WIFI SECURITY POLICES

Dennis Keritsis

I. Intro

This paper outlines the history of WEP, WEP's technical aspects, and WEP's weaknesses. Then, the paper will outline the design history of WPA in view of WEP's vulnerabilities. That is, WPA was never intended to be a final and secure framework. Instead, it was a temporary solution to WEP's vulnerabilities. Ultimately, WPA2 will be discussed in view of WPA. Additionally, the vulnerabilities of WPS and public WIFI will be discussed. A 16-block ratings matrix based off three levels will be provided, and an explanation for each of the ratings will be given.

II. WEP

II(A). WEP History

WEP was introduced in 1999 (Lehembre, 2005), and is associated with the 802.11(b) standard (Morris, 2003). At the time of release, WEP was intended to be as secure as a wired connection (Gali, 2013; Bulub, 2012). Put another way, WEP was not designed with security in mind (Lehembre, 2005). RC5 is and was vulnerable (Lehembre, 2005). In fact, at the time of WEP's release in 1999, RC5 was already found to be vulnerable four years earlier in 1995 (Lehembre, 2005). Just one year later after release in 2000, another WEP weakness was published (Lehembre, 2005). At this point, WEP could only prevent basic wire sniffing (e.g. Wireshark) (Bulub, 2012). RC5 touches on the Confidentiality aspect within the CIA triad.

With respect to Integrity within the CIA triad, WEP uses CRC (Lehembre, 2005). Much like RC5, it is no surprise that the use of CRC is found to be non-cryptographic. Specifically, WEP uses CRC32 (Lehembre, 2005), which is commonly used with error detection, not security (Lehembre, 2005). Again, WEP was not made with security in mind (Lehembre, 2005).

With the security holes associated with RC4 and CRC32, some experts noted that WEP was still usable in some cases (Lehembre, 2005) like home usage which typically does not rank high as a target for hackers. However, when Korek released chop-chop in 2004, security experts agreeded that WEP is not acceptable anywhere, not even home usage (Lehembre, 2005).

II(B). WEP Technical

As noted above, WEP uses RC4 (Srikanth, 2019). RC4 utilizes an Initialization Vector (IV), and the algorithm itself is symmetric with a secret key (Srikanth, 2019), wherein key is static (Gali, 2013; Lehembre, 2005). IVs are transmitted in plain text and are prepended to the ciphered message itself (Lehembre, 2005). With respect to the integrity, WEP uses CRC (Perez, n.d.) which produces an ICV which is only a checksum (Lehembre, 2005).

II(C). WEP Weakness

As outlined above, the RC4 takes an IV, wherein the RC4 provides Confidentiality in our CIA triad. Additionally, the CRC provides our integrity in our CIA. Weaknesses discussed with start with the IV.

II(C)(1). WEP Weakness IV

Simply put, the IV is just too short at 24 bits (Srikanth, 2019; Perez, n.d.; Lehembre, 2005). Using a tool such as airo-dump (Srikanth, 2019), a user can capture a plurality of IVs (Srikanth, 2019). After a sufficient capture, the attacker can analyze the IVs with aircrack-ng (Srikanth, 2019). These tools are readily available and would be easy to use for a script kiddie. That is, a hacker with relatively low skill could crack WEP.

Further, when gathering a sufficient number of IVs, an attack would not need to capture every IV from a set of 16 million (Bulub, 2012). Instead, only about 9,000 IV within the set of 16 million are statistically significant (Bulub, 2012). That is, brute force tactics do not need to be used for RC4 since there is a relationship between the key stream output and the IV (Bulub, 2012). Based on this statistical fact, an attacker can filter for the cryptographically weak IVs (Bulub, 2012) to speed up the cracking process. Further, an attacker can speed up the process of gathering the critical number of IVs by causing the AP to generate more IVs instead of waiting for a client connected to an AP generate the IVs and intercepting the transmitted IVs (Srikanth, 2019).

