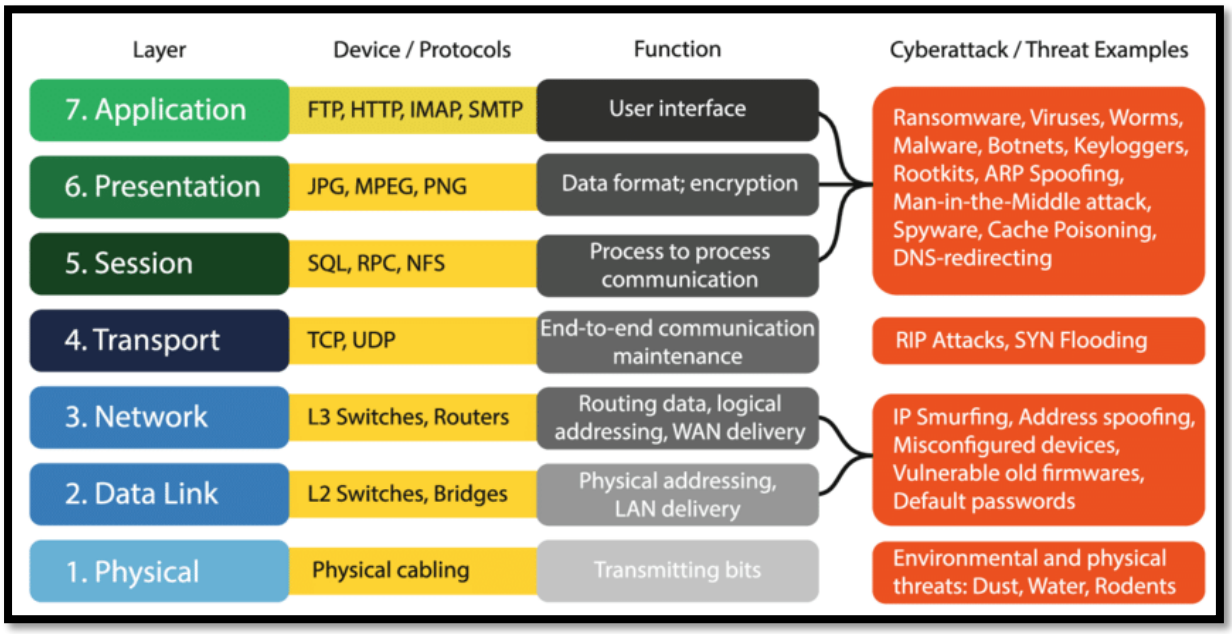
MINOR PROJECT

ATTACKS ON THE OSI MODEL, THEIR IMPACT AND MITIGATION STRATEGIES

INTRODUCTION

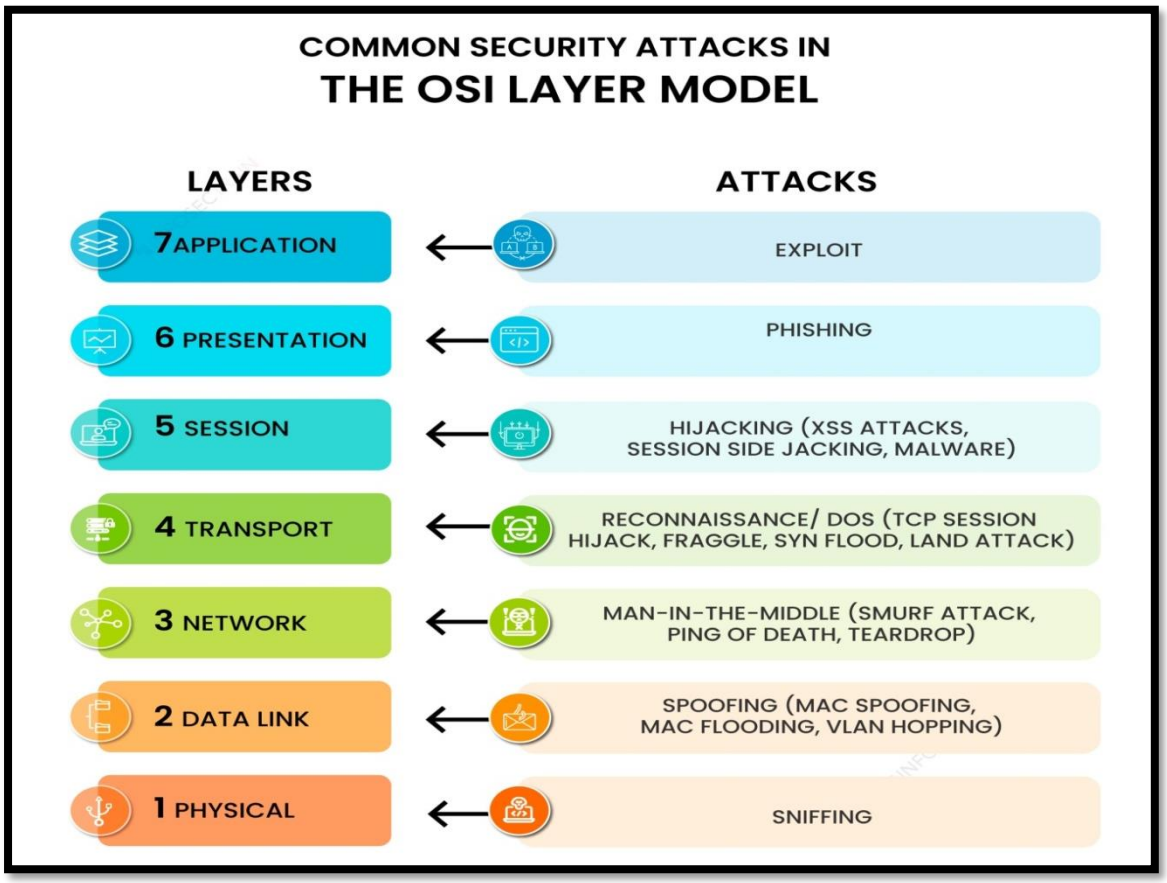
The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard Protocols. The OSI provides a standard for different computer systems to be able to communicate with each other. The OSI (Open Systems Interconnection) model is a framework for describing a networking system's functionality. The OSI model classifies the computing functions of the various network segments, specifying the rules and requirements necessary to ensure the network's software and hardware interconnection.

The OSI Model can be seen as a universal language for computer networking. It is based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.



Each layer of the OSI Model handles a specific job and communicates with the layers above and below itself. DDOS attacks target specific layers of a network connection; application layer attacks target layer 7 and protocol layer attacks target layers 3 and 4.

7 Layers of the OSI Model and Common Security Attacks in Each Layer



1. Application layer

The application layer is the closest to users in the OSI layer model and establishes the communication between the user and applications with which they interact individually. The common security attack on this layer is an exploit.

Attack: Exploit

Exploit means taking advantage of a software vulnerability. An exploit in the application layer refers to a type of cyber-attack that targets vulnerabilities in software applications. These attacks take advantage of bugs or weaknesses in the code of the application to gain unauthorized access or perform malicious actions. This indicates that the target of an attack

includes a software vulnerability that allows attackers to build the means to access and exploit it. Without employing an exploit, attackers can take down a website or important system by using DoS (Denial-of-Service) or DDoS (Distributed Denial-of-Service) cyberattacks. Many exploits are designed to enable super user-level access to a victim system.

2. Presentation layer

The presentation layer specifies the two devices' encoding, encryption, and compression methods for proper communication. Anything sent from the application layer is received by the presentation layer, which is transformed into a format suitable for transmission via the session layer. Phishing is one of the common security attacks carried out by attackers in this layer.

Attack: Phishing attack

Phishing attacks in the presentation layer comprise using social engineering tactics to trick users into providing personal and sensitive information or clicking on a malicious link. This is often done by creating fake websites or email messages that appear to be from a legitimate source. This attack aims to steal sensitive information such as login credentials and credit card information or install malware on the victim's system by disguising the attack as a legitimate request.

