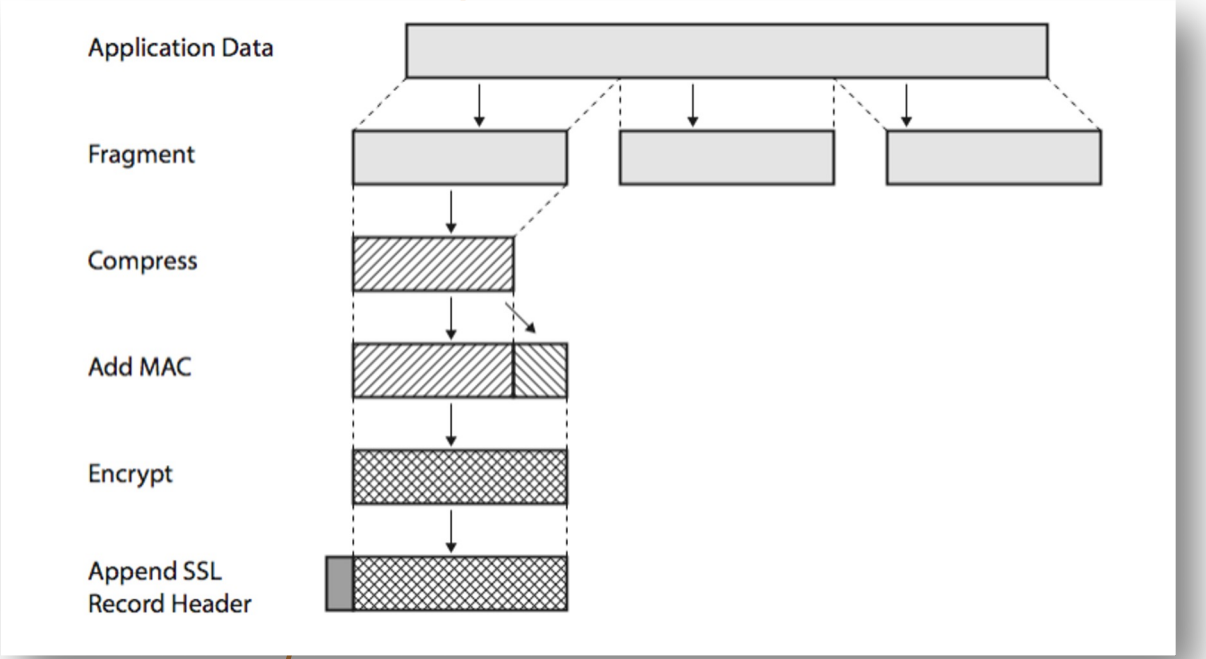
Connection: A connection is a network transport that **provides** a suitable type of **service**, such connections are **transient**, **peer-to-peer relationships**, associated with **one session**

Session: An SSL session is an association between a **client** and a **server**, created by the **Handshake Protocol**. Sessions define a set of **cryptographic** security **parameters**, which can be shared among multiple **connections**. **Sessions** are used to avoid the expensive negotiation of new security parameters for each connection.

- Between any pair of parties (applications such as **HTTP** on **client** and **server**), there may be multiple **secure connections**.
- In theory, there may also be multiple simultaneous **sessions** between parties, but this feature is **not used in practice**.

SSL Record Protocol

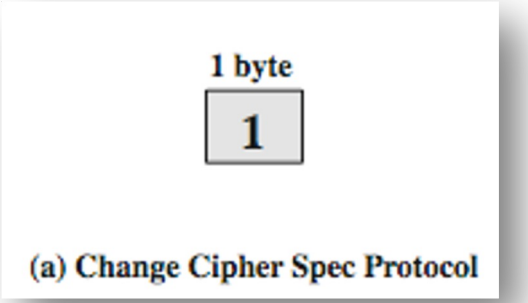
- **SSL Record Protocol defines** two services for SSL connections:
  - **Confidentiality**: The Handshake Protocol defines a **shared secret key** that is used for conventional encryption of **SSL payloads**. The message is compressed before being concatenated with the MAC and encrypted, with a range of ciphers being supported as shown.
  - **Message Integrity**: The **Handshake Protocol** also defines a shared secret key that is used to form a **message authentication code** (**MAC**).



