TRENDS IN WIRELESS NETWORK SECURITY

Anita C. Eluwa, (M.S. in Cybersecurity)

Department of Computer Science

St. Mary's University San Antonio, TX

celuwa@mail.stmarytx.edu

April 29, 2022

TABLE OF CONTENTS

ABSTRACT

Wireless networks are an integral part of day-to-day life for many people, with businesses and home users relying on them for connectivity and communication. This scholarly research will examine the security vulnerabilities and threats in wireless communications and the background literature. The security requirements of wireless networks including their authenticity, confidentiality, integrity, and availability will be identified and summarized. Different research and surveys have been undertaken by academic researchers on the current trend of wireless security from inception to date. These research findings will be analyzed, and efficient defense mechanisms and countermeasures will be investigated and provided for improving the security of wireless networks.

KEYWORDS: Wireless network, Wireless Security, CIA triad, WLANs, WEP, WPA, WiMAX, WIGig,

1. INTRODUCTION

Wireless networks allow endpoints or devices to connect to the internet without the use of a wire or a cable. They are computer networks that use wireless connections between network devices. Wired technology use wires or cables to transmit data, communicate with devices and connect to the internet but wireless technology uses radio waves for data transmission. These transmissions could be done in four (4) ways: Radio Frequency Transmission, Infrared Transmission, Microwave Transmission, Lightwave Transmission.

Wireless networks follow the protocols from the Open Systems Interconnection (OSI) protocol architecture. Ranging from the application layer, presentation layer, session layer, transport layer, network layer, data link layer and physical layer. Each layer of the OSI model has threats and vulnerabilities found in them and the security requirements implemented are independent of each protocol in the layers. Every security measure implemented satisfies the confidentiality, integrity, and availability of the wireless network. The paper aims to ensure that end-users and customers understand the security threats associated with wireless security and identify the countermeasures that are suitable for each threat found in the network.

The rest of this paper is organized as follows. Section 2 highlights the literature review of past surveys and research on the threats to wireless and network security with the recommended defense mechanisms. Section 3 identifies the security requirements of wireless networks with respect to the confidentiality, integrity, availability, and authenticity. Section 4 gives an analysis of the weaknesses found in 5 layers of the OSI model (physical, datalink, network, transportation, and application) and provides countermeasures for these vulnerabilities. Section 5 explains the types of wireless security protocols used and their features. Finally, section 6 gives a summary of the research essay and provides concluding remarks.

2. LITERATURE REVIEW

2.1 Survey of Current and Future Trends in Security in Wireless Networks (Vikas, 2011).

Vikas Solomon Abel conducted a survey in 2011 of the current and future trends of wireless security. In this survey, he highlights the general attacks on a wireless network. These attacks are divided into four categories: passive attacks, active attacks, man-in-the-middle attacks, and jamming attacks. He then classifies the attacks into the attacks found in most of the layers in the OSI model (physical, link, network, transport, session, application). These attacks will be explained in-depth in the next section of this paper. The future work of this paper suggests that further experimental studies be conducted on identity attacks on the wireless network. No countermeasure was however provided for these attacks.

2.2 A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends (Zou , Jia, Xianbin, & Lajos, 2016).

This paper examines the security vulnerabilities and threats in wireless communications and investigates efficient defense mechanisms for improving the security of wireless networks, with special attention to physical-layer security (Zou , Jia, Xianbin, & Lajos, 2016). This paper also identifies the attacks in the different layers of the OSI model (from the physical to the application layer). Some of the countermeasures provided against the attacks are: Using security protocols and features like BD_ADDR to protect against Bluetooth attacks. WPA2 and WPA3 security protocols to protect against Wi-Fi attacks. Implementing Artificial-Noise-Aided Security and Security-Oriented Beamforming Techniques to prevent eavesdropping (this countermeasure is particular to the eavesdropping threat found in the physical layer). This paper however points out some open challenges in wireless networks to date. The issue of mixed attacks in wireless networks, where multiple attacks such as eavesdropping, and Dos

(Denial-of-service) attacks can affect the network at the same time. The countermeasures provided counters just one attack. Hence, the issue of multiple attacks remains open.

2.3 Wireless Security Issues and their Emerging Trends (Kaur, 2017).

This paper focuses on Wireless LANs (WLANs) and their security issues. The main wireless protocols used in WLAN are WEP, WPA, WPA2, and MSS and these wireless protocols operate on the data link layer and physical layer of the network protocol stack (Kaur, 2017). These protocols however have their weaknesses. One major vulnerability of WEP mentioned in the paper is the size of the initial vector (IV) which is short and often re-used. This then led to the introduction of WPA, WPA2, and MSS in that order. These protocols were introduced to increase the security of the previous one but none of them has been threat free. The weakness of MSS is its difficulty to implement on existing systems which does not stop an attack from happening but rather reduces it. The two important countermeasures for WLAN provided by the author includes WiMAX (Worldwide Interoperability for Microwave Access) which is used for large networks and WiGig (Wireless Gigabit Alliance) which communicates wirelessly for multi-gigabit speeds for network nodes. The vulnerabilities of these technologies are not discussed in this paper but are considered a future work and recommendation.