The key stream is used to create the cipher text from the plain text by XOR-ing the plaintext with the key stream (Bulub, 2012). Therefore, what is needed to decrypt is only the key stream and not the key itself (Bulub, 2012). For example, an attacker only needs to wait for an IV to be reused to launch an attack (Bulub, 2012). Statistically, after about 5,000 IVs have been transmitted, there is a 50% chance that a random IV will be used (Bulub, 2012). The statistical attack works because WEP does not manage the IVs (Bulub, 2012).

II(C)(2). WEP Invariance Weakness in RC4 and RC4 key Chopped Away

As noted above, the IV is feed into the RC4 algorithm, wherein the output is the key stream, wherein the key stream is XORed with the message itself to create the cipher text (Srikanth, 2019). Even though the IV is discussed separately, the IV is part of the RC4 algorithm. As noted above, the IV and key being feed into the algorithm are correlated (Bulub, 2012). This correlation is called an invariance weakness (Lehembre, 2005). Therefore, RC4 is the source of the weakness (Srikanth, 2019).

It is important to note that some researchers have run tests manipulating the character set and the key length. For example, Tasoluk (2011) discusses how a 104-bit WEP key with a 62-character set will take over 6,000 years to crack. Further, originally WEP was release with a 40-bit key but it eventually

made it to 104 bits (Perez, n.d.). Eventually, there was a 256-bit key that was used (Martin, 2019). And it is a truism that a longer key will offer more protection. However, the tests run are based on a brute force method (Tasoluk, 2011). Essentially, the weakness of WEP does not lay within the *implementation* (that is, using the appropriate key length). Rather, the weakness of WEP lays with the vulnerable algorithms used within WEP.

Put another way, having a longer key *will* increase the time it takes to crack that key when using brute force (Tasoluk, 2011). However, long keys will not be saved from the chop-chop method by Korek (Lehembre, 2005). When Korek released chop-chop, this marked the end for WEP since a crack may only take 10 minutes (Lehembre, 2005).

II(C)(3). CRC32

WEP uses CRC which provides a low level of integrity since it is a checksum (Lehembre, 2005). Specifically, CRC is vulnerable due to its linearity (Perez, n.d.; Lehembre, 2005; Bulub, 2012). That is, for each bit changed in the IVC, there is a single bit that is changed in the message (Perez, n.d.; Lehembre, 2005; Bulub, 2012). Given CRC's linearity, an attacker would be able to undermined the integrity of a message with no way for a user to know that the message has been manipulated.

III. WPA

III(A). WPA History

This section will discuss WPA and how it was developed in view of the weaknesses found in WEP. WPS is a subset of 802.11(i) (Morris, 2003). As noted above, CRC is a linear function which undermined the integrity of the message for WEP (Perez, n.d.). WPA replaced noncryptographic

(Sheldon, n.d.) with a MIC called Michael (Sheldon, n.d.; Morris, 2003) which prevents replay attacks (Sheldon, n.d.).

With respect to Confidentiality in CIA, WPA continued to use RC4 (Sarmiento, 2008); however, WPA improved Confidentiality by replacing the static key management found in WEP with dynamic key management (Sarmiento, 2008) using TKIP sequence (Sarmiento, 2008). It is true that RC4 is vulnerable (Lehembre, 2005). However, the WIFI alliance was looking for a temporary and fast solution to the vulnerabilities in WEP. The primary issue was hardware(Sheldon, n.d.; Morris, 2003) . That is, AES required more robust hardware to replace RC4 (Sheldon, n.d.; Morris, 2003). Therefore, the temporary and fast solution was to deliver a firmware update while waiting for the hardware development to catch up at a later point in time (Perez, n.d.). In short, WPA was intended to a be a temporary solution, not a secure one.

