CYB60004

Networks and Cybersecurity Frameworks

Assignment 3

Wireless Security Standards

Pulkit Patel

103139787

Executive Summary

This assignment tests my knowledge of wireless security standards. I studied and analyzed the 802.11 standards' functional and security elements. My first portion depicts the historical background of Wi-Fi. The functional and security sections are the second and third sections, respectively.

elements of 802.11.

The fourth and final component is my assessment of 802.11 and its direction. As a result of the

I have covered as much material as 2,000+ words due to presentation constraints.

Contents

Introduction

A variety of security features are defined in the IEEE 802.11 specifications, including:

Authentication guarantees that only authorized devices are allowed to connect to the network.

Encryption: This safeguards the privacy of data transferred via a network.

Data integrity ensures that data is not tampered with during transmission.

The IEEE 802.11 standards' security features have improved over time. The first versions of the measure included a security technique known as Wired Equivalent Privacy (WEP). However, because WEP was shown to be readily hacked, it is no longer considered secure. Wi-Fi Protected Access (WPA) is the current security standard for IEEE 802.11 networks. WPA employs a more robust encryption method than WEP and contains additional security measures such as message integrity checks.

WPA2, a newer security protocol, has also been launched. WPA2 is a safer security protocol than WPA and is preferred for IEEE 802.11 networks. Along with WPA2, the IEEE 802.11ax standard provides a new security feature, Enhanced Data Protection (EDP). EDP adds another layer of security against eavesdropping and data tampering threats. The IEEE 802.11 family of standards' security features continually improves to handle emerging security threats. You may assist in securing your wireless network from unauthorized access and data breaches by implementing the most recent security standards and best practices.

Historical background

The first standard of IEEE 802.11 was published in 1997. Since then, the standard has been modified several times and is being supplemented by further features and possibilities in each new edition. The most recent version of the standards, IEEE 802.11ax, has been launched in 2019. In the 2.4 GHz frequency range, an original IEEE 802.11 standard has been used. It could handle data speeds of up to 2 Mbit/s. The first commercial products based on the IEEE 802.11 standard were manufactured in 1999.

In 1999, a new version of the IEEE 802.11 standard was introduced: IEEE 802.11b. The data rate could have been up to 11 Mbit per second with this change. The IEEE 802.11b standard was immediately adopted by most Wi-Fi users and is still used today. In 2003, a new version of the IEEE 802.11 standard was introduced: IEEE 802.11g. This amendment has extended the capacity to receive data up to 54 Mbit per second at the 2.4 GHz frequency band. IEEE 802.11g has been created that is backward compatible with devices in the field of 802.11b.

In 2009, IEEE 802.11n was published, a new update of the standard. This amendment introduces the capacity to transmit data rates exceeding 600 Mbit per second at 2.4 GHz and 5 GHz frequency bands. IEEE 802.11n also included additional capabilities like multiple input multiple output (MIMO) and beamforming.

In 2014, a new update of the IEEE 802.11 standard, known as "802.11ac," was launched. This amendment has made it possible to achieve maximum data speeds of up to 6.9 Gbps in the 5 GHz frequency band. New features, such as 1024 QAM modulation and wider channel bandwidths have also been added by IEEE 802.11ac.

The newest version of the IEEE 802.11 standard, which was released in 2019, is now known as 802ax. In the 2.4 and 5 GHz frequency bands, this amendment will increase data speeds to up to 9.6 Gbit per second. IEEE 802.11ax also introduces new features such as OFDMA and Target Wake Time (TWT).

The IEEE 802.11 family of standards is constantly developing to meet consumer and application needs. Faster information processing speed, improved performance, and other security and efficiency features are offered by the most recent standards.

Functional Aspects

- The data rates are divided into two Mbit per second to 9.5 Gbit, according to the IEEE 802.11 standards. The exact data rate that can be obtained is determined by the standard, the distance between the devices, and the environment.
- Here are the frequency bands of 2.4 GHz and 5 GHz, according to IEEE 802.11 specifications. The 2.4GHz spectrum is smaller in congestion compared to the 5 GHz band, but it has been hit by more interference from other devices.
- The range of an IEEE 802.11 network shall be determined by a specific standard, the power output from the access point, and its surroundings. There's more power in the 2.4 GHz band than at 5 GHz.
- Authentication, encryption, and data integrity are some security features set out in the IEEE 802.11 standards. Wi-Fi Protected Access (WPA2) is the current security standard for IEEE 802.11 networks. Other characteristics defined by the IEEE 802.11 standards include Quality of Service (QoS), mobility, and mesh networking.

The functional properties of the IEEE 802.11 standard family have changed over time. The updated standards shall provide a faster rate of data, improved performance, and additional security and efficiency features.

This is some of the most important functionality upgrades in the existing IEEE 802.11ax standard:

- OFDMA: Orthogonal Frequency Division numerous Access (OFDMA) is a novel technique for allocating airtime that allows numerous devices to simultaneously send data on the same channel. This has the potential to increase network efficiency and minimize latency.
- Target Wake Time (TWT): A new power-saving feature that allows devices to sleep for extended periods is Target Wake Time (TWT). This has the potential to extend battery life and decrease interference.