SSL Record Protocol's process: fragmenting application **messages**, optionally **compressing data**, **appending** a **MAC** for **integrity**, **encrypting**, **adding** a header with SSL details, and transmitting in TCP segments. Upon receipt, data is decrypted, verified, decompressed, and delivered to higher-layer applications.

SSL Change Cipher Spec Protocol

- The **Change Cipher Spec Protocol** is one of the **three** SSL-specific protocols that use the **SSL Record Protocol**, and it is the **simplest**, **consisting** of a **single message**, which consists of a **single** byte with the **value 1.**
- The sole **purpose** of this message is to cause the **pending** state to be copied into the **current** state, which updates the cipher suite to be used on this **connection**.



(a) Change Cipher Spec Protocol

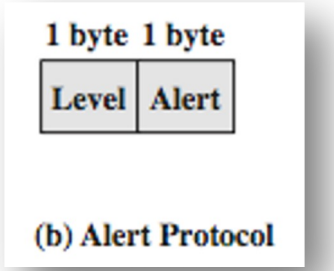
SSL Alert Protocol

The **Alert Protocol** is used to convey **SSL-related** alerts to the peer entity.

As with other applications that use **SSL**, **alert messages** are **compressed** and **encrypted**, as specified by the current state.

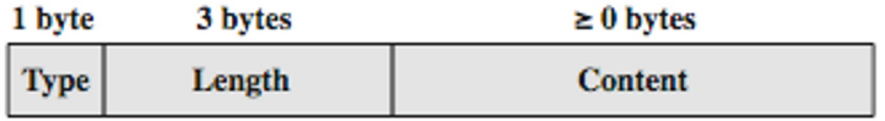
Each message in this protocol consists of two bytes the first takes the **value warning**(**1**) or **fatal**(**2**) to convey the severity of the message.

The **second** byte **contains** a code that indicates the specific alert. The first group shown are the fatal alerts, the others are **warnings**.



(b) Alert Protocol

SSL Handshake Protocol



(c) Handshake Protocol

- The most **complex part of SSL** is the Handshake Protocol.
- This protocol **allows** the **server** and **client** to authenticate each other and to **negotiate** an **encryption** and **MAC** algorithm and **cryptographic** keys to be used to **protect data** sent in an SSL record.
- The **Handshake** Protocol is used before any application data is transmitted.
- The Handshake Protocol consists of a series of **messages** exchanged by **client** and **server**, which have the format and which can be viewed in **4 phases**.

