EECS 325 Project 1b

An Analysis of Various Wireless Network Security Technologies as Enforced by the Wi-Fi Alliance

Since 1999, the Wi-Fi Alliance has defined innovative, standards-based Wi-Fi technologies and programs, certified products that meet quality, performance, security, and capability standards. As a result, consumers and enterprises alike have enjoyed the benefits of increased wireless network security technologies enforced by Wi-Fi Alliance approved certifications and policies. Even though wireless security has drastically improved over the years as a result of the Wi-Fi Alliance's actions, it is apparent that wireless security is nowhere near perfect as pointed out by members of the networking security community. This paper will summarize four major generations of wireless security technologies as approved by the Wi-Fi Alliance since the organization's inception. This paper will also analyze the effects of these technologies in consumer and enterprise markets and will go on to provide vulnerability solutions for future wireless network security technologies.

Jacob Alspaw

28 November 2018

Table of Contents

1. Introduction

The Wi-Fi Alliance is a worldwide network of organizations and companies that bring Wi-fi enabled technologies to enterprises and consumers. Members of the alliance come together from across the globe to collaborate with the shared vision of connecting Wi-Fi users to everyone and everything. The organizations aim to reinforce the interconnectedness of today's society by enabling and creating environments in which users are provided the best possible end experience. The alliance goes about enforcing standards by invoking mandated policies and providing certifications for Wi-Fi enabled products.

Since 2000, the Wi-Fi Alliance has inspected and approved through certification more than 40,000 distinct products[4]. For consumers that have purchased a Wi-Fi device since 2000, it is likely they have seen the Wi-Fi CERTIFIED™ seal of approval displayed prominently on the product's packaging. The seal designates inspected and approved products that meet standards based on their advertised features. Standards that the Wi-Fi alliance enforce include "proven interoperability, backwards compatibility, and the highest industry-standard security protections" [4].

Fig. Wi-Fi Alliance certification symbol

The adoption of Wi-Fi over other technologies has been a growing trend over the past two decades. As of June of this year, Wi-Fi carries a majority of the internet's traffic and continues to grow through an expanding variety of interconnected applications that billions of people rely on everyday[4]. Because of Wi-Fi's extreme global popularity, there is an outstanding need for evolving security solutions that keeps users and their transmitted data safe from prying eyes.

Since the inception and implementation of the first Wi-Fi enabled devices, security standards have evolved in an effort to ensure that transmitted data remains private. The Wi-Fi alliance has been directly responsible for improving upon four major generations of Wi-Fi enabled network security technologies: WEP, WPA, WPA2, and WPA3. This paper will summarize the four major generations of wireless security as outlined in the provided articles, analyze the effects of these technologies in consumer and enterprise markets, and will finally go on to provide vulnerability solutions for future wireless network security technologies.

2. Summary of Articles

2.1 WEP

Wired Equivalent Privacy (WEP) is a simple and low-level protocol intended to protect and secure wireless connections between a mobile station and an access point. At the time it was first developed in the late 1990's, WEP was very popular in use and was often the first security choice presented to users by router configuration tools. The technology offered a reliable solution for providing data confidentiality comparable to that of a traditional wired network. WEP precedes all forms of WPA and was the only encryption protocol available for 802.1x networks prior to 2003 [5].

WEP encrypts data packets using the RC4 algorithm as they are sent out from the access point or mobile station's wireless network card. The packet- receiver then decrypts the packets using the same 40-bit key. Each byte of data is encrypted using a different packet key, a combination of a pre-shared password, a state array, and a 3-byte initialization vector generated by the computer [4]. A 3-byte random number being used with the RC4 algorithm creates 16,777,216 different ciphers for one WEP key [1]. This was initially thought to be cryptographically secure because expensive, yet successful brute-force attacks would only divulge information contained within a single packet.

Requests are authenticated using Shared Key authentication. Shared Key authentication involves a client that must provide a pre-existing key in order to be able to connect to the network. The key is generated by the device using a password required by the network to join the system. The process begins with the client sending an authentication request to the wireless access point. The access points responds to the client with an encrypted file. The client then tries to decrypt the file using the key created from the password and sends the contents back to the access point. At this time, the access point compares the original file to the contents of the file sent from the mobile station. If the contents match, then network access is granted [1][3].

2.2 WPA

A series of studies from various academic institutions had shown that an intruder equipped with the right set of tools and a fair amount of technical knowledge could bypass WEP protection all together and gain unauthorized access to a wireless area network. Studies determined and even demonstrated that an intruder who collects enough data can pose a threat to a WEP network. A 3-byte initialization vector is not sufficient to create satisfactory variability in WEP keys. According to the birthday paradox, in a random gathering of 23 people, there is a fifty percent chance that two people will have the same birthday. The same phenomenon occurs with WEP packet encryption. After 5000 packets with randomly generated initialization vectors, a first collision occurs with high probability[3].. Thus, there was need for a stronger security specification.