2.4 5G Security: Current Status and Future Trends (Millar, et al., 2020)

In this paper, the authors present the security landscape of 5G networks, as well as the evolution of requirements and trends in 5G security (Millar, et al., 2020). The fifth generation of mobile telecommunication is relatively new and provides reliability and quality to mobile communication. Before a new generation is introduced, there are security requirements that must be met, and the induction of the security requirement is part of the engineering design process. However, there are still some threats that are targeted at 5G systems. Some of the threats highlighted are eavesdropping, physical attacks, outages, failures or malfunctions and

legal threats. The authors explain that one way to curb these threats is to ensure that the validation of the security requirement is accurate before being implemented. The authors also highlight some of the future trends and technologies that have motivated the deployment of 5G networks. Such as AI & ML (Artificial Intelligence & Machine Learning), Automation and Zero-touch Service Management, Dynamic Liability and Root Cause Analysis, and Trusted Execution Environments. The countermeasures to mitigate the potential attacks in 5G networks are recommended for future work.

2.5 Security Requirements and Challenges of 6G Technologies and Applications (Abdel Hakeem, Hussein, & HyungWon, 2022).

The previous paper by (Millar, et al., 2020) explained the introduction of the 5G network and the security challenges associated with it. This paper is focused on the future of 6G wireless network technology that is projected to be implemented by 2030. Research shows that the 6G network will offer a significant experience for everyone by enabling hyper-connectivity between people and everything and it is also expected to extend mobile communication possibilities where earlier generations could not have developed (Abdel Hakeem, Hussein, & HyungWon , 2022). The authors explain that different potential technologies will be used to implement the 6G networks. Some of these technologies include artificial intelligence and machine learning (AI&ML), post-quantum cryptography, visible light communication (VLC), enhanced edge computing, and distributed ledger (DL) technologies such as blockchain and molecular communication. However, some security and privacy concerns might be a threat to the 6G network. Research confirms that the current security measures such as IPsec and firewalls will not have the capability of protecting the network from intruders. The zero-trust architecture (ZTA) is proposed to be the best security measure for the network. The future work of this paper has the intention of investigating in-

depth the different attacks on the 6G network and solutions will need to be researched in the future.

3. SECURITY REQUIREMENTS OF WIRELESS NETWORKS

This section explains the security requirements of a wireless network. The first thing that needs to be understood is the concept of wireless security. In layman's terms, wireless security is the protection of wireless networks from intruders or unauthorized entities. It ensures that the network and data transmission and communication are safe and only accessible to the user. The purpose of wireless security is aimed at ensuring that the CIA (Confidentiality, Integrity, and Availability) security triad requirement is met. In security, confidentiality ensures that the data transmission and communication are only accessible to an authorized user. Integrity ensures that the data is accurate and not modified in any way. Availability ensures that the data or network is available and accessible at any time only for authorized users. Wireless communications or networks should satisfy the requirements of the CIA. There are also some extra requirements such as Authenticity and Accountability (CIAAA). In wireless networks, authenticity is also a major requirement.

3.1 Confidentiality

To achieve confidentiality, the network is encrypted. Encryption is the process of converting a plaintext (which could be the original data being transmitted) to a ciphertext (unreadable by the attacker). This can be done in two ways: symmetric or asymmetric. For example, in symmetric encryption, a secret key is shared between the sender and the receiver (the destination). The encryption uses an algorithm and a key to convert the data to ciphertext and the receiver then uses the same key to decrypt the message when it gets to the destination. This way, the attacker does not know the secret key and is unable to see the data being

transmitted or sniff the data. The physical layer security provides the means of protecting the confidentiality of wireless networks. This will be explained further in section 4.

3.2 Integrity

The transmission and communication of information on a wireless network should be reliable and accurate. This is where integrity comes into play. There should not be any form of modification or alteration of the data by an attacker or an unauthorized user. This is one of the reasons why access control and the concept of least privilege are very important. This helps reduce the number of authorized entities that can access the information and the wireless network. It prevents unnecessary access to the server room and other sensitive assets available.

3.3 Availability

A wireless network should be accessed by authorized users at any time requested. Availability ensures that this is done appropriately. Failure to access a wireless network can lead to denial service where authorized parties will be unable to access the wireless network. Hence, unable to work and meet deadlines. This can also lead to loss of data. The violation of this is called a denial-of-service (DOS). This is a very common attack that unauthorized users use to get access to a wireless network. They can also cause interferences that are used to disrupt the communication between the user and the network. This is called a jamming attack. Jamming attack is peculiar to the physical layer of the OSI model. These attacks will be explained further in the next section.

