OPEN WIFI AND THE WEWORK BREACH

Graduate Project 1: The Paper

Eliora Horst

COMP 448: Network Security

Instructor: Corby Schmitz

Loyola University Chicago

Introduction

Right before the turn of the millennium, untethered access to the internet became possible. WiFi as we know it in the year 2022 didn't fully emerge until 1999, when the Institute of Electrical and Electronics Engineers (IEEE) created the first wireless protocol, which they dubbed the IEEE 802.11 standard. After consultation with a marketing agency, they rebranded with the term Wi-Fi, and formed the WiFi Alliance.[10] The current version of this wireless network standard is IEEE 802.11n, which increased the range at which WiFi networks can function from 150ft indoors to 175, as well as increasing speed from up to 55Mbps to up to 600Mbps (theoretical).[10] As the ubiquity of internet access has become more and more standard, security measures have had to work hard to keep pace. Gaining access to a private or corporate WiFi network is the foot in the door many malicious parties need in order to execute their plans of attack. While security protocols are updated regularly, there is a huge human component that is necessary to manage when it comes to securing a network.

WiFi Security

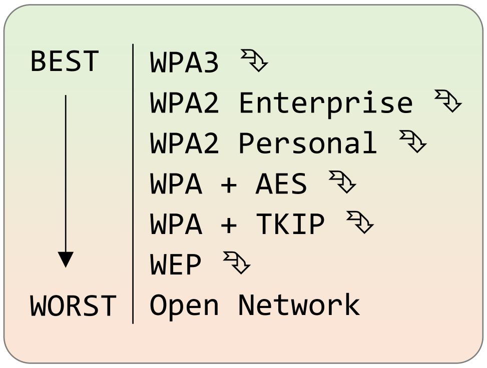
With each release of faster and more robust wireless protocols there has been a necessity for security protocols to be bundled in. Since 1999 there have been three main security protocols implemented to fortify the security of wireless networks – WEP, WPA, and WPA2.

WEP	The first wireless security standard was implemented the same year as the WiFi Alliance was born – 1999. The Wired Equivalent Policy (WEP) was designed to provide the same level of security to wireless networks that wired networks had within them inherently. WEP had several key weaknesses that made it relatively easy

	for breaches. The first issue was key management - The issue being there was no standard established for it. Set up of keys between access points and client stations was time consuming, and many WEP networks ended up using a single key across the entire network. The key size was also dangerously small, only 40 bits; at the time bit keys of this size were seen as reasonable for the kind of security they were expecting to deal with, but this turned into a serious problem. The second issue was the initialization vector being far too small – 24 bits. Like with the keys, the management of IV values was not established, so IV's were reused. If an attacker were to gain ahold of value, they could decrypt packets without the key. The next issue WEP had was it used a cryptographic cypher that initially was designed to check for errors, not protect secure systems. Through this, cyber attackers were able to modify packets with relative ease. The final major issue was that its system allowed for authentication messages to be forged. WEP was vulnerable to all kinds of attacks, including replay, dictionary, DOS, and Known Plain Text attacks. WEP was "officially abandoned" in 2004.[8]
WPA	WiFi Protected Access (WPA) was initially implemented as a temporary security enhancement for WEP[8]. WPA was formally chosen to override WEP in 2003. Even though WEP was now defunct, many organizations were still using WEP systems that had been patched with WPA, which still made them vulnerable. WPA also kept some of the same features as WEP so it would be more compatible with older systems, so it became vulnerable for many of the same reasons WEP was. WPA introduced the "Temporal Key Integrity Protocol" (TKIP) to make encryption more secure. The kinds of attacks that turned out to pose the most threat to WPA protected systems

	were ones made through WiFi Protected Setup (WPS), a system which was meant to simplify the joining of devices to accesses points.
WPA2	Like it's predecessor, WPA2 was rolled out in the same year with IEEE 802.11i, and replaced WPA just two years later. The biggest distinction between versions one and two was the inclusion of the Advanced Encryption Standard (AES). WPA2 also offered personal and enterprise options, expanding the security levels for different kinds of need. The main security flaw in WPA2 is that once an attacker gains access inside a network, it is relatively easy to move around and attempt attacks on other machines in the network. While not an issue for induvial or home users, this can pose a not insignificant threat to large companies that have huge networks. WPA2 still supports WPA, which makes it still vulnerable to the same kinds of attacks as WPA. It uses a four-way handshake between clients and access points, and was especially weak to Dictionary attacks. WPA2 also is not supported by older devices, leaving those older systems more vulnerable than ever to attacks.