III(B). WPA Mode

WPA provides two modes: PSK and Enterprise (Perez, n.d.). The WPA PSK utilizes a pre-shared key (Sheldon, n.d.). The PSK mode is more convenient and can be limited to a small office or home office (Sheldon, n.d.). Enterprise mode on the other hand uses an authentication protocol from the 802.1(x) standard (Sheldon, n.d.; Arana, 2006), wherein Enterprise has at least five (5) different standards (Arana, 2006). This authentication feature was an improvement to the MAC filtering authentication used in WEP (Bulub, 2012).[1]

[1] Sarmiento (2008) does not consider MAC filtering as a form of authentication. Either way, MAC filtering is not secure as MAC address can be readily spoofed. For example, MAC spoofing on Windows is easy as it only requires a manipulation of the registry.

III(C). WPA Technical

WPA uses the same stream cipher of RC4 but it utilizes TKIP sequence (Sheldon, n.d.). Additionally, the key is 128 bits instead of WEP's 48 bit key (Perez, n.d.) which makes WPA harder to crack (Sheldon, n.d.). The TKIP is a dynamic sequence which means that there are no longer static keys (Morris, 2003). Put another way, there are no duplicate keys and no weak keys generated (Perez, n.d.). However, TKIP has a higher computational cost (Sheldon, n.d.), and clearly the WIFI alliance was fine with this as there was no new requirement for hardware, only firmware update (Perez, n.d.). Lastly, the keys are SALT-ed with the SSID which adds more informational entropy. With randomized (i.e. nondefault) SSID, SALT-ing would prevent against precomputed hash tables (i.e. rainbow tables).

WPA also moved away from noncryptographic functions like CRC (Sheldon, n.d.), and instead opted for Michael which is a MIC of 64 bits (Sheldon, n.d.; Morris, 2003).

III(D). WPA Weakness

III(D)(1). WPA Weakness People and Passphrase

It is a truism that people are the greatest weakness to security. WPA is acceptable for small office or home office use (Sheldon, n.d.). However, many non-savvy home users might get frustrated with lengthy password and might opt for a simple password. According to Tasoluk (2011), 86% of passphrases are six (6) characters or less. PSK depends on a strong passphrase (Lehembre, 2005; Sarmiento 2008). This means many users are left vulnerable due to poor password usage.

III(D)(2). WPA Weakness Keys

Assuming that a strong passphrase is in place, PSK mode is still vulnerable as WPA can be brute forced with CoWPAtty or Aircrack-ng (Sheldon, n.d.). For example, there is an attack similar to the chop-

chop attacked called the Beck-Tews attack (Sheldon, n.d.) along with Hole196 on the Group Temp Key (Sheldon, n.d.). For another example, the creators of WPA wanted quick reconnection time and therefore they decided to reuse the old key to establish reconnection (Martin, 2019). Although this is a nice feature to speed up reconnection time, the KRACK attack exploits this vulnerability (Martin, 2019).

III(E). WPA Strengths

WPA is considered to be reasonably safe and is still in use today (Sarmiento, 2008). Sarmiento (2008) recommends, however, that WPA should not be used in the corporate world for security reasons.

IV. WPA2

IV(A). WPA2 History

The history of WPA2 will be understood in view of WPA. AES in WPA2 is one of the main differences between WPA and WEP (Sarmiento, 2008). WPA was intended to be a temporary solution for hardware that could not be readily provisioned (Gali, 2013). As the hardware caught up to speed, WPA2 became a reality.

IV(B). WPA2 Technical

With respect to Confidentiality, AES is one of the primary feature changes in the evolution of wireless communications, and moving from RC4 to AES changed the game (Srikanth, 2019). As noted above, RC4 was already known to be vulnerable prior to the release of WEP (Lehembre, 2005). With respect to Integrity, WPA2 uses CCM (Sarmiento, 2008).

IV(C). WPA2 Weakness

People are the greatest vulnerability when it comes to security. If WPA2 is in PSK mode, WPA2 can be brute forced with CoWPAtty or Aircrack-ng and retrieve the PSK (Sheldon, n.d.) Tasoluk (2011) finds that a 256 PSK with an 8-character passphrase can be broken from 100 micro seconds to 3.63 minutes with a 10-character set to 62 characters set, respectively. This is a huge deal weakness because 86% of people use a passphrase with 6 or less characters (Tasoluk, 2011). As noted above under the WPA section, many users are left vulnerable to attack by not utilizing secure passwords. If WPA2 is in Enterprise mode, hole196 supposedly can exploit a vunerablity in the EAP authentication framework (4 Hidden Security Threats).