3.4 Authenticity

Authenticity ensures that the true network node is identified and confirmed. It distinguishes the authorized users from the unauthorized users. In wireless networks, before a communication link for data transmission is established, mutual authentication must be

performed by the communication nodes. In wireless networks, there are different authentication techniques. There is the MAC (Media Access Control) authentication, network-layer authentication, transport layer authentication, and application-layer authentication. The MAC address is unique to the wireless network interface card that a network node provides. Network-layer authentication requires that the user connecting to the network authenticates himself before establishing a session with the server. This could be done using the user's credentials (username or password). The transport layer uses the TLS (Transport Layer Security) security protocol to provide authentication and encryption. It uses a 4-way handshake protocol that provides connection security and enables the client and server to authenticate themselves before any transmission of data. The application layer authentication ensures that the applications are authenticated, and the websites are also authenticated. This could also be done with the user's credentials.

Wireless networks should be as secure as wired networks. This means that every security requirement of a wired network should be the same as the wireless network. This includes the requirements mentioned above: confidentiality, integrity, availability, and authentication. It is however a bit challenging to achieve the same requirements for wired and wireless because the CIA requirement is faced with threats and vulnerabilities that are not necessarily found in the wired network. Hence, it is important to implement as many security measures as possible and policies that will aid in protecting the network from these attacks. The requirements explained are summarized in the below table.

Security Requirements	**Specific Objectives to be Achieved**
Authenticity	Specified to differentiate authorized users from unauthorized users.

Confidentiality	Specified to limit confidential data access to intended users only.
Integrity	Specified to guarantee the accuracy of the transmitted information without any falsification
Availability	Specified to make sure that the authorized users can access wireless network resources anytime and anywhere upon request.

Table 1: A Summary of Wireless Security Requirements.

4. SECURITY VULNERABILITIES IN WIRELESS NETWORKS

The previous section explained the security requirements of a wireless network. These requirements highlighted earlier should satisfy both wired and wireless networks. Both wired and wireless networks adopt the OSI layer model architecture with each layer consisting of its protocols. These protocols are vulnerable and susceptible to their attacks, and it is more difficult to protect the wireless network from these attacks compared to wired networks. This section presents a review of the various vulnerabilities found in the wireless network. The OSI layer has its unique vulnerabilities because of the protocols that they rely on and these layers (application, transport, network, data link (MAC), physical) will be explained in detail with its existing threat.

Table 2 below shows the OSI layers that will be explained with its existing main protocols. The application layer uses HTTP (Hypertext Transfer Protocol) for the exchange and delivery of web services, FTP (File Transfer Protocol) is used for the exchange of files, and SMTP (Simple Mail Transfer Protocol) is used for email exchange and transmission. In the transport layer, the two main protocols are the TCP and UDP. The TCP (Transmission Control Protocol) is used to establish a connection and provides reliability for data transfer.

TCP also used the 3-way handshake scheme for the transmission of data between the client and server. UDP (User Datagram Protocol) is connection-less oriented, non-reliable and does not use the 3-way handshake scheme for transmission of data. In the network layer, the main protocol found is the IP (Internet Protocol) which is used to deliver packets based on IP addresses. We also have the ICMP (Internet Control Message Protocol) also known as PING which is used for sending error messages that show that a service requested is currently unavailable or cannot be reached. The data link layer also known as the MAC (Media Access Control) layer has different protocols that have been adopted by wireless networks. We have the ethernet, Wi-Fi, and witches. Lastly, the physical layer specifies the data transmission medium, multiplexing, circuit switching, error connection, coding and modulation, and every other channel operation.

OSI Layers	**Main Protocols**
Application	HTTP, FTP, SMTP
Transport	TCP, UDP
Network	IP, ICMP, IPsec
Data Link (MAC)	Ethernet, PPP, IEEE 802.11 (Wi-Fi), switches
Physical	Transmission Medium (copper, optical cable), Coding and Modulation

Table 2: Wireless OSI Layers and Main Protocols

The main protocols that every layer in the OSI model relies on has been highlighted. The potential attacks found in each layer and countermeasures against these attacks will now be summarized.

4.1 Physical Layer Attacks

The physical layer is the first layer in the OSI protocol architecture, and it provides the electrical and physical transmission of signals. The physical layer is prone to a couple of vulnerabilities. Physical destruction of the physical assets (cables, fiberoptics), physical theft of data, and unauthorized network access. Because of the physical layer characteristics, it is also vulnerable to eavesdropping and jamming attacks. Eavesdropping also known as sniffing occurs when an attacker (unauthorized user) attempts to intercept the transmission of data between two users (sender and the receiver). With this, the attacker can read the data being transmitted and use the data for illegal purposes. Jamming occurs when radio frequencies interfere with the data communication and operations of the wireless network. This can be done intentionally or unintentionally. When it is done unintentionally, a cordless phone might be placed close to a microwave or a router and the signal transmitted will interfere with the wireless network and cause a jam. An intentional jam occurs when the attacker analyzes the wireless network spectrum and transmits a signal that interferes with the communication on the discovered frequencies. This then leads to a denial of service of the device and the network.