Wireless Security Protocols



BEST
WORST

WPA3
WPA2 Enterprise
WPA2 Personal
WPA + AES
WPA + TKIP
WEP
Open Network

In 2018 WPA3 was announced as the replacement for WPA2. While it has yet to see wide implementation, it makes significant security upgrades to WPA2. The four-way handshake vulnerability by implementing the Simultaneous Authentication of Equals (SAE) handshake, also known as the "Dragonfly Key Exchange". It works by hashing the generated key that is unique to every single exchange. It allows access points and stations to authenticate each other while protected itself, so attackers can't attempt to perform a Dictionary attack or something similar. WPA3 also improves upon the safety of establishing connections, and makes use of QR codes to quickly and safely onboard new devices to a network.

The WeWork Breach

WeWork is a real estate company that company that designs and builds both virtual and physical offices spaces for people and companies. A big issue WeWork had was that its WiFi security was shaky at best. In 2019, an article from *Fast Company* did an extensive write up on the security flaws with the company. It found that all WeWork networks implemented WPA2 Personal, which made it susceptible to password compromises. "Possession of the password for a WPA2 network provides the added ability to decrypt traffic from any client within range…"[3] Anyone who was an employee who used a WeWork network had access to the exact same password – a password that had managed (in 2019) to be shared across 528 locations all across the globe. Not only was this password widely disseminated, it was also incredibly easy to guess. Fast Company warned of the dangers of a man-in-the-middle attack, but WeWork seemed confident that their password security was up to par. In a statement to FC a representative said, "In addition to our standard WeWork network, we offer members the option to elect various enhanced security features, such as a private VLAN, a private SSID, or a dedicated end-to-end physical network stack."[3] Fast Company gave some advice as to how WeWork could improve their security, including basic things like frequent password changes and unique passwords per location. Three months after the Fast Company article came out, a Dubai-based researcher with the cybersecurity firm spiderSilk discovered a public GitHub repository full of scripts that referenced amazon cloud files filled with WeWork customer data. Customers personal information, including full names, contact information, and bank details, were stored publicly on the internet by WeWork developers. It is unclear how long these vulnerabilities in WeWork's system were available for any attacker to easily exploit.

In response to the exposure of WeWork's network vulnerabilities, Rob Gurzeev, CEO of CyCognito, a cybersecurity firm, said this: "Unfortunately, this kind of IT ecosystem risk isn't unique to WeWork. In fact, IT and security teams often don't even know if and where all of their organizations' digital infrastructure and assets are, or whether they're fully protected." The WeWork incident highlights how dangerous it can be to rely on old and outdated technology when it comes to data security. Networks needs to be kept updated, while maintaining integrity and security for the users to need to access it. The more users and customers know how to keep their credentials secure and maintain their networks, the harder it will be for attackers to gain access to vulnerable materials. The human element is often the weakest link in maintaining good network security.

Bibliography

1. "802.11 Wireless Standards | Network+ Exam Cram: Wireless Networking | Pearson IT Certification." Accessed February 4, 2022. https://www.pearsonitcertification.com/articles/article.aspx?p=1329709&seqNum=4.
2. AI, Society of. "What Is WiFi Security??" *Medium* (blog), January 25, 2021. https://societyofai.medium.com/what-is-wifi-security-d75f3989a206.
3. Captain, Sean. "WeWork's Laughably Weak Wi-Fi Password Is Downright Dangerous." Fast Company, August 21, 2019. https://www.fastcompany.com/90391748/weworks-wi-fi-network-is-easy-to-hack.
4. CPO Magazine. "WeWork Breach of Confidential Business Information Serves as a Good Reminder About the Holes in Public WiFi Security," September 30, 2019.

https://www.cpomagazine.com/cyber-security/wework-breach-of-confidential-business-information-serves-as-a-good-reminder-about-the-holes-in-public-wifi-security/.

5. CPO Magazine. "WeWork Exposes Customer Contracts and Personal Data in Another Security Mishap," December 6, 2019. https://www.cpomagazine.com/cyber-security/wework-exposes-customer-contracts-and-personal-data-in-another-security-mishap/.
6. "What Is WPA3 and What You Should Test in WPA3 Enabled Devices | Qa | Cafe." Accessed February 4, 2022. https://www.qacafe.com/resources/what-is-wpa3-how-to-test-wifi/.
7. "Whatswrongwithwep.Pdf." Accessed February 4, 2022. http://www.opus1.com/www/whitepapers/whatswrongwithwep.pdf.
8. NetSpot. "WiFi Security: WEP, WPA, WPA2 And Their Differences." Accessed February 4, 2022. https://www.netspotapp.com/blog/wifi-security/wifi-encryption-and-security.html.
9. Panda Security Mediacenter. "WPA vs WPA2: Which WiFi Security Should You Use?," April 8, 2020. https://www.pandasecurity.com/en/mediacenter/security/wpa-vs-wpa2/.
10. Sparks, Matthew. "What Does Wi-Fi Stand For?" New Scientist. Accessed February 4, 2022. https://www.newscientist.com/question/what-does-wi-fi-stand-for/.