IV(D). WPA2 Strengths

PSK is less security than Enterprise mode because when using eEAP, the brute force attacks with CoWPAtty or Aircrack-ng will not work (Sheldon, n.d.). As such, the best way to secure a network is to use eEAP (Sheldon, n.d.). This should be the method of choice for enterprise clients. Additionally, WPA can prevent replay attacks (Martin, 2019). Overall, WPA2 is not considered broken by most standards (Perez, n.d.).

V. WPS

V(A). WPS What is this?

Many everyday uses have trouble with configuring their wireless devices (How to set up…). Therefore, WPS is an easy way to set up wireless connections with a press of a simple button (How to set up…). WPA also has a PIN mode along with the push button (Rianto, 2013). The push button will

allow multiple devices to connect as one time along this might allow for unintended devices to jump in during the 2-minute window (Rianto, 2013). To stop unintended devices from joining the network, the PIN option may be used (Rianto, 2013), which is 8 bits long (Rianto, 2013). WPS can be used with the WPA/WPA2 frameworks (Rosdahl, 2015), and WPS is part of the EAP authentication frameworks (Sanatinia, n.d.).

It is commonly used today, and Wardriving shows about 38% of routers used WPS and had it enabled (Sanatinia, n.d.). It will be shown that many users with WPS are left exposed.

V(B). WPS Security

V(B)(1). WPS Security PIN and Math

WPS uses an 8-digit PIN which is split 4-4 (Rianto, 2013) because the first 4 operations act as a check point (Rianto, 2013). That is, the access point will provide an EAP-ACK or EAP-NACK for verification of the first 4 bits (Sanatinia, n.d.). Mathematically, instead of 8 digits of 10^8 calculations (100,000,000), there only needs to be 10^4+10^4 (20,000) calculations (Rianto, 2013). Further, the last bit is a check sum and therefore, an attack only needs to find 10^4+10^3 (11,000) calculations (Rianto, 2013). This means it takes less time to crack the code (Rianto, 2013).

V(B)(2). WPS Security Countermeasure

An obvious way to prevent brute force attacks are locking down the router (Rianto, 2013) and introducing delays (Sanatinia, n.d.), back offs, or timeouts (Rosdahl, 2015). However, many vendors did not introduce delays (Santina, n.d.). Similarly, in 2012, many routers did not provide back offs or timeouts (Rosdahl, 2015). Based on this, many routers are exposed to brute force attacks. So the clear question is: Why not just disable WPS?

Many security professionals do recommend disabling WPS such as Rosdahl (2015). However, not all vendors have a built-in disable feature for WPS, and this to access this, a firmware update is required (Rianto, 2013). Again, users are the biggest security threat and the average person will not patch their device (Sanatinia, n.d.).

V(B)(2). WPS Security Script Kiddie

Reaver is software that is open and available that is designed to exploit the weak PIN (Rianto, 2013; Sanatinia, n.d.). As such, the world is open for script kiddies to use predesigned programs and hack into people's WIFI. For example, Linksys E2000 can be cracked with PSK mode within 9 hours (Rianto, 2013; Sanatinia, n.d.).

VI. Public WIFI

VI(A). Public WIFI Inherently Dangerous

Public WIFI as the name indicates is "public," and it is open to for all to use. It is a truism that connection to a network, especially a physical network, *implies trust*. The thing that makes public WIFI so dangerous is that the implied trust by virtue of connection is undermined by the very medium of transfer, i.e. airwaves. It is well known that wardriving is a common tactic used by cyber criminals to connect to a network at distance. Additionally, it is well known that SSID spoofing is used by cyber criminals to use man in the middle attacks.