4.11 Countermeasures Against the Physical Layer Attacks

Some of the attacks on the physical layer include physical destruction of cables, physical theft of data, eavesdropping, and jamming. There are countermeasures to prevent these attacks from happening. To prevent the physical destruction of cables, the best mitigation technique is to protect the cabling and wires from foot traffic. Maintenance and regular checks of the equipment and cables. To prevent physical theft of data, the best mitigation technique is to have a secure location where the physical devices will be located and ensure that there is restricted access to the location. To prevent eavesdropping, encryption is needed. This prevents the attacker from reading the original content of the data. To do that, they'll need to have the

key which is only known to the sender and receiver. Using a virtual private network (VPN) is also recommended mostly when using a public network. A VPN allows users to share information across a public network without making the content of the data public. It will provide online privacy and prevent eavesdropping. To prevent jamming, intrusion detection systems are recommended because they detect jamming attacks instantly. Frequency-Hopping Spread Spectrum (FHSS) minimizes unauthorized interception and jamming of radio transmission by switching a carrier among frequency channels using a shared algorithm that is known to the transmitter and the receiver. Direct Sequence Spread Spectrum (DSSS) multiplies the data that is transmitted, and a Pseudo-Noise (PN) digital signal and the processing makes it difficult for an attacker to descramble the transmitted data to recover the original signal. Table 3 shows a summary of the physical layer attacks and their countermeasures.

Physical Layer Attacks	**Countermeasures**
Physical destruction of cables and wiring	Protect cabling and wires from foot traffic, maintenance of wires and cabling.
Physical theft of data	Implement a secure location for the devices and cables to prevent unauthorized access.
Eavesdropping	Encryption, Virtual Private Network (VPN)
Jamming	Intrusion Detection System, FHSS, DSSS

Table 3: Summary of the Physical Layer Attacks and Countermeasures.

4.2 Data Link Layer (MAC) Attacks

The data link layer is the second layer of the OSI architecture and is responsible for ensuring a reliable point to point multipoint connections in a network. It handles the transfer of data from a physical link in a network. It is also responsible for data frame detection, and error control. In the MAC layer, every network node has a Network Interface Card (NIC). This

NIC provides a connection that is dedicated and strong to a network. It also works with the physical layer by implementing the necessary physical layer devices that are used to communicate with the ethernet or Wi-Fi. The NIC has MAC addresses that are included in the headers when transmitting data and used as a means of user authentication. The most common attack in this layer is called MAC spoofing. This is a primary technique of MAC attacks and occurs when an attacker attempts to change its assigned MAC address with a malicious intention (Nagarajan & Huang, 2010). Another attack particular to the link layer is identity theft. This happens when an attacker steals a legitimate MAC address of a node and pretends to be the true owner of the address to gain access to sensitive data of the node. The third attack that the link-layer faces is the man in the middle attack (MITM). This is when an attacker attempts to intercept the MAC addresses of nodes in communication. This way, the attacker stops the transmission and redirects the communication to the attacker himself rather than the legitimate receiver. Address Resolution Protocol (ARP) spoofing is also very common in the link layer. The ARP is used in IP routing, finds the MAC address, and maintains a table where the MAC addresses are mapped to IP addresses. ARP spoofing is almost like a man-in-the-middle attack where an attacker links his MAC address with the IP address of a legitimate computer. When this happens, the attacker receives any information that is expected to be sent to the legitimate IP address.

4.21 Countermeasures Against the Data Link (MAC) Layer Attacks

To mitigate MAC spoofing, alert-based traffic monitoring tools are highly recommended. These network monitors can help create alerts that detect when the same MAC address is trying to use two IP addresses. An intrusion detection system is also recommended as it helps to monitor abnormal behaviors in the system and gives a warning to the users. One way to prevent identity theft in the MAC layer is by using a whitelist technique that

automatically blocks unknown MAC addresses attempting to transmit data from the Ethernet or switches to the network. MAC filters are also good as they are used to restrict access to the network connection. MITM attacks can be prevented using Public Key Infrastructure (PKI) mutual authentication. PKI uses public-key encryption to protect communication and transmission of data and authenticates the legitimacy of public keys. Mutual authentication ensures that both the sender and the receiver authenticate each other before data is received. In PKI mutual authentication, digital certificates are generated and are used to authenticate the identity of the MAC addresses in communication. This way, an attacker won't have the ability to intercept the data or redirect the transmission to himself. VPNs can also be used to provide a private communication between the sender and the receiver making it difficult for an attacker to intercept. ARP spoofing can be prevented using packet filters. The packet filters inspect the packets in transmission and block packets with conflicting MAC source addresses. There is an ARP spoofing detection software that inspects and certifies the data and addresses before they are transmitted. Table 4 shows a summary of the data link layer attacks and their countermeasures.

