WIRELESS COMMUNICATION SECURITY AND IT'S PROTECTION METHODS

Nikitha Merilena Jonnada

PhD in Information Technology (Information Security Emphasis), University of the Cumberlands, Williamsburg, Kentucky, USA

ABSTRACT

In this paper, the author discusses the concerns of using various wireless communications and how to use them safely. The author also discusses the future of the wireless industry, wireless communication security, protection methods, and techniques that could help organizations establish a secure wireless connection with their employees. The author also discusses other essential factors to learn and note when manufacturing, selling, or using wireless networks and wireless communication systems.

KEYWORDS

Wireless, Network, Security, Hackers, VPN, IP address.

1. INTRODUCTION

Many individuals and organizations widely use wireless communications. They allow many industries to develop new manufacturing ideas and provide various wireless communication methods. The technology that we have today supports a wide range and variety of wireless devices. Previously, almost all the devices humans used were wired devices, which helped the users use the electricity to use a device. Wireless devices were introduced to make the user's usage easy. In today's world, we want everything to be wireless and easy. The technology has advanced so much that we even have self-driving cars, a faster network, high-resolution camera lenses, wireless charging, and voice command devices. Wireless communication has made our lives easy. We even want to use wireless technology to charge our mobiles. We use wireless keyboards, mouse, printers, remotes, gaming consoles, and many other wireless devices. Wi-Fi is another wireless connectivity for the internet [1].

Wireless devices help humans multi-task. For example, we can play a game on the television and use a voice command to play music on a speaker. Even when wireless technology makes our lives easy, it has many drawbacks and security concerns. Wireless devices are more prone to be attacked or hacked by a hacker as these devices support a connection to both authorized and unauthorized Wi-Fi networks. Many suppliers provide open Wi-Fi at coffee shops and restaurants, letting users connect while away from their home network. The hackers could easily access these open networks and, in turn, become a threat to the connected users as their data gets exposed within that network. We need to be careful when connecting to an unrecognized network as sometimes these networks could be a trap for hackers to steal the data from the users who get connected to that network.

DOI: 10.5121/ijdps.2024.15601

2. RESEARCH QUESTIONS

- Are there too many security concerns with wireless connections?
- Do wireless protection methods work to provide security?

3. WIRELESS COMMUNICATIONS SECURITY

Security can be an issue with almost everything being developed and used with wireless technology. Another issue could be the connectivity range. Security is the central issue still being longed for, even with extreme technological advancements. Humans were able to increase the internet speeds, provide a broader range for Bluetooth and Wi-Fi, and create robots using artificial intelligence and machine learning. However, security standards still need to be improved.

Whenever we develop a new solution to provide security to data and devices, hackers tend to surpass our efforts by introducing a new technique to hack into our systems and steal our data. The developers use encryption methods for wireless communication to secure the connection between the two devices, such as a wireless keyboard. The connection here gets established between the keyboard and the laptop or the other device we are trying to use for the wireless keyboard. Encryption is one method that the developers use to provide a secure connection between the parties so that an intruder cannot eavesdrop or illegally access the data [2].

Many wireless connections come with numerous security concerns. A wireless network could be more convenient, but hackers also use it as a hacking medium. Many organizations use cloud networks to store their information, which would help authorized users access the required data remotely. As the cloud is a virtual storage location, it can get exposed to many unauthorized users trying to gain network access. Organizations increasingly adapt to artificial intelligence (AI) and machine learning (ML). Robotics is an exciting and interactive platform. This can make the tasks easy for us, but like the wireless networks, even AL and ML have many limitations and security concerns. Even with advanced technologies like AI and ML, the primary security concern is the data fed to the automated devices [3].

A robot that functions as needed is programmed in a particular way to achieve the desired results. A large amount of data gets fed for the robot to listen, process the information, and respond to the user's command as needed. This data could be at risk as the robot is still a machine working on the data and internet or a medium prone to hacks. AI is trying to achieve the required security through its processes. Still, no machine or network can achieve complete security, even with the daily introduction of many new technologies, software, and hacking methods. Security is the primary concern with the Internet of Things (IoT). No matter how advanced the methodologies are, hackers tend to introduce a technique that questions the set security standards [4].