People are the greatest security risk. A layperson would connect to a malicious evil twin or rouge AP and fall victim to a MITM attack. Without knowing, they could easily be SSL stripped as most people are unaware do not check for the padlock that indicates a valid certificate. Using WPA2, WPA, and WEP will not save them.

Similarly, Mirzoev (2012) outlines that WPA is used; however, without client isolation, ARP spoofing and side jacking are threats to individuals on the network. Further, Srinivasan (n.d.) outlines that clients on the network lack information about the AP's authenticity.

VI(B). Public WIFI Countermeasures

First, Wright (2010) (the authors of our book) recommends using a static ARP in order to prevent ARP spoofing. Mirzoev (2012) remedy's ARP snooping by turning on PSPF. Additionally, by turning PSPF on, we can prevent ARP spoofing (Mirzoev, 2012). Client isolation is not activated by default for WEP, WPA, or WPA2 (Mirzoev, 2012).

Second, the PKI countermeasure is recommended by Srinivasan (n.d.) in order to give information about the authenticity of the AP. This will help prevent MITM attacks. (Srinivasan, n.d.). It is true that 802.1x, with certificates, could give us the authenticity we need; however, Enterprise versions of WPA are not easy to implement (Adams, 2019). As such, clients might not be willing to pay a large price for public WIFI with Enterprise mode. Srinivasan (n.d.) outlines VOUCH-AP. This alternative appears to be affordable.

Last, public WIFI can be password protected. Wieniawski (2011) recommends using WPA2 gives its strong unique key provisioning mechanism. That is, unlike WPA, each client that connects with a password would be given a different key (Wisniewski , 2011). Also, to keep the WIFI "public," he recommends having a trivial password such as free (even though you need 8 characters) (Wisniewski , 2011). It is true at this point, rainbow tables could be used to precompute and attack; however, other have noted that a modification to the SSID can be done, i.e. SALT-ing (Wisniewski , 2011). That is, if we have Starbucks, we could change the SSID to Starbucks <password>.

VII. Rating and Overview

This section will outline three (3) colors for each of the recommendation levels. A table will be precented and an explanation will be given. The explanation will distill the facts of the paper outlined in the above sections.

0 (RED) Never – This means never use this mode because a script kiddie can access the network. Based on this, the network will only offer protection equal to that of a wired connection.

1 (ORANGE) Reasonable – This is secure enough to be used day to day and/or for targets that do not require robust security.

2 (GREEN) Recommended– This is secure enough to be applied in the corporate world and/or it provides a secure framework that cannot be easily broken into based on a specific use case (i.e. “with”).

	WEP	WPA	WPA2	WPS
Home personal	0	1 with strong passphrase and with PSK	2 with strong passphrase and with PSK	0
Home office	0	1 with strong passphrase and with PSK	2 with strong passphrase and with PSK	0
Large organization	0	0	2 with 802.1(x)	0
Public	0	1 with PSPF and with static ARP entry and with VOUCH-AP	2 with PSPF and with static ARP entry and with VOUCH-AP and with provided password	0

VII(A) WEP.

My decision of rating WEP zeros (0) all the way down was an easy one. Confidentiality is very poor since it is based on RC4, and ever since chop-chop was released in 2004 security experts do not

even recommend this for home usage (Lehembre, 2005). Corporate clients require more robust security since they are targets for hackers given their deep pockets. Therefore, a system that is unsuited for a home user cannot be suited for a home office or large organization. Additionally, when WEP was designed, it was intended to be as secure as a wire connection (Gali, 2013; Bulub, 2012). Therefore, WEP's security was not place in the forefront. For Confidentiality, there are a flurry of other technical reasons for a zero rating all the way down such as static key usage (Gali, 2013; Lehembre, 2005), IV invariance (Bulub, 2012), a short IV (Srikanth, 2019; Perez, n.d.; Lehembre, 2005), and the like.

Most importantly, when it comes to determining WEP's rating, script kiddie tools such as airo-dump and aircrack-ng (Srikanth, 2019) must be taken into account. That is, when script kiddies with little to no training can crack a wireless system, that system should be considered broken. Especially, if the crack can occur in 10 minutes (Lehembre, 2005).