Data Link (MAC) Layer Attacks	**Countermeasures**
MAC Spoofing	Alert-based traffic monitoring, Intrusion Detection system
Identity theft	Whitelist technique, MAC filters
Man-in-the-middle (MITM) attack	PKI mutual authentication, VPN
ARP Spoofing	Packet filters, ARP spoofing detection software

Table 4: Summary of the Data Link (MAC) Layer Attacks and Countermeasures

4.3 Network Layer Attacks

The main protocol in the network layer is the Internet Protocol (IP), making the IP address prone to various attacks. The goal of the attacks on this layer is to disrupt the path between the source and destination that is chosen from the routing protocols (Ioannou & Vassiliou, 2016). IP spoofing is one major attack on the network layer. Just like the MAC spoofing, IP spoofing occurs when an attacker impersonates a legitimate IP address to pretend to be the legitimate user. The receiver then responds to the forged IP address of the attacker without knowing it. This could potentially lead to a denial of service because the attacker floods the network with forged IP addresses leaving the network paralyzed and unable to use. This kind of attack is called the Smurf attack. To achieve this, the attackers use a program called "smurf" that builds a network packet which appears at the attacked server as it is coming from the trusted IP address (Sula, 2018). The third attack that the network layer faces is called IP hijacking. IP hijacking occurs when an attacker disrupts a session between a client and server. The attacker takes over another legitimate user's IP address and creates a new connection to the network. This then gives him access to the legitimate user's data and confidential information. This is very dangerous because most times the users are unaware of this because they just get disconnected from the network. Ping of Death (PoD) is also a type of DOS attack in the network layer where the attacker sends ICMP (Internet Control Message Protocol) packets continuously that are larger than the maximum packet size allowed without waiting for a response. Thereby flooding the network.

4.31 Countermeasures Against the Network Layer Attacks

There are different ways to prevent IP spoofing. The first method is packet filtering. A packet filter blocks traffic with IP addresses from going through the network. With this, packets coming in and out of the network are monitored and controlled. The second way to prevent IP

spoofing is by using an access control list. This list helps to deny private IP addresses from interacting with the network. Another way of preventing IP spoofing is by implementing authentication mechanisms. This helps to authenticate and validate legitimate users from attackers trying to access the network. It is important to ensure that the switches and routers are configured appropriately. This configuration helps to automatically reject spoofed looking IP addresses trying to send packets into the network. Lastly, encrypting sessions on the router will enable secure communication between the hosts on the network. Smurf attacks can be prevented using firewalls to help monitor and reject packets coming from forged IP addresses. Another way to prevent smurf attacks is to configure the hosts and routers so they avoid responding to ICMP echo requests. IP hijacking can be prevented using a VPN. This will encrypt the data, hide the IP address being used and will prevent an attacker from intercepting the session. Using secure cryptographic protocols like Hypertext Transfer Protocol Secure (HTTPS), Transport Layer Security (TLS) or Secure Socket Layer (SSL) provides encrypted communication between a client and server. Hence, preventing the session from being hijacked. Ping of Death (PoD) can be mitigated by blocking fragmented pings from the device in use. This helps to prevent the packets from exceeding their maximum size. Increasing the memory buffer of the system can also help to prevent PoD from occurring. With this, there is enough space in the memory for ICMP echo requests and responses without flooding the network. Table 5 shows a summary of the network layer attacks and their countermeasures.

Network Layer Attacks	**Countermeasures**
IP Spoofing	Packet filters, Access control lists, Authentication, Changing Router and Switch Configurations, Encryption.
Smurf Attack	Firewalls, Configure hosts and routers,
IP hijacking	VPN, Secure cryptographic protocols like the TLS

Ping of Death (PoD)	Block fragmented pings, Increase memory buffer

Table 5: Summary of the Network Layer Attacks and Countermeasures

4.4 Transport Layer Attacks

The two main protocols in the transport layer are the TCP and UDP. These protocols are susceptible to various attacks. The first attack is called TCP flooding attack also known as ping flooding. It is a type of DoS attack in the transport layer where an attacker sends large numbers of ping requests like the ICMP echo requests to a user. The user then sends ping responses such as ICMP echo replies to the attacker. This process then continues until it floods the buffer of the user's device and blocks the user from sending and responding to ping requests and replies. Another attack that the TCP suffers from is the TCP sequence prediction attack. In this attack, the attacker floods the receiver until a DoS attack happens, after this, the attacker then sends the packet with a correct sequence number to the victim host with the spoofed IP address of his host and this packet can damage the network by asking the victim to run malicious scripts or to execute different commands (Pandey & Saini, 2014). The UDP protocol is also liable to an attack called UDP flooding. This flooding occurs when the attacker sends a high number of UDP packets to the victim's system and waits for responses from the victim. The attacker then continues to flood the system with UDP packets until it crashes the victim's system, and it becomes unreachable or unusable.