Figure 1. Wireless Communication

4. WIRELESS PROTECTION METHODS

4.1. Encryption

The data and the connection must be encrypted for safety when establishing a wireless connection. This is one method the organizations use when developing wireless devices. The established connection must be secure, or the customers will not prefer to purchase or use the wireless devices or connections. When transferring data over a wireless medium, it is safe to encrypt it as it could still be protected even if an unauthorized user tries to access the information by hacking it.

Encryption is a standard method many organizations use to achieve a secure and safe data transfer. As the hackers target wireless and cloud mediums to gain access to the data, it is essential to practice safety while handling the data [5].

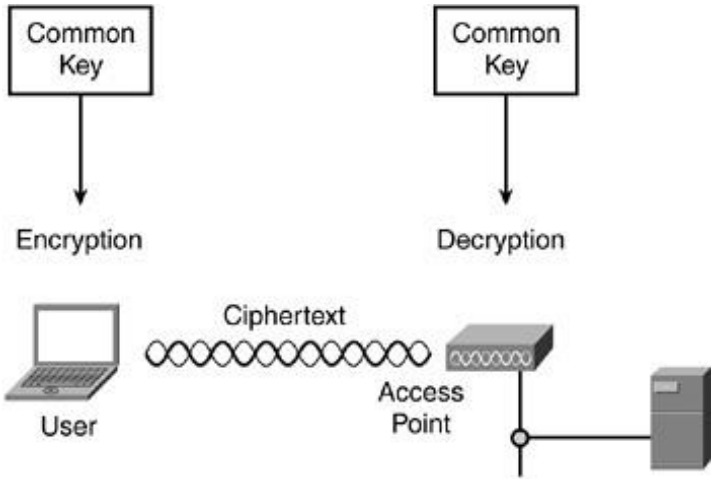

Figure 2. Encryption

4.2. VPN (Virtual Private Network)

Wireless usage has increased since the COVID-19 pandemic. Many organizations have adapted to the work-from-home culture for the safety of their customers. When working from home, the employee needs a VPN (Virtual Private Network) to connect remotely to the central server to access the data and stay connected with the organization. When this connection is enabled, the IP address of the employees' system gets masked, making it hard for the hacker to trace. This is another reason many organizations continue to use remote work. Security could be a concern as the user gets connected remotely to the organization's database, where large amounts of organizational data get stored. The hackers could target the remote workers as they try to connect to their organization over an unsecured internet connection. The data and the established connection are safe if the user uses a secured connection. [6].