Wi-Fi Protected Access (WPA) is a strong interoperable Wi-Fi security specification that acted as a reliable replacement to WEP in early 2003. WPA greatly increased the level of protection for over-the-air data transmission on existing Wi-Fi networks. It addressed all known weaknesses of it predecessor, WEP. The Wi-Fi Alliance does not claim that WPA is “bullet-proof” [5]. However, it does provide stronger data encryption than WEP and adds authentication methods that some say are missing in WEP.

WPA uses an enhanced encryption scheme designed around Temporal Key Integrity Protocol (TKIP). The protocol employs a key hierarchy along with a Message Integrity Check (MIC or “Michael”) to protect against message forgeries. The new keys are greatly increased from 40-bits to 128-bits. Whereas WEP’s single static key provided roughly 16 million cipher combinations, TKIP’s key hierarchy provides roughly 500 trillion possible key cipher combinations that can be used to encrypt any given data packet [5]. Keys are automatically distributed and are dynamically reliant on the session, meaning the each key is per user, per session, per packet [5].

The Message Integrity Check is then used to prevent an attacker from capturing, altering, and then sending packets. A hashing algorithm is used on the packet contents and then compared to the MIC. If either the sender or receiver calculates a MIC and the value does not match, then the packet is deemed a forgery and discarded [5].

WPA uses 802.1X authentication with EAP or Extensible Authentication Protocol. EAP is a port-based network access control method that handles the presentation of users’ credentials. Credentials can be in the form of “digital certificates, unique usernames and passwords, smart cards, secure IDs, or any other identity credential that the IT administrator is comfortable deploying” [5]. Allowing great variability in credential type makes WPA flexible.

EAP in accordance with 802.1X creates a system in which clients mutually authenticate with an authentication server. This process prevents users from accidentally connecting to unauthorized access points and also ensures that intruders can’t mask as authorized users [5]. Clients will send user’s credentials to an authentication server via the access point. If the server accepts the user's credentials, the master TKIP key provided to both the access point and the client. The client and the access point will then need to invoke a four-way handshake in which each party acknowledges the other. Installing the keys completes the process [5].

Home networks do not have the resources required to manage IT staff to install or maintain large server configurations. Yet, WPA still offers home users the benefits of WPA security through the use of a password. The password still provides a strong TKIP encryption, but must be manually entered on client devices and on the access point.

2.3 WPA2

WPA was very short lived with the introduction of WPA2 in 2004. Like WEP, WPA still used RC4, a stream cipher algorithm used for encryption and RC4 was relatively weak compared to other existing encryption algorithms known in 2003. In 2003, WPA2 was already being developed to act as the next improvement on wireless security specifications and fix many flaws found in WPA. The RC4 stream cipher algorithm, found in WPA and WEP, was replaced with a new and robust block-cypher algorithm called AES. A stream cipher "only executes against one character at a time, [while] a block cipher operates against an entire block of text all at once" [1].

The primary difference between WPA and more effective WPA2 is how packets are encrypted. WPA2's AES encryption uses successively longer key bit sequences to encrypt transmitted packets. AES is significantly more effective than the previously used RC4 algorithm. The time needed to break a 128-bit key AES encryption is $2.2x10^{17}$ years with a basic supercomputer. The number of years increases to 10^{36} years with a 192-bit key and is considered unbreakable for the time being [1].

Because WPA2 no longer utilized RC4 as the cipher, it has the advantage of no longer using the TKIP. Forgoing the TKIP encryption became a necessity because TKIP was demonstrated to be vulnerable to attacks as of March 2009. The vulnerability cemented the necessity for change to WPA2 in legacy systems that were still using WPA.

While authentication methods remain relatively equal between WPA and WPA2, the same is not the case for system requirements. Whereas older systems were only required to perform a software update to upgrade from WEP to WPA, the transition from WPA to WPA2 requires hardware replacements. WPA was not meant to be anything more than an intermediate standard between WEP and WPA2 [1] and was created to reduce the costs of transitioning into more secure environments. Still, implementation of

WPA2 protected networks requires newer hardware because the available CPUs on existing hardware are too limited.

2.4 WPA3

WPA3 is the newest Wi-Fi network security standard and was announced within the last year. It reintroduces legacy TKIP encryption alongside AES encryption to offer increased cryptographic consistency. WPA3 also makes smart steps to introducing new mandatory policies that were optional in WPA2 [4]. Policies include Simultaneous Authentication of Equals (SAE) and Protected Management Frames (PMF) that address and protects against a major vulnerability recently found in WPA2 by protecting against eavesdropping and packet forging.

