CHAPTER 8

Comparison of WEP, WPA, WPA2, and WPA3 in Wireless Security Protocols

Muhammad Anwar, Ayaz Hussain, Abdul Qahar, and Farkhana Muchtar

8.1 INTRODUCTION

Wireless Local Area Networks (WLANs) are inexpensive, flexible, and simple to set up. WLANs have quickly become the norm because of these threats, and choosing a security protocol for an IT infrastructure is crucial. It is one of the primary goals of this paper to inform readers who aren't experts on wireless security protocols about the dangers posed by these systems and to outline the limitations of wireless security measures. Different attacking methods come in wireless networks as shown in Figure 8.1. So wireless security protocols are used to protect against these attacks. The abbreviation of WPA refers to Wi-Fi Protected Access and is similar to Wired Equivalent Privacy (WEP) in that it ensures privacy over an open wireless network. Here, we examine the similarities and differences between WEP, WPA, WPA2 and WPA3 in terms of their operational and security hurdles. If we use a legendary attack, like the air attack, we can validate and authenticate all three protocols at once. This test can be run on a "backtrack" operating system. These results demonstrate that WEP is the weakest of the three tested protocols that WPA was only a short-term fix, and that WPA2 is the permanent solution. Wireless networks are currently the most promising technological advancement with the potential to drastically alter our planet. This paper's central focus is on wireless security protocols such as WEP, WPA, WPA2, and WPA3. WPA2 is more secure than WPA (Zaidan, 2021) because it employs the more modern Advanced Encryption Standard (AES) encryption standard. Unfortunately, when a brute force attack or Machine Identification Code (MIC) is used to decode WPA2's contents (Kissi & Asante, 2020), the protocol is completely defenceless. In wireless communication, information is transferred between nodes without the use of a physical connection such as a transmission cable.

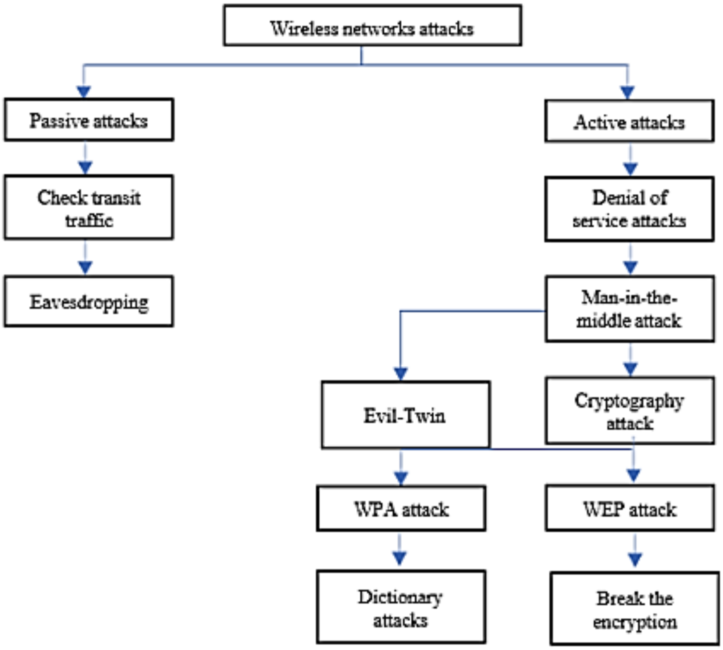

Figure 8.1 Wireless network attacks

WEP was the first wireless network encryption standard. A wireless network's safety is ensured by this protocol. The WEP protocol is easily cracked today (Atluri & Rallabandi, 2021). Protocol WPA followed, with its improved security protocol still unbroken as of WPA2's release. Today, wireless security is one of the most pressing issues in the field. Several vulnerabilities exist in wireless networks. The wireless LAN card is a standard feature on many modern laptops (Khastoo et al., 2020). Data privacy and data integrity are two essential concepts for a safe and secure network. One way to protect sensitive information is to encrypt every packet in transit, while another way is to check for and fix any mistakes in the data.

An overview of the relevant background literature is included in Section 8.2 of this chapter. Section 8.3 details the discussion of this chapter, and Section 8.4 provides a summary of the chapter's findings.

8.2 Wired Equivalent Privacy

The primary goal of the WEP protocol was to ensure highly secure two-way communication via radio transmissions. Wi-Fi security has long been recognized as a major concern in the networking industry. Wireless Encryption Protocol is a network that encrypts data sent via wireless networks. The Wi-Fi Encryption Mechanism is a protocol for securing wireless networks using the 802.11 standards. WEP protects 802.11 networks with encryption and data integration (Rana et al., 2021). Privacy on Par with Hardwired Systems In 1997, the IEEE 802.11 standard was updated to include WEP. WEP is a form of wireless encryption that provides a minimal level of protection for networks without wires. The use of WEP ensures that information is secure during transmission. Data privacy and data integrity are two core module functions in the WEP. When compared to a wired LAN, WEP's security was no better and often no worse. WEP was a framework that ensured the safety of wired LANs through bidirectional data encryption using the RC4 algorithm (Chandra & Azis, 2021). Two Open Systems Interconnection Layers This is a simulation of the WEP protocol. To authenticate users and encrypt and decrypt messages, WEP stores a secret key called a WEP key (Ramana et al., 2022).