- IEEE 802.11ax is intended to satisfy the requirements of future wireless applications such as virtual reality, augmented reality, and the Internet of Things.

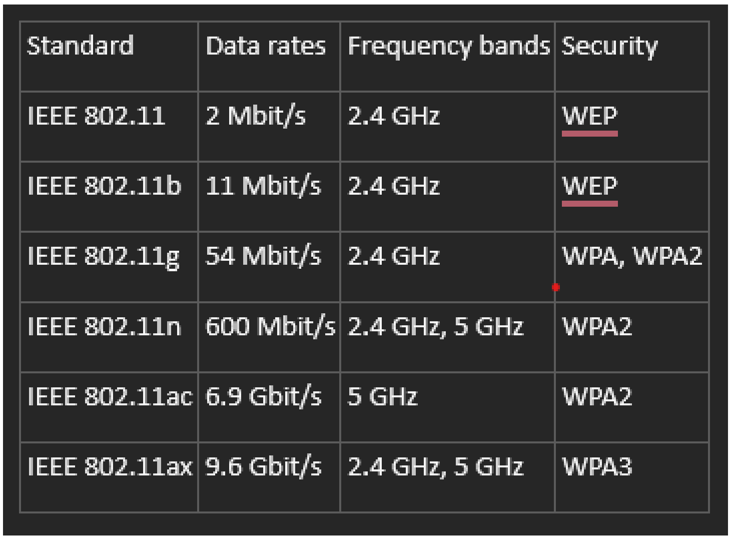
The IEEE 802.11ax standard is designed to meet future wireless application requirements, e.g., in Virtual Reality, Augmented reality, and the Internet of Things.

802.11 Standards

- This is the 1stIEEE 802.11 standard, it'll handle data speeds up to 2 Mbit per second.
- IEEE 802.11b: It can handle data rates up to 11 Mbit per second.
- In 2003, IEEE 802.11g was added to the standard. Data rates up to 54 Mbps may be supported by the 2.4 GHz frequency band.
- IEEE 802.11n: In the 2.4 GHz and 5 GHz frequency bands, it can support data rates of up to 600 Mbit per second.
- IEEE 802.11ac: It supports data rates of up to 6.9 Gbit/s in the 5 GHz frequency band.
- IEEE 802.11ax: The data rate may be sustained at 9.6 GB per second in the 2.4 and 5 GHz frequency bands.

The IEEE 802.11 family of standards continues to evolve to meet consumer and application needs. The most recent standards provide faster, improved performance, and additional safety and efficiency features.

The following table summarizes the essential aspects of each standard:



Standard	Data rates	Frequency bands	Security
IEEE 802.11	2 Mbit/s	2.4 GHz	WEP
IEEE 802.11b	11 Mbit/s	2.4 GHz	WEP
IEEE 802.11g	54 Mbit/s	2.4 GHz	WPA, WPA2
IEEE 802.11n	600 Mbit/s	2.4 GHz, 5 GHz	WPA2
IEEE 802.11ac	6.9 Gbit/s	5 GHz	WPA2
IEEE 802.11ax	9.6 Gbit/s	2.4 GHz, 5 GHz	WPA3

Over time, security features of the IEEE 802.11 standard have become more and more sophisticated. As the original WEP protocol has been proven to be easily compromised, it is not deemed safe anymore. WPA2 is an existing protocol for protecting IEEE 802.11 networks. The WPA2 technology has a stronger encryption technique than the WEP and is accompanied by additional security measures like message integrity checks.

Moreover, a new security feature, Enhanced Data Protection, is included in the IEEE 802.11ax standard. Regarding eavesdropping and data manipulation, the EDP has added a further layer of security.

Security Aspects

Authentication: This ensures that authorized devices can only make a network connection. Encryption: This is designed to protect the confidentiality of communications over a network. Data integrity: It is ensured that no changes are made to the data during transmission.

Over time, the security features of IEEE 802.11 have become increasingly sophisticated. A security protocol known as "WIRED Equivalent Privacy" had been included in the initial versions of this standard. Nevertheless, the WEP was found to be very easy to crack and therefore there is a lack of confidence in it. The current security protocol for IEEE 802.11 networks is Wi-Fi Protected Access (WPA). WPA is based on a more advanced encryption algorithm than WEP and has additional protection features, such as message integrity checks.

There has also been an upgrade of the WPA2 security protocol. WPA2 is a safer alternative to WPA and should be used for IEEE 802.11 network security. In addition to WPA2, the IEEE 802.11ax standard includes a new security feature called Enhanced Data Protection (EDP). The EDP provides further protection in response to eavesdropping and data modification attacks.

Authentication: Before connecting to the network, you need to authenticate your device to ensure it's authentic. Two authentication methods are supported by the IEEE 802.11 standards: open system authentication and shared key authentication. Open system authentication: It's the easiest way to authenticate. No credentials may be provided by any device that connects to the network. This type of authentication is the most unreliable and should be avoided when using production networks. Shared Secret Key Authentication: For this type of authentication, the device must provide confidential keys for an access point. If the device has access to a shared secret key, it will be checked by an access point before connecting to the network. In contrast to the open system authentication, it has a higher degree of security.