WPA3 has replaced pre-shared keys (PSK or passwords) in exchange for SAE. SAE uses a specific handshake called a Dragonfly handshake and applies it to a Wi-Fi network for password-based authentication. To generate session keys, the handshake negotiates a key specific to a client which is then used in a traditional Wi-Fi four-way handshake. Neither the key specific to the client or the key generated by the handshake can be obtained by a passive attack, active attack, or offline dictionary attack in which an adversary can guess multiple passwords per request [1]. Forward secrecy is also ensured because the client's negotiated key cannot be recovered even if the access point's password becomes known.

Upgrading from WPA2 is simply done with an upgrade to an access points software. When the upgrade is complete and the access point has been configured to use WPA3 with the same passphrase as before, all previous devices will be able to connect to the access point without need for reconfiguration [1].

3. Analysis of Articles

3.1 Advantages and Disadvantages of Generational Standards

At the time of their inception, each Wi-Fi networking security standard proved effective against attackers. With the constantly evolving Wi-Fi Protected Access family of technologies, the Wi-Fi Alliance has continued to provide the latest in security improvements. As time has progressed, it is easy to conclude that the successive generational improvements upon these standards has had their advantages and disadvantages.

The undisputed advantage of new Wi-Fi security standards is that with each new generation of security improvements, our sensitive data becomes increasingly protected and safe from network intruders. But is it possible that the disadvantages accrued by the social costs and monetary costs from upgrading our systems have outweighed and eclipsed the advantages? When considering to upgrade our wireless network access points, choosing to do so will always be the smarter and safer choice, but that doesn't mean that clients are willing to put in the effort and take the necessary steps required to upgrade a system.

From the viewpoint of a large enterprise, one of the biggest disincentives of upgrading a system is the monetary costs that are required by staffing a team to deploy a new network. Moreover, large corporations would have been required to replace existing infrastructure if upgrading from WEP to WPA2. To many organizations, increased network security measures can seem more like a want rather than a need because of monetary investments that upgrades require. Legacy systems are often found across many of the world's largest corporations because the benefits don't necessarily outweigh the costs.

From the viewpoint of an at-home consumer, monetary costs can still be an issue when upgrading from WEP to WPA secured networks. Even then, the bigger issue for the individual consumer most likely is social costs. More specifically, it may not be completely irrational to believe that many Wi-Fi consumers have little to no experience in managing their home network beyond setting a network SSID and password. So how can security experts expect the majority of Wi-Fi users to secure themselves by upgrading their personal networks and then configure them to use the newest technologies? That would require users to have some working knowledge of how to use and upgrade their router, to know newer network security standards, and then to even care about their network security in the first place. The problem is that many people do not view themselves as potential targets and are unwilling to change.

3.2 Is WPA3 the Pinnacle of Wireless Network Security Standards?

Currently, WPA3 is the best choice when considering which major wireless networking security standard to use. WPA3 can be used for a wide range of uses including highly controlled corporate environments to more flexible home networks. It is by far the most secure option to use as of 2018 because it addresses all known security vulnerabilities in WEP, WPA, and WPA2. Even though it is a vast improvement over its predecessors, consumers and enterprises should remain skeptical of the technology.

At one point in time, many thought WPA2 was impenetrable because of the new AES encryption scheme, but that was disproven 14 years after its release when a new vulnerability was discovered and demonstrated [1][4]. The vulnerability, called KRACK, rendered every WPA2 protected device insecure and left each client vulnerable. WPA3 has become the “new and shiny” replacement for WPA2 that has led many to believe that the new technology will also be impenetrable. The KRACK vulnerability made WPA2 open to attacks. It is entirely possible and even probable that a new vulnerability will be discovered in WPA3 that will also render the security standard open to attacks.

Even though the Wi-Fi alliance addressed many concerns with WPA2 in WPA3, they may not have done everything they could have to bring wireless security entirely up to date. The researcher responsible for discovering the 2016 KRACK attack on WPA2, Mathy Vanhoef, criticized the Wi-Fi Alliance for doing a poor job at investigating alternatives for security protocols and certifications [4].

Vanheof says that the new SAE protocol introduced in WPA3 will prevent debilitating attacks like KRACK, but questions if the specific Dragonfly handshake type is good enough. Vanhoef goes on to note that even though the Dragonfly handshake is mathematically secure, there were other handshake options that would pose a lower risk to users in potentially causing issues in the future [4].