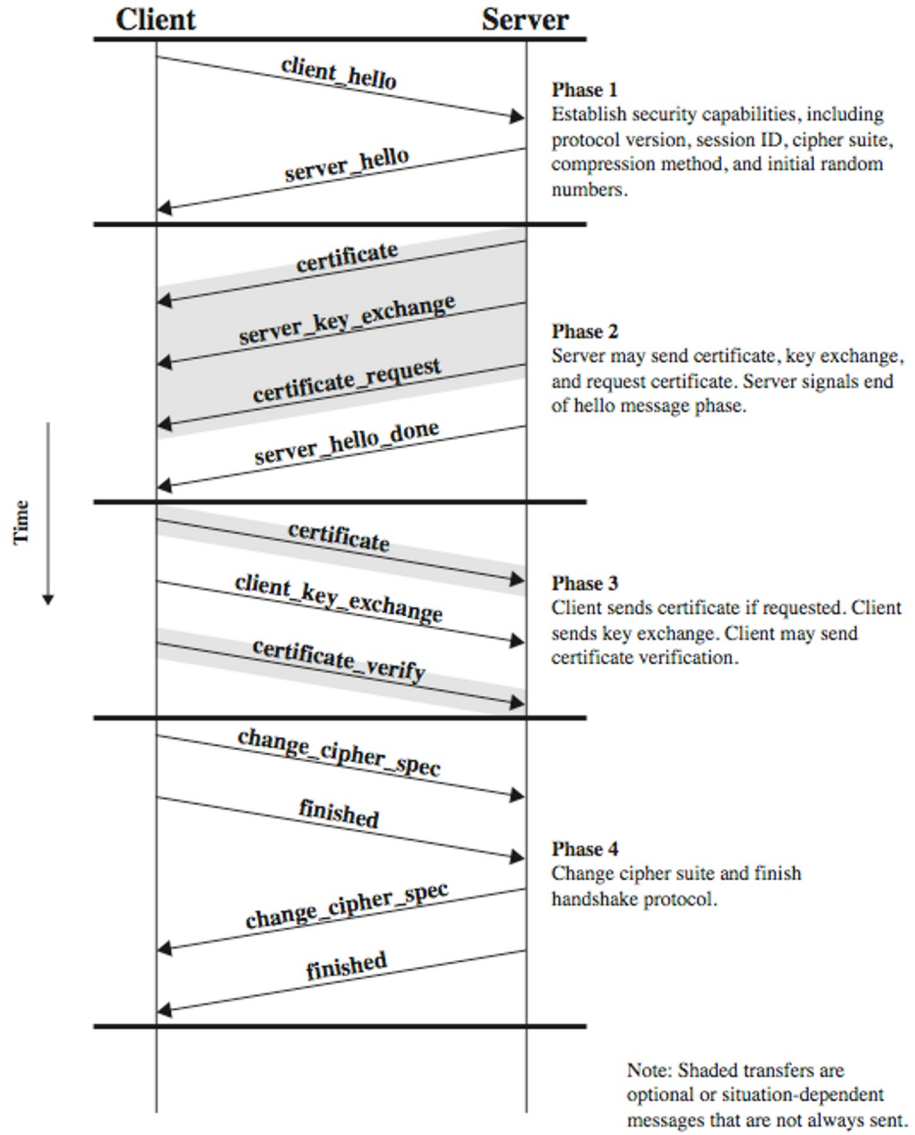
SSL Handshake Protocol

Phase 1. Establish Security Capabilities - this phrase is used by the client to **initiate** a logical **connection** (sending **Client_hello**) and to establish the **security capabilities** that will be associated with it

Phase 2. Server Authentication and Key Exchange - the server **begins** this phase by **sending** its **certificate** if it needs to be **authenticated**.

Phase 3. Client Authentication and Key Exchange - the client should **verify** that the **server** provided a **valid certificate** if required and check that the **server_hello** parameters are acceptable

Phase 4. Finish - this phase completes the setting up of a **secure connection**. The client **sends** a **change_cipher_spec** message and copies the pending CipherSpec into the current **CipherSpec**. At this point, the **handshake** is complete, and the **client** and **server** may begin to exchange application layer data.



TLS

- TLS is a security protocol that provides privacy and data integrity for Internet communications.
- The essential use case for **TLS** is to **encrypt** traffic between **web applications** and **servers**.
- It was **proposed** by the **Internet Engineering Task Force** (**IETF**), and the first version of the protocol was published in **1999**.
- **The most recent version is TLS 1.3, which was published in 2018.**

What is Transport Layer Security (TLS)? | Cloudflare

What is the difference between TLS and SSL?

- **Origin of TLS**: TLS evolved from **Secure Sockets Layer** (**SSL**), initially developed by Netscape.
- Development Transition: TLS **version 1.0** started as SSL **version 3.1**.
- **Usage of Terms**: Despite the distinction, the terms **TLS** and **SSL** are often used **interchangeably** due to their **historical connection**.

What is Transport Layer Security (TLS)? | Cloudflare

Why is SSL/TLS important?

Originally, **web data** was **transmitted** in plaintext, making it **vulnerable** to interception. For example, when **entering credit** card **Internet unencrypted**information on a **shopping website**, the data traveled across the.

SSL was **developed** to maintain **user privacy** by **encrypting** data transmitted between **users** and **web servers**. This **encryption** ensures that **intercepted** data **appears scrambled** to **unauthorized parties**, **safeguarding sensitive** information such as **credit card numbers**.

SSL prevents **cyber attacks** by authenticating **web servers**, thwarting attempts by attackers to **create fake websites** and **steal data**. Additionally, it **prevents** tampering with **data during transit**, **acting as a safeguard.**

What is SSL (Secure Sockets Layer)? | Cloudflare

Homework: Redirecting Victim Traffic to a Counterfeit Webpage (DNS Spoofing)

PRACTICAL TASK

Objective: To enhance your practical skills, it is crucial to engage in hands-on work. The aim of this exercise is to simulate real-world network interactions, create a counterfeit webpage, and redirect the victim's traffic to open this page when the user visits a particular website.