VII(B) WPA.

Some security experts submit that WPA is reasonably safe and may be used for more pedestrian networks such as home usage and home office (Sarmiento, 2008). Generally, these users do not have big pockets and are not the target of hackers. However, as established by Tasoluk (2012) many users (86%) do not use the proper length of password based on its respective character set. This leaves many users exposed to having their key cracked. Therefore, WPA can be said to be *contingently* and reasonably safe if a home user or home office has a proper password in place. WPA is open to attacks similar to chop-chop like the Beck-Tews attack (Sheldon, n.d.) along with hole196 on the group temp key (Sheldon, n.d.). Additionally, the KRACK attack exploits key management for reestablishing connections (Martin, 2019). Based on these vulnerabilities, I rate WPA for home and personal a one (1) or Orange.

For corporate clients, Sarmiento (2008) recommends using WPA2 and not WPA. This is true because WPA is open to attacks similar to chop-chop like the Beck-Tews attack (Sheldon, n.d.) along

with hole196 on the group temp key (Sheldon, n.d.). The KRACK attack exploits key management for reestablishing connections (Martin, 2019). Therefore, based on these vulnerabilities, a script kiddie could use CoWPAtty or Aircrack-ng (Sheldon, n.d.) and cause some havoc to corporate clients. This is why the corporate section gets a zero or red since corporate clients need more robust protection.

VII(C) WPA2.

This is the most secure protocol out of the three, and many security experts do not consider this broken (Perez, n.d.). Although PSK is less secure than Enterprise, CoWPAtty or Aircrack will not work on this (Sheldon, n.d.). However, even though WPA2 is not considered broken, it is important to consider the *implementation*. That is, people are the greatest risk to a network. Tasoluk (2012) discusses that 86% of users do not have proper password length. Having WPA2 framework in place will not alone protect a user. They need a strong password. Therefore, the rating of Green (2) on home office and persona use is contingent on the proper use of a password.

For our corporate clients, we want an extra layer of protection with the 802.1(x) authentication standards. This will protect them from MITM as some of the 802.1(x) standards authentication through CA's. Although, hole196 can exploit the EAP framework, the EAP is the most secure way protect a corporate client (4 Hidden Security Threats). When compared to WEP and WPA, WPA2 with EAP authentication is very secure. For these reasons, a recommendation rating of two (2) is given in Green.

VII(D) WPS.

WPS gets zeros and red all the way down. Simply put: the 8 bits are not properly utilized in the system. That is, the EAP-ACK and EAP-NACK undermine the math of the system (Sanatinia, n.d.). Instead of over 100,000,000 combinations to be checked against, only 11,000 need to be checked as the math breaks down to 10^4+10^3 (Rianto, 2013). There are countermeasures in place by *some* vendors such as back offs or timeouts (Rosdahl, 2015). But WPS did not systematically implement this feature into the

EAP authentication framework (Sanatinia, n.d.). Further, it is possible to do a firmware update to disable the WPS button, but the average person will not go to such length (Sanatinia, n.d.). Again, just like passwords and poor implementation, people are the greatest security threat. Additionally and practically, the world is open to script kiddies through the use of predesigned programs such as Reaver (Rianto, 2013; Sanatinia, n.d.). This allows WPS to be cracked in about 9 hours in some systems (Rianto, 2013; Sanatinia, n.d.).

I would not recommend WPS for any users (rating red and zero) given that a script kiddie could crack the system.

VII(D) Public WIFI.

This section is a row, not a column. That is, it is a way of using WIFI and not an IEEE or WIFI Alliance protocol. I would not recommend using WEP or WPS with public WIFI for the reasons state above. Specifically, WEP does not provide sufficient Confidentiality and Integrity. WPS is not mathematically as the EAP authentication framework (Sanatinia, n.d.) did not have back off or delays (Rosdahl, 2015) built in and cracking requires only 11,000 combinations that can be done quickly (Rianto, 2013).