4.41 Countermeasures Against the Transport Layer Attacks

Installing an Intrusion Prevention System (IPS) helps to detect anomalous traffic patterns and can be used to prevent TCP flooding. Firewall filtering is a good way to prevent TCP flooding. It prevents malicious packets from flooding the system and unauthorized port scanning. It is also important to install up to date networking equipment that has rate limiting

capabilities. TCP sequence prediction attacks can be prevented by using a firewall or configuring the routers to deny packets from an internal IP address to generate from an external surface. With this, the TCP sequence prediction attack will be prevented from reaching its target. Slowing down ICMP responses can help mitigate UPD flood attacks. This can however have affect the legitimate traffic due to the delay and segregation. Just like the TCP flooding, UDP flooding can also be prevented using firewalls to stop malicious UDP packets from communicating with the network. Table 6 shows a summary of the transport layer attacks and their countermeasures.

Transport Layer Attacks	**Countermeasures**
TCP flooding attack	Intrusion Prevention System (IPS), Firewall filtering, network equipment with limiting capabilities.
TCP Sequence Prediction Attack	Firewall or router configurations,
UDP flooding attacks	Slowing down ICMP responses, Firewalls

Table 6: Summary of the Transport Layer Attacks and Countermeasures

4.5 Application Layer Attacks

The application layer protocols such as HTTP, FTP, and SMTP are prone to specific security attacks. As mentioned earlier in the previous section, HTTP is responsible for the exchange and delivery of web services. The HTTP is prone to malware attacks. These malware attacks include trojan horses, keyloggers, viruses, worms, backdoors, bots, ransomware, etc. Malware is a program or malicious software that is designed to disrupt a service and gain access to unauthorized information. The malware attack in the HTTP protocol exploits the vulnerabilities in the webservers and results in the web servers not being able to retrieve data or content from the user. The second attack the HTTP protocol is prone to is called Structure

Query Language (SQL) injection. This attack occurs when an attacker attempts to inject the application with malicious codes and false SQL statements to gain unauthorized access to legitimate data and websites. SQL injection has five (5) types. The first is the Blind SQL injection. This is when attackers use true or false questions to query a database. The response provided by the database then determines what the answer will be. The second type is called Union-Based SQL injection. This occurs when an attacker uses a UNION SQL operator with two SELECT statements into one single result. The attacker then returns the result as part of the response. The third type is the Boolean-Based SQL injection. This is also used in blind SQL injection where the attacker sends different requests to the database. Each request will have a different condition from the other, then the attacker can tell what the stored data is based on the result. The fourth type is the Error-Based SQL injection. In this attack, the attacker exploits vulnerabilities in the database and uses error messages to return query results and gets access to sensitive data. The fifth type is the Time-Based SQL injection. In this attack, the attacker uses operations that take a while to complete to determine if vulnerabilities are present in the application to enable them to exploit. The third attack on the HTTP protocol is called Cross-site Scripting (XSS). This is also a type of injection and occurs when an attacker injects malicious scripts into legitimate websites. There are three (3) types of XSS. The first is the DOM (Document Object Model) Based XSS. This occurs when an attacker writes without sanitization to the DOM to modify the data by including malicious JavaScript code in the web page. The second type is called Reflected XSS. This is when an attacker tricks a user into clicking on a malicious link, the injected code then moves to the vulnerable website and reflects the attack to the user's browser. The third type is the Stored XSS. This is when a malicious code is stored in the database and can be retrieved by the user without the data being safe enough to be opened on a browser. This is the most dangerous type of XSS.

FTP (File Transfer Protocol) is used for the exchange of files and is prone to an attack called Directory Traversal attack. This is when an attacker exploits any vulnerability in the file names to gain unauthorized access to files that contain confidential information. SMTP (Simple Mail Transfer Protocol) is used for email exchange and transmission. SMTP is prone to different attacks such as phishing, email spoofing, and password sniffing. Phishing is when an attacker sends a malicious email with the purpose of convincing the user to click on a link and reveal sensitive information. Email spoofing is when an attacker poses to be a legitimate source to also trick the user to provide sensitive data. Password sniffing occurs when the attacker sniffs the network traffic and steals the passwords and credentials of the user.