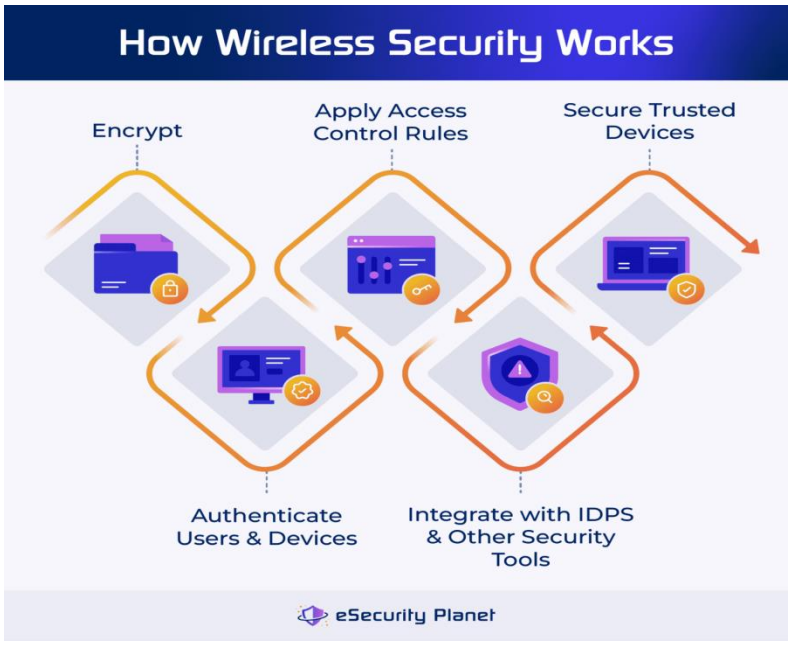

Figure 3. How Wireless Security Works

4.3. Authentication

When setting up wireless communication, we always see a notification or an authentication message that tells us that the connection is secure and that it is being established only between the two devices or parties we are trying to connect. Let's say we are trying to connect a wireless headphone to a laptop. Once the connection gets established, we can use the headphones without issues. If we try to connect another device to the same wireless headphone, we would have to disconnect it from the laptop to connect it to another device. This is one way the companies tell their users that their connection is protected [7].

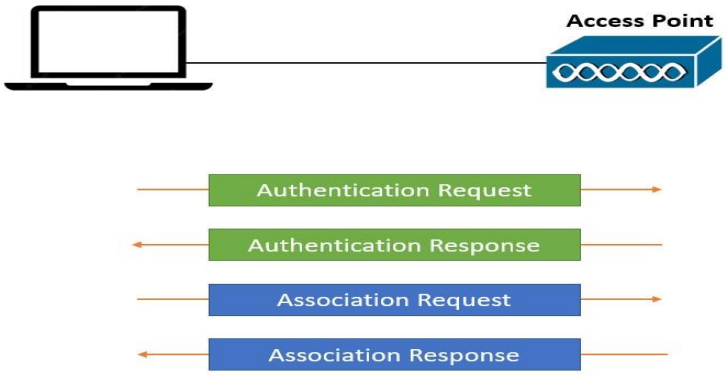

Figure 4. Authentication

5. FIREWALLS AND INTRUSION DETECTION SYSTEMS (IDS)

Firewalls and intrusion detection systems protect the network from external attacks and intruders. They help protect the networks and systems from external sources. These act as the first layer of defense against external viruses and activities that try to enter the network [8].

5.1. Firewall

A firewall is an essential network security system that helps monitor and control incoming and outgoing traffic. This is based on the security rules that the security analysts predefine. A firewall protects organizations by establishing a barrier between their internal trusted network and an untrusted external network like the Internet [8].

5.2. Types of Firewalls

5.2.1. Packet-Filtering Firewalls

This firewall operates at the network layer. This helps examine various data packets to determine if external traffic is from a trust based on the predefined rules. This helps block traffic from the entry point [8].

5.2.2. Stateful Inspection Firewalls

This firewall helps track the state of the actively established connections and makes the necessary decisions depending on the traffic data. Unlike a packet-filtering firewall, a stateful inspection firewall helps keep track of the session state. This type of firewall checks if an established connection is part of the existing communication or if it is unauthorized and responds accordingly [8].

5.2.3. Proxy Firewalls

This type of firewall acts as a bridge between the services and the users by forwarding the requests on the user's behalf. This firewall provides an extra layer of protection by hiding the details of the internal network [8].

5.2.4. Next-Generation Firewalls (NGFW)

This type of firewall combines traditional features with additional functions like deep packet inspection (DPI), filtering, application awareness, and intrusion prevention systems (IPS). This helps block specific applications and provides control over encrypted traffic [8].

5.3. Key Features of Firewalls

5.3.1. Traffic Filtering

This type of firewall blocks unauthorized access to the network and filters the traffic based on rules like IP address, ports, and protocols [8].

5.3.2. Network Address Translation (NAT)

NAT conceals internal network addresses, making it difficult for attackers to target specific devices inside a network [8].

5.3.3. Virtual Private Network (VPN) Support

Many firewalls support VPN connections by providing safe access to a remote network [8].

5.3.4. Logging and Alerts

A firewall helps log the traffic data to generate alerts by detecting any suspicious activity and allows the network administrators to monitor and respond to various threats [8].