Guidelines: Follow the steps below to set up a controlled, simulation-based lab environment using virtual machines (a victim and an attacker). This setup will enable you to perform a Man-in-the-Middle (MitM) attack and ensure that users always encounter a fake webpage when they visit a webpage.

1. Use the GNS3 network simulator to create a topology with a node (victim machine) and a Kali Linux machine acting as the attacker.

2. Ensure you install these machines on your preferred virtual machine software and integrate them with the GNS3 server.

3. Ensure the installation of the Bettercap tool and the Apache server on your Kali Linux.

Task: Use Bettercap to simulate a Man-in-the-Middle (MitM) attack. Once the attacker is successfully positioned in the middle of the traffic from the victim, all packets transmitted from that device will be intercepted. Create a counterfeit web page; on the right side, you will find very simple HTML code for this purpose. This fake page should be displayed on the victim's machine whenever the user visits a particular webpage. Furthermore, it is required to use a website developed solely for the educational purpose of describing security breaches; So, we require the use of vulnweb. Utilize any related web application on this website to make the fake page appear on the victim's device. Report the results and demonstrate how all traffic is consistently redirected whenever the user visits that webpage.

You may use this simple HTML code

```
<!DOCTYPE html>
<html>
<body>

<h1>My Fake Page</h1>


</body>
</html>
```

What is an SSL certificate?

- SSL, **requires an SSL certificate**, also known as a **TLS certificate**.
- The **SSL certificate** functions as proof of a **website's identity**, similar to an **identification card**.

- Stored on the **server**, the certificate contains crucial information, including the **website's public key**, facilitating **encryption** and **authentication**.

- When a user's device **connects** to the **website**, it utilizes the **public key** to establish **secure encryption** keys.

- **Simultaneously**, the **website's server** holds a **private key** used to **decrypt data encrypted** with the **public key**.

- **Certificate authorities** (**CA**) are entities tasked with issuing **SSL certificates**.

What is SSL (Secure Sockets Layer)? | Cloudflare

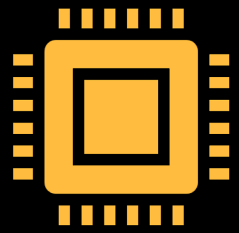
What are the types of SSL certificates?

- There are several different types of **SSL certificates**:
  - **Single-domain SSL certificates** are designated for individual domains, like **www.example.com**
  - **Wildcard SSL certificates** cover a **domain** and its **subdomains**. For example, www.example.com and blog.example.com, developers.example.com, etc.
  - **Multi-domain SSL** certificates extend coverage to multiple unrelated domains.
- **SSL certificates** are classified into different **validation levels**, which are considered as **background checks**, and each level **changes according** to the comprehensiveness of the checking process.
  - **Domain Validation** involves proving **domain control** and is the least stringent and **most affordable**.
  - **Organization Validation** requires direct **contact** between the **Certificate Authority** (**CA**) and the **requester**, **enhancing user trust**.
  - **Extended Validation** entails a **comprehensive organization** background check before **certificate issuance**, offering the **highest level of assurance**.

What is SSL (Secure Sockets Layer)? | Cloudflare

How does SSL/TLS work?

SSL encrypts data transmitted over the web, making it **unreadable** to unauthorized **interceptors**, thus enhancing privacy protection.



SSL starts an **authentication procedure** known as a **handshake** between two **communicating** devices to verify that both **devices** are indeed who they claim to be.

SSL additionally utilizes digital **signatures** to ensure data **integrity**, confirming that the **data remains** unaltered prior to **reaching** its designated recipient.

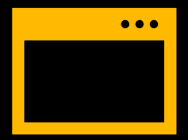
What is SSL (Secure Sockets Layer)? | Cloudflare

Web Security

- The World Wide Web (WWW) is extensively used by **businesses**, **government** agencies, and **individuals**.
- The Internet and the Web are extremely **vulnerable** to **compromises** of various sorts, with a range of threats

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	• Cryptographic checksums
Confidentiality	• Eavesdropping on the Net Net • Theft of info from server Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	• Encryption, web proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	• Difficult to prevent
Authentication	Impersonation of legitimate users Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques

Web Security



The Internet and the Web are susceptible to various compromises, including passive and active attacks.