4.51 Countermeasures Against the Application Layer Attacks

To protect against malware attacks on HTTP, network security tools are highly recommended. The use of anti-malware software will help identify and protect the endpoint devices from malware threats. The use of a firewall will monitor the traffic and block malicious traffic from getting into the network. It is important to use SSL/TLS certification for every website. SSL (Secure Socket Layer) is a protocol that is used to provide secure communication between the client and the server. TLS (Transport Layer Security) is a successor of SSL that protects web applications from eavesdropping and alteration. SSL/TLS certification provides authentication and shows that the webserver is trusted and secure. This then uses HTTPS (Hypertext Transfer Protocol Security) instead of just HTTP. SQL injection can be prevented by using prepared statements with parameterized queries, Stored Procedures, allowing all list input to be validated and sanitized. Enforcing the principle of least privilege also reduces the risk of an SQLi because it grants only necessary privileges to the database. There are a few ways to prevent XSS. These include filtering input on arrival, encoding data on output and the use of appropriate response headers. Directory traversal attacks on the FTP can be prevented

by validating the user input before processing. One of the best ways to prevent falling for a phishing email is through end-user training. This goes a long way because once the user knows how to differentiate a phishing email from a legitimate email, then there is a lower or no chance of being a victim of such an attack. Asides from end-user training, there are phishing filters that can be used to filter out phishing emails from our inboxes and move them to the junk or spam folder. Email spoofing can be prevented by using email authentication mechanisms. This helps to prevent attackers from impersonating a domain or pretending to be from a trusted source. Encryption is used to protect against password sniffing. This prevents the attacker from reading the password from the network traffic. Also, the use of a VPN is necessary when communicating on public Wi-Fi. Table 7 shows a summary of the application layer attacks and their countermeasures.

Application Layer Attacks	**Countermeasures**
Malware Attacks	Network Security Tools, Anti-Malware Software, Firewall, SSL/TLS Certification
SQL Injections	The use of Prepared Statements with Parameterized Queries, Stored Procedures, List Input Validation, Principle of Least Privilege
Cross-site Scripting (XSS)	Filter input on arrival, encode data on output, Use appropriate response headers
Directory Traversal Attack	Validate user input before processing
Phishing	End-User Training, Phishing filters
Email Spoofing	Email Authentication
Password Sniffing	Encryption, VPN

Table 7: Summary of the Application Layer Attacks and Countermeasures

This section analyzed five layers of the OSI model architecture along with their protocols. The different attacks found in five (5) layers of the OSI model architecture and the countermeasures to protect against these attacks were provided. Section 5 highlights the different wireless security protocols and their functionalities.

5. WIRELESS NETWORKS SECURITY PROTOCOLS

A wireless Local Area Network (WLAN) is a communication network that provides wireless connections to devices from a local area within a limited geographical area. The IEEE standard for WLAN IS 802.11. There are also different standards of 802.11. There's the 802.11, 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac and 802.11af. The WLAN uses authentication protocols to secure the network. The protocols used are WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), and WPA3 (Wi-Fi Protected Access 3). Let's now highlight the functionalities of these protocols and their strength.

5.1 WEP (Wired Equivalent Privacy)

WEP is the first authentication protocol that is designed to provide security of data. It was introduced in 1997 and was the first attempt to ensure wireless protection. WEP uses a 64 or 128 bit key for encryption using a single key. It uses an RC4 cryptographic algorithm to encrypt and decrypt packets. This achieves confidentiality of data. It uses a cyclic redundancy check (CRC) to achieve integrity. Authentication is achieved with the shared key that is known by the users only. Over time, various vulnerabilities were discovered with the WEP, and its security became very weak. This then led to the introduction of WPA.

5.2 WPA (Wi-Fi Protected Access)

WPA is the second security protocol and a successor of WEP. It was introduced in 2003 after WEP became obsolete. It shares some similarities with WEP with a few differences in its encryption algorithm. It uses a temporal key integrity protocol (TKIP) for more power encryption and the TKIP changes the key dynamically. WPA uses a 128-bit key size for encryption and a Message Integrity Check (MIC) to check for the integrity of the data. WPA has two (2) modes; WPA Personal or Pre-Shared Key (PSK) and WPA-Enterprise. The WPA-PSK is commonly used in home or college environments while the WPA-Enterprise is used for business purposes or an organization. It uses a protocol called Extensible Authentication Protocol (EAP) which is used for authentication. WPA became weak when a passphrase choice weakness was found.

5.3 WPA2 (Wi-Fi Protected Access 2)

WPA2 is an upgraded version of WPA. It was introduced in 2004 and provides higher security than WPA and WEP. It uses two mechanisms: the AES and CCMP for encryption and authentication. AES (Advanced Encryption Standard) is an algorithm that is used for the encryption of data and the CCMP (Counter Mode Cipher Block Chaining Message Authentication Protocol) is a protocol that is based on the AES algorithm and provides message authenticity and integrity verification. Recall that WPA uses TKIP for authentication, but CCMP provides a higher and more reliable authentication. Recently WPA2 is the most used security protocol but it has been identified that it is prone to weaknesses as well. One weakness that WPA2 faces are the brute force attack and dictionary attack. It is however recommended that WPA2 EAP be implemented over the TLS. This adds an extra layer of security to the network with a certificate for verification and validation.