3. Session layer

The session layer establishes communication channels between devices, known as sessions. It starts sessions, keeps them open and effective while data is transferred, and closes them after communication is completed. Hijacking is one of the common security attacks that occurs in this layer.

Attack: Hijacking

Hijacking in the session layer occurs when an attacker intercepts and takes control of an established communication session between two parties. This can be carried out by exploiting vulnerabilities in the protocol used to establish the session or using the tools to intercept and manipulate network traffic. Once the attackers hijack the session, they can access sensitive information or gain unauthorized access. There are two types of session hijacking:

- Active session hijacking: In this, the attacker takes control of an active user session on a network and intercepts and alters network traffic in real time.
- Passive session hijacking: In this, attackers monitor network traffic and wait for users to log into a website; at that point, the attackers take over the session.

4. Transport layer

The transport layer performs flow control, transmitting data at a frequency corresponding to the receiving device's connection speed and error control, determining whether data was received wrongly and requesting it if necessary. The most common security attack that is carried out in this layer is reconnaissance.

Attack: Reconnaissance

A reconnaissance attack in the transport layer typically involves an attacker attempting to gather information about a target system or network by actively probing the transport layer protocols, such as TCP or UDP. This can include techniques such as port scanning, which involves sending messages to various ports on the target system to determine which ports are open and potentially vulnerable to attack. Additionally, an attacker may use tools such as packet sniffers to capture and monitor network traffic to gather information.

5. Network layer

There are two primary jobs that the network layer does. One breaks up the segments into network packets and then puts the packets back together at the other end. The other is sending packets through a physical network by finding the best route. One of the most common security attacks in this layer is a man-in-the-middle attack.

Attack: Man-in-the-Middle (MITM) attack

In the network layer, a man-in-the-middle attack occurs when an attacker intercepts and modifies communication between two parties without their knowledge. The attackers become a man in the middle of the communication, able to read, modify, or inject new information into the communication. Attackers also intercept and alter communication by manipulating the routing of packets between the two sources. This can be done by using a technique such as ARP spoofing, where attackers send fake ARP messages to a target system, tricking it into sending packets to the attacker's device instead of the intended source.

6. Data link layer

The data link layer establishes and terminates communication between two technically connected network nodes. It divides packets into frames and transmits them from source to destination. In this layer, attackers use spoofing attacks to target the network system.

Attack: Spoofing attack

A spoofing attack in the data link layer occurs when an attacker alters a device's Media Access Control (MAC) address to impersonate another device in the network. This can allow the attackers to gain access to network resources or intercept and modify network traffic intended for the legitimate source. There are different ways that attackers carry out MAC spoofing.