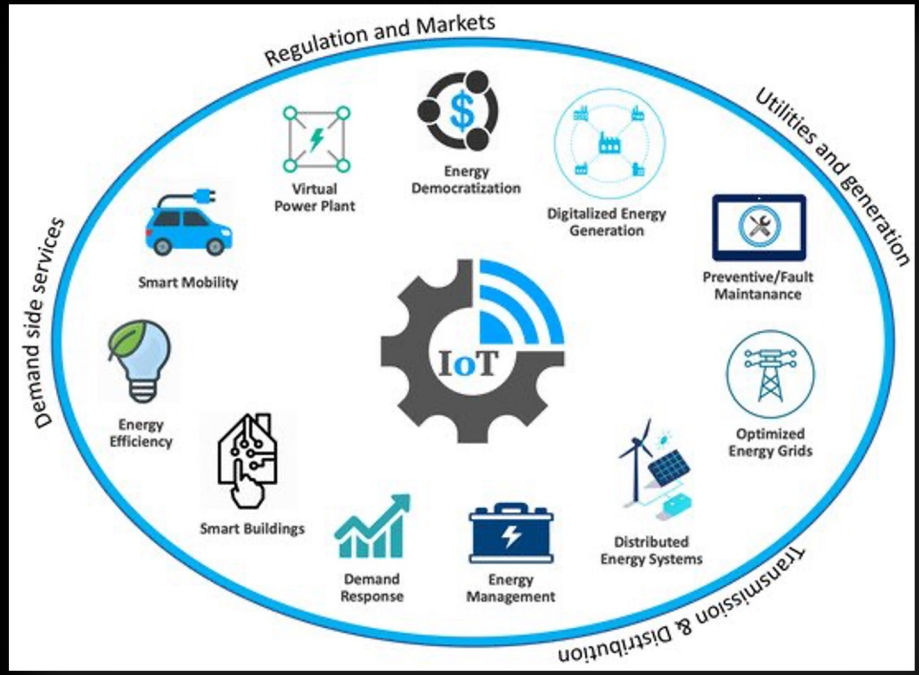
Passive attacks involve eavesdropping on network traffic and accessing restricted information on a website.

Active attacks include impersonation, message alteration in transit, and modifying information on a website.

Additional security mechanisms are necessary to mitigate these threats on the web.

Internet of Things (IoT) for Energy Sector

- Advanced technologies like the **Internet of Things** (IoT) have numerous applications in the **energy sector**, including **energy supply**, **transmission**, **distribution**, and **demand management**.
- IoT can be **utilized** to enhance energy **efficiency**, boost the share of **renewable energy**, and minimize the environmental footprint associated with energy consumption.
- Different parts of such an **integrated** smart energy system are depicted.



Source: IoT and the Energy Sector | Encyclopedia MDPI

IoT and the Energy Sector | Encyclopedia MDPI

SSL/TLS for the IoT

- Manufacturers and vendors of **Internet-connected smart devices** must prioritize security due to society's growing **reliance** on their products and awareness of vulnerabilities.
- A **crucial measure** for IoT businesses is to implement **trusted SSL/TLS certificates** for authentication and encryption on their devices.
- IoT Hub uses **Transport Layer Security (TLS)** to secure **connections** from IoT devices and services.
- **SSL/TLS employs** asymmetric encryption to secure Internet data exchange between **two computers**.
- It verifies the **identities** of the **server** and/or **client**.
- Typically, an **HTTPS** server offers the **visitor's browser** a certificate signed by a **trusted CA** like **SSL.com**.

Azure IoT Hub TLS support | Microsoft Learn
Securing the Internet of Things (IoT) with SSL/TLS - SSL.com

Connect with CyberSecPro:
How to register and other practical information

1. Website:
   www.cybersecpro-project.eu
2. X (Twitter):
   https://twitter.com/CyberSecPro_eu
3. LinkedIn:
   https://www.linkedin.com/company/cybersecpro-euproject/

Thank you

Please send all questions to:
Stefan Schauer
Stefan.Schauer@ait.ac.at
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at