It is surprising and even alarming that the Wi-Fi Alliance is using technologies the security groups have already pointed out to be flawed. Vanhoef has already expressed the potential for SAE to be vulnerable to side-channel attacks in which a network intruder takes advantage of observations of authentication timing to gain information about a password [4]. Another vulnerability was discovered in 2013 by a team of cryptology researchers at Newcastle University. The team found in their analysis of SAE that the handshake is vulnerable to “small subgroup attacks” where the keys exchanged by the router and the connecting device are forced to much smaller, more solvable subgroups [4]. Even with the knowledge of a 5 year old vulnerability, the Wi-Fi Alliance still chose to implement WPA3 with a proven compromised technology.

On top of using already compromised technologies, the Wi-Fi alliance seemingly took steps backwards in providing WPA3 between its first announcement and actual release. When the Wi-Fi Alliance first presented WPA3, there was a promised suite of four features that were intended to improve security [4]. Only two of the features ever actually made it to WPA3: SAE and a 192-bit encryption scheme. The other two features were never released as part of WPA3 and were instead released as entirely different standards. The first missing standard, Easy Connect, was meant to allow users to more easily connect their IoT devices such as smart TVs [4]. The other feature, Enhanced Open, was meant to provide greater security to open networks, such as coffee shops or guest networks [4].

It is as if WPA3 was a rushed attempt at fixing an existing problem, but was intended to be a long lasting solution unlike the original WPA that was solely meant to be an intermediary step to something better. The Wi-Fi Alliance could have been more open about its selection process of optional and mandatory features in WPA3. Vanhoef describes the Wi-Fi Alliance's selection process of determining new standards as closed off to a majority of the network security community [4]. The process was secretive and what the consumers get is relatively weak security compared to what it could have been. An open process with the input of more researchers could have resulted in an even stronger WPA3.

4. Future Work in Wireless Network Securities

There is no doubt amongst experts that the current wireless network security standard, WPA3 is an improvement over WPA2, but there are many improvements that could be made to WPA3 to form a new WPA4.

- **A new key size:** WPA3 introduces a new 192-bit key, but modern advancements in CPU technology should be able to support even greater key sizes. It may require another hardware upgrade like the transition from WEP to WPA2, but the transition from a 192-bit AES key to a 256-bit AES key would be a great bound forward in packet encryption.

- **Include mandatory features:** In WPA2, Package Management Frames (PMF) were an optional feature. In WPA3, the Wi-Fi Alliance decided that PMF should instead be a mandatory feature along with the Dragonfly handshake. I propose that Easy Connect and Enhanced Open, the two optional features of WPA3 be included in the next generation of Wi-Fi Protected Access and be made mandatory. WPA3, Easy Connect, and Enhanced Open should not have been separated into three specifications in the first place. Having additional options will confuse consumers whereas having one specification with mandatory components is simpler.

- **New handshake:** As Vanhoef notes, the Dragonfly handshake is not the best solution. A new handshake should be proposed that replaces the Dragonfly handshake for a handshake that will potentially cause less issues in the future.

- **Open Process for Selecting Standards:** The Wi-Fi Alliance should have consulted other organizations, researchers, and security experts before enforcing the WPA3 specification. Hopefully, the alliance will enact a more open process and consult other organizations and security experts for WPA4, or the next standard in Wi-Fi security. Doing so would only limit potential vulnerabilities by first discussing with the community.

- **Societal Changes:** Their is a real need for societal changes that encourages consumers and enterprises alike to upgrade their outdated legacy systems. It may be appropriate to enforce a hard cutoff date whereby every consumer and enterprise will need to upgrade to and use some modern wireless security specification (at least WPA2) by a specific date. Doing so would incentivise consumers and enterprises to take the necessary steps to upgrade vulnerable systems.

5. Bibliography

[1] F. H. Katz, “WPA vs. WPA2: Is WPA2 Really an Improvement on WPA? .” Armstrong Atlantic State University , Savannah, Georgia.

[2] M. Koziol, “Computer Security Researchers: WPA3 Could Have Been Better, Stronger,” *IEEE Spectrum: Technology, Engineering, and Science News*, 11-Sep-2018. [Online]. Available: https://spectrum.ieee.org/tech-talk/telecom/security/computer-security-researchers-think-more-could-have-been-done-for-wpa3. [Accessed: 28-Nov-2018].

[3] S. Seys, D. Singelee, and B. Preneel, “Wireless Network Security.” K.U.Leuven, Department of Electrical Engineering, Leuven, Belgium.

[4] “Wi-Fi CERTIFIED WPA3 Technology Overview.” Wi-Fi Alliance, Austin, Texas, Jun-2018.

[5] “Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks .” Wi-Fi Alliance, Austin, Texas, 29-Apr-2003.