- Address Resolution Protocol (ARP) spoofing
- DHCP spoofing
- MAC flooding

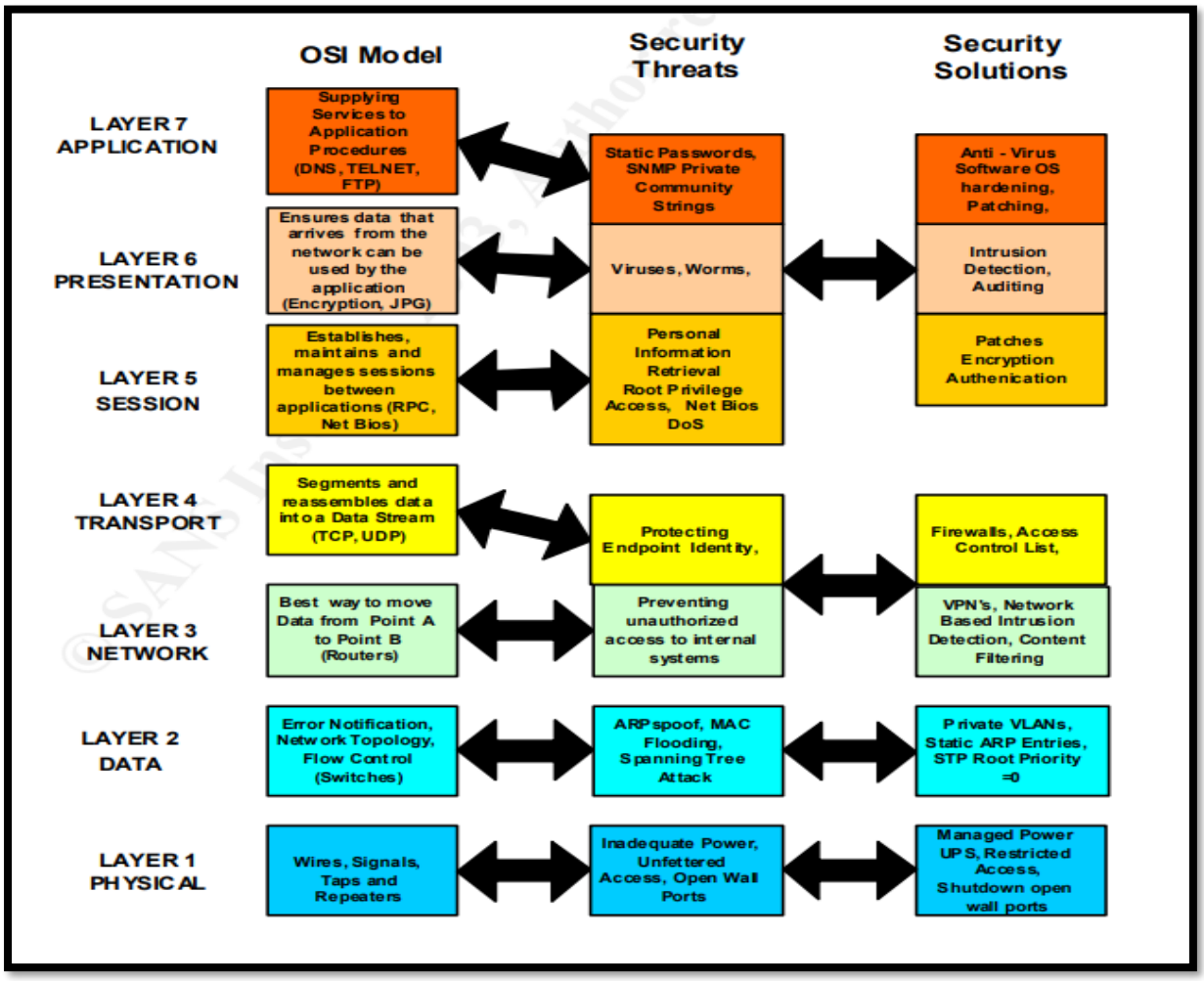
7. Physical layer

The physical layer is responsible for adequately connecting network nodes via wired or wireless means. Sniffing is the most common security attack used by attackers to target the data link layer.

Attack: Sniffing attacks

A sniffing attack in the data link layer occurs when an attacker captures and analyzes network traffic to gather sensitive information. This is done using a packet sniffer tool, which captures and decodes all the packets passing through a particular network segment. Sniffing attacks steal sensitive information such as login details, credit card numbers, and other personal and sensitive information.

Mitigation Strategies:



Real-world case studies:

- **WannaCry ransomware attack**

The WannaCry ransomware attack of May 2017 was one of the most widespread ransomware attacks, exploiting a leaked Windows software vulnerability. It resulted in hundreds of thousands of infections and up to billions of dollars in damages, the impact of which is still felt today.

The attackers, which investigators found to be a North Korean hacker collective called The Lazarus Group, exploited a Windows vulnerability discovered by the United States National Security Agency (NSA). The vulnerability, found in older Windows systems, was leaked by another hacker group called the Shadow Brokers in April 2016. This was only one month after Windows released patches for the exploit, meaning that computers that had yet to update were still left vulnerable

Methodology

The ransomware used an exploit known as Eternal Blue, which was developed by the NSA after discovering a vulnerability in older Windows software. The exploit used the Windows SMB, which can be tricked into remotely executing code by way of packets.