5.4 WPA3 (Wi-Fi Protected Access 3)

WPA3 is an upgraded version of WPA2. It was introduced in 2018 to eliminate the security issues with WPA2. It offers the highest level of security among all the protocols. It also uses an AES-CCMP for its encryption. It uses AES-GCMP as well. GCMP (Galois Counter Mode Protocol) uses 256 key bit encryption and provides higher performance than AES-CCMP. WPA3 also has two modes: WPA3 Personal for homes and WPA3 Enterprise for organizations and it uses a Secure Hash Algorithm (SHA)-256 to achieve integrity. WPA3 certification is required for all Wi-Fi devices, and it is recommended that it should be used rather than WPA2. Table 8 below shows a summary of all the protocols and their features.

	WEP	**WPA**	**WPA2**	**WPA3**
Stands For	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
Developed	1997	2003	2004	2018
Security Level	Very Low	Low	High	Very High
Encryption	RC4	TKIP with RC4	AES-CCMP	AES-CCMP AES-GCMP
Key Size	64 bits 128 bits	128 bits	128 bits	128 bits 256 bits
Authentication	Open System & Shared Key	Pre-Shared Key & 802.1x with EAP	Pre-Shared Key & 802.1x with EAP	AES-CCMP AES-GCMP
Integrity	CRC-32	64 Bits MIC	CCMP with AES	SHA-256

Table 8: A Summary of The Wireless Network Security Protocols and Their Features.

5.5 WiMAX

WiMAX stands for Worldwide Interoperability for Microwave Access. It was introduced in 2001 and it has the IEEE standard of 802.16. It is mainly used for large area networks and can provide broadband access to a lot of remote places. Its base station can typically cover a large area of almost 3000 square miles. WiMAX uses a wireless link with a microwave or millimeter waves and uses a licensed spectrum. It uses a point-to-multipoint (P2MP) architecture and antennas to provide broadband. It has a transmission speed of up to 70 Mbps. It is however slower than Wi-Fi.

5.6 WiGIG

WiGIG stands for Wireless Gigabit Alliance. It was introduced in 2009 and has the IEEE standard of 802.11ad. It was introduced to provide wireless communications at multi-gigabit speeds for different network nodes. It has a frequency band of 60Hz and guarantees a data transfer rate of up to 7Gbps. It supports high-performance wireless implementations of HDMI, display port and USB. The WiGIG uses a technique called beamforming to reduce congestion and increase the performance level. WiGIG is super-fast and is expected to be faster than the most recent Wi-Fi 6 with an IEEE standard of 802.11ax but it has a smaller range and supports only distances of up to 10 metres while a Wi-fi can support up to 100 metres.

6. CONCLUSION

This paper presented a survey of the security challenges and threats that wireless network poses. It started with the security requirements of a wireless network, and then identified the threats found in 5 layers of the OSI model architecture; the application, transport, network, datalink (MAC), and physical layer. Defense mechanisms and countermeasures to

mitigate these threats were also provided. For future work, I shall study the vulnerabilities found in the WiMAX and WiGIG and provide the countermeasures to mitigate these threats.

REFERENCES

Abdel Hakeem, S. A., Hussein, H. H., & HyungWon , K. (2022). Security Requirements and Challenges of 6G Technologies and Applications. *Sensors* , 1-43.

Admin. (2021, January 5). *Different Types of Wireless Communication Technologies.* Retrieved from https://www.watelectronics.com/different-types-wireless-communication-technologies/

Agency, C. &. (2020, May). *Securing Wireless Networks.* Retrieved from https://www.cisa.gov/uscert/ncas/tips/ST05-003

Ioannou, C., & Vassiliou, V. (2016). The Impact of Network Layer Attacks in Wireless Sensor Networks. *International Workshop on Secure Internet of Things (SIoT), IEEE*.

Kaur, J. (2017). Wireless Security Issues and their Emerging Trends. *International Journal of Control Theory and Applications, 10(13)*, 85-90.

Micro, T. (2015, November 09). Retrieved from Understanding Targeted Attacks: Six Components of Targeted Attacks: https://www.trendmicro.com/vinfo/in/security/news/cyber-attacks/targeted-attacks-six-components

Millar, G., Kafchitsas, A., Mavrooulos, O., Kourtis, A., Xilouris, G., Christopoulou, M., . . . B. (2020). 5G Security: Current Status and Future Trends. *INtelligent Security and PervasIve tRust for 5G and Beyond*, 1-101.

Nagarajan, V., & Huang, D. (2010). Using power hopping to counter MAC spoof attacks in WLAN. *IEEE Consumer Commun. Netw. Conf., Las Vegas, NV, USA*, 1-5.

Pandey, A., & Saini, J. R. (2014). Attacks & Defense Mechanisms for TCP/ IP Based Protocols. *International Journal of Engineering Innovation & Research*.

Sula, E. (2018). A review of Network Layer and Transport Layer Attacks on Wireless Networks. *International Journal Of Modern Engineering Research (IJMER)*, 23-27.

Zou , Y., Jia, Z., Xianbin, W., & Lajos, H. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends. *Proceedings of the IEEE* , 1727-1765.