5.4. Benefits of Firewalls

- Firewalls help prevent unauthorized access and users from entering the system and network.
- They help protect internal networks from various external threats.
- They help control traffic by enabling security analysts to control network traffic.
- They help the analysts track malicious acts and potential attacks by alerting them as needed.
- They help improve the network's performance by blocking unnecessary traffic and reducing the overload or burden on the networks [8].

6. INTRUSION DETECTION SYSTEMS (IDS)

6.1. Network-Based IDS (NIDS)

NIDS monitors the network traffic to detect any suspicious activities and security breaches that are happening within the network. It analyzes data packets that pass through the network and alerts administrators to potential threats. It helps detect unusual traffic patterns like large traffic volumes from one IP address, indicating a DDoS (Distributed Denial of Service) attack [9].

6.2. Host-Based IDS (HIDS)

HIDS is usually installed on individual host systems to monitor and analyze various activities that happen on that system. It checks for unauthorized or malicious activities, changes in system

logs or files, login and logout times, and checks if any unauthorized software gets installed. It detects if files change within the system and if malware gets installed [9].

6.3. Signature-Based IDS

Signature-based IDS uses predefined signatures or patterns to identify known attacks. It works like an antivirus scanner, matching incoming traffic with a database of attack signatures. An SQL injection gets detected, and the system sends an alert [9].

6.4. Anomaly-Based IDS

Anomaly-based IDS establishes a baseline of regular network activity and alerts when deviations from this baseline occur. It is more effective at detecting unknown or new types of attacks. A sudden surge in network traffic or unfamiliar requests might trigger an alert if they fall outside typical patterns [9].

6.5. Hybrid IDS

As the name suggests, hybrid IDS functions like signature-based and anomaly-based detection methods. It helps organizations by providing a more feasible solution for detecting known and unknown attacks. Hybrid IDS uses signatures to detect known malware and helps analyze traffic patterns to determine various attacks [9].

7. CONCLUSION

Connections like Wi-Fi, hotspot, and Bluetooth might come with certain limitations. Sometimes, these connections could get hacked when connected to an unsecured internet. For example, when we connect our device to a home network, it is secure as we set a password to our network, and only we would know the password. But when we connect our device to an open internet connection at a coffee shop, the connection could be more robust with solid firewalls. We must be careful while establishing a connection using our devices to protect our data from getting stolen. Every innovation has its advantages and disadvantages. We must learn about it before using it. Wireless networks have drawbacks, but many individuals and organizations widely use them for many purposes. By following specific measures, we can protect our data using wireless connections and mediums from getting stolen or hacked.

REFERENCES

[1] Islam, M., & Jin, S. (2019). Advances in Wireless Communications and Networks.
[2] Rong, B. (2023). Security in Wireless Communication Networks. 10-11.
[3] Zhu, G., Liu, D., Du, Y., You, C., Zhang, J., & Huang, K. (2020). Toward an Intelligent Edge: Wireless Communication Meets Machine Learning. 19-25.
[4] Han, X., Zhiqin, W., Li, D., Tian, W., Liu, X., Liu, W., . . . Ning, Y. (2024). AI enlightens wireless communication: A transformer backbone for CSI feedback. 1-14.
[5] Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. 1-1000.
[6] Wang, H. L., Ma, H. F., & Cui, T. J. (2022). A Polarization-Modulated Information Metasurface for Encryption Wireless Communications.
[7] Bai, L., Zhu, L., Liu, J., Choi, J., & Zhang, W. (2020). Physical layer authentication in wireless communication networks: A survey. 237 - 264.
[8] Mukkamala, P. P., & Rajendran, S. (2020). A Survey on the Different Firewall Technologies.
[9] Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H., Rashidi, S., . . . Rahmani, A. M. (2021). Deep Learning-Based Intrusion Detection Systems: A Systematic Review.

AUTHOR

Nikitha Merilena Jonnada earned her PhD in Information Technology (Information Security Emphasis) from the University of the Cumberlands in 2024. The author is continuing her research within the security emphasis and is also expanding her research into artificial intelligence and machine learning to develop security measures using the latest technology standards.