The malware would send an initial packet, known as a dropper, to the device, and it would be executed by the SMB. The next step was unusual — the dropper would attempt to connect to an unregistered domain made of a seemingly random string of numbers and letters, halting the attack if a successful connection was made, and continuing the attack if no connection was established. Security analysts theorize this was put in place to act as a kill switch by the hackers, if they desired to halt an attack from afar.

Once the connection failed, the malware would send two more packets — the encrypter and the decrypter. The dropper could extract and execute the encrypted file, which contained a program that hid and encrypted the victim's files, as well as a set of ransom notes in various, shoddily-translated languages.

The malware used RSA and AES keys for the encryption, making it difficult to decrypt manually within the deadline. Though the decryptor was included within the payload, users that paid the ransom weren't guaranteed to get their files back. Due to bad coding, there was no way to trace the payment to the computer it was made from.

Impact

The WannaCry attack occurred in the span of four days; however, the damage proved to be heavy. Infected systems in over 150 countries resulted in a measly $100,000 payout for the attackers — however, the losses in productivity and erased files are predicted to have reached into the billions.

Businesses lost hundreds of records, and hospitals reported surgery cancellations due to erased patient files. Even more terrifying: Ambulances reportedly rerouted due to the attack, as it affected stored GPS information, possibly resulting in lost lives.

- ## Stuxnet Attack

Stuxnet, the world's first known cyber weapon, not only had technical and political ramifications of using a cybersecurity exploit as a key player in the Iran nuclear negotiations, but more importantly, it cements cyber weapons as a non-trivial defensive and offensive tool in the modern nuclear age.

First discovered in 2010, Stuxnet was a computer worm that exploited a vulnerability in the Siemens software of Iran's nuclear computers, causing their Uranium enrichment centrifuges at the Natanz nuclear enrichment facility to rotate out of control and eventually explode.

Methodology

Consequently, all of Stuxnet's capabilities revolve around its ability to execute a targeted and contained attack on Iran's nuclear computing units specifically. On Iranian nuclear control systems, normal use is as follows. The Siemens Step 7 software is used to program industrial systems, which is transferred to the PLC (Programmable Logic Controller) which runs the centrifuges. In turn, Windows database software is used to store important information about the centrifuge such as including its speed, or notification of potential errors. Stuxnet managed to successfully exploit zero-day, or previously unknown or undiscovered vulnerabilities in the Siemens Step 7 and Microsoft software, to incapacitate the centrifuges while remaining undetected.

Stuxnet uses to gain access to the computer network is through an infected USB drive, and automatically load itself to computers with open file sharing. From there, it used the default password of the Siemens Step 7 to gain access to the database and load itself onto the computer. To propagate to other computers on the network, it was able to infect PLC datafiles and copy itself to the datafile. It also has a peer-to-peer update mechanism to update all instances once one of them gains control at the system level.

The last step of gaining access is to check that the PLC is controlling at least 155 total frequency converters, a little under the known amount of Iranian centrifuge control. This verifies that Stuxnet is specifically targeting the Iranian centrifuges only. Once it loads malicious code to the PLC, it also verifies that the motors are 800Hz-1200Hz as an additional check that it is indeed on the correct centrifuge controller.

Impact

Stuxnet is estimated to have set back the Iran nuclear program by 2 years. Despite Stuxnet, Iran was revealed to be a nuclear state in the mid 2000's. More significantly, however, Stuxnet was proof that cyber attacks could impact the physical world, and be used to damage physical infrastructure. In the age of technology, modern warfare will increasingly rely on cyber weapons like Stuxnet to weaken enemy resources. Additionally, the code of Stuxnet is available on the internet, making it an open source cyber weapon potentially capable of attacking power grids, nuclear plants, or other infrastructure if the source code is accurately altered. Stuxnet makes it extremely clear the need for strong security practices as we move on to an increasingly digital, and increasingly vulnerable world.

Reference:

1. Stuxnet – Dangerous World (ucsc.edu)
2. Common Security Attacks in the OSI Layer Model (infosectrain.com)
3. Case Study: WannaCry Ransomware - SDxCentral
4. The OSI model and cyber attack examples, originally published in... | Download Scientific Diagram (researchgate.net)