Encryption: encryption is the process by which data is scrambled so that unauthorized persons cannot access it. The standards support several encryption algorithms such as Temporal Key Integrity Protocol, 802.11 Advanced Encryption Standard, and 128-bit TCP. TKIP: To remedy WEP's security gaps, TKIP was intended to be an interim encryption protocol. TKIP isn't as safe as AES but is still much safer than WEP. AES: It is a powerful encryption algorithm regarded as unbreakable. For the IEEE 802.11 network, an optimal encryption algorithm is AES. WEP: The original encryption algorithm used in the IEEE 802.11 standards is known as WEP. Security of the WEP is not considered to be guaranteed and should not be applied in production networks.

Data integrity: data integrity shall ensure that it is not amended during transmission. Several data integrity algorithms are supported by the IEEE 802.11 standards, such as the Message Integrity Check Mic and the Cipher Block Chaining Message Authentication Code CCMP. MIC: It's a simple algorithm for ensuring data integrity, which is not very secure. CCMP: A secure algorithm for data integrity that is deemed to be unbreakable. The CCMP algorithm is used in the IEEE 802.11 network to ensure data integrity.

Security Solution

Firewalls: Firewalls are devices which control the flow of traffic between networks. They can be used to block unauthorized access to your network and protect devices from malware.

Intrusion detection system: IDSs are monitoring your network for suspicious activity. They can detect unauthorized access, malicious attacks, and other threats.

Intrusion prevention systems: IPSs are like IDSs, but they can also take measures to prevent unauthorized access or mitigate attacks.

Data loss prevention: DLP solutions are designed to prevent the leakage of sensitive data. They can be used to scan files and email for sensitive data and block unauthorized access to that data.

Encryption: Data protection can be protected from unauthorized access with encryption. It can also be used for data encryption at rest, in transit, or both.

Identity and access management (IAM): IAM solutions are designed to manage user access to systems and resources. You can use them for creating, managing, and assigning user accounts, setting permissions, or monitoring users' activities.

Security information and event management (SIEM): SIEM solutions collect and analyze security logs from all over your network. For the purposes of identifying threats and security incidents, they can be used.

Conclusion

The IEEE 802.11 standards have defined several security features including authentication, encryption, and data integrity. Over time, the safety features of IEEE 802.11 standards have become more sophisticated. It has been found that a simple breach of the original WEP protocol is possible, making it no longer considered safe. WPA2 is the security protocol for IEEE 802.11 networks currently. WPA2 uses a more robust encryption algorithm than WEP, including additional security features like message integrity controls. A new security feature called Enhanced Data Protection is also part of the IEEE 802.11ax standard. The EDP shall provide additional protection against eavesdropping and data modification attacks. Using the latest security protocols and best practices, you can help protect your wireless network from unauthorized access and data breaches.

These are some good practices for the security of your IEEE 802.11 network: Use a strong password to connect to your wireless network. Enable encryption with WPA2 or WPA3. Make sure your wireless firmware is up to date. To prevent unauthorized access to the network, try using a firewall. Keep in mind what information you're transmitting over the wireless network.

References

www.youtube.com. (n.d.). *The Evolution of IEEE 802 11 standards - BAG NAC*. [online] Available at: https://www.youtube.com/watch?v=qZLPq5mebFM.

www.diffen.com. (n.d.). *WEP vs WPA - Difference and Comparison | Diffen*. [online] Available at: https://www.diffen.com/difference/WEP_vs_WPA.

etutorials.org. (n.d.). *Chapter 8. WLAN Encryption and Data Integrity Protocols :: Wireless lan security :: Networking :: eTutorials.org*. [online] Available at: http://etutorials.org/Networking/Wireless+lan+security/Chapter+8.+WLAN+Encryption+and+Data+Integrity+Protocols/ [Accessed 20 Aug. 2023].

Venafi (n.d.). *Active & Passive Attacks [Definition & Differences] | Venafi*. [online] venafi.com. Available at: https://venafi.com/blog/what-active-attack-vs-passive-attack-using-encryption/.

Professor Messer (2015). *802.11 Wireless Standards - CompTIA Network+ N10-006 - 5.3*. *YouTube*. Available at: https://www.youtube.com/watch?v=SeANpj-4mFs [Accessed 17 Aug. 2020].

Mitchell, B. (2019). *802.11 WiFi Standards Explained*. [online] Lifewire. Available at: https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553.

www.youtube.com. (n.d.). *A3 - 802.11 Security Standards*. [online] Available at: https://www.youtube.com/watch?v=GoxTxj40w5w [Accessed 20 Aug. 2023].

Anon, (2019). *WEP (Wired Equivalent Privacy) - Tech-FAQ*. [online] Available at: https://www.tech-faq.com/wep-wired-equivalent-privacy.html [Accessed 20 Aug. 2023].