As noted above, WPA can be considered reasonably secure. It would not place it in the recommended category for this because it uses RC4 (Lehembre, 2005). But if the public WIFI can be consider low security, we can liken this to a home or personal office and WPA might be viewed as acceptable.

However, I would add some contingencies such as implementing PSPF and static ARP. Additionally, an authentication framework such as VOUCH-AP should be used to prevent MITM attacks at a low cost compared against EAP.

If the public WIFI can be considered higher security. I would recommend still implementing PSPF and a static ARP entry with VOUCH-AP. However, I would additionally add that password protection be in place and a password could be handed out to the users of WIFI. This way, the key management system can be leverage and provide more confidentiality. That is, unlike WPA, each client that connects with a password would be given a different key (Wisniewski , 2011).

References Cited

4 Hidden Wi-Fi Security Threats. (2012, March 22). Retrieved December 01, 2020, from http://techgenix.com/4-hidden-wi-fi-security-threats/

Adams, J. (2019). WiFiCue: Public Wireless Access Security Assessment Tool. Retrieved December 3, 2020, from https://arxiv.org/pdf/1910.04325v1

Arana, P. (2018, December 28). Arana - 2006 - Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2).pdf - Benefits and Vulnerabilities of Wi-Fi Protected Access 2(WPA2 Paul: Course Hero. Retrieved December 01, 2020, from https://www.coursehero.com/file/36644663/Arana-2006-Benefits-and-Vulnerabilities-of-Wi-Fi-Protected-Access-2-WPA2pdf/

BULBUL, H., BATMAZ, I., & OZEL, M. (2012, July 04). Wireless network security: Comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols. Retrieved December 01, 2020, from https://eudl.eu/doi/10.4108/e-forensics.2008.2654

Cache, J., Wright, J., & Liu, V. (2010). *Hacking exposed wireless: Wireless security secrets and solutions*. New York, NY: McGraw-Hill.

Gali, T. (2013). A Comparative Study between WEP, WPA and WPA2 Security ... Retrieved December 1, 2020, from http://www.ijsr.net/archive/v4i5/SUB154986.pdf

How to Set up the Secured Wireless Connection using WPS. (n.d.). Retrieved December 1, 2020, from http://www.edimax.com/images/Image/FAQ/Wireless/General-Wireless/How_to_Setup_the_Secured_Wireless_Connection_using_WPS(the-most-user-friendly-Standard-Wireless-Security-Technology).PDF

Lehembre, G. (2005). Wi-Fi security – WEP, WPA and WPA2. Retrieved December 1, 2020, from http://tele1.dee.fct.unl.pt/rit2_2015_2016/files/hakin9_wifi_EN.pdf

Martin, A. (2019). WEP VS WPA2 Encryptions. Retrieved November 30, 2020.

Mirzoev, D., & White, S. (2014, April 08). The Role of Client Isolation in Protecting Wi-Fi Users from ARP Spoofing Attacks. Retrieved December 03, 2020, from https://arxiv.org/abs/1404.2172

Morris, K. (2003). Wireless Security: Past, Present, and Future. Retrieved December 01, 2020, from https://cyber-defense.sans.org/resources/whitepapers

Perez, J. (n.d.). A SURVEY OF WIRELESS NETWORK SECURITY PROTOCOLS.

Rianto, I. (2013). ANTICIPATING WPS PIN VULNERABILITY TO SECURE WIRELESS NETWORK. Retrieved December 1, 2020, from https://journal.binus.ac.id/index.php/comtech/article/download/2554/1962

Rosdahl, A. (2015). Hands-on with wifi security v2 - OWASP. Retrieved December 1, 2020, from https://owasp.org/www-pdf-archive/Hands-on_with_wifi_security_publish.pdf

Sanatinia, A. (n.d.). Wireless Spreading of WiFi APs Infections using WPS Flaws ... Retrieved December 1, 2020, from http://www.ccs.neu.edu/home/sashank/publications/wps_ieee_cns.pdf

Sarmiento, O. P. (2008). (PDF) Basic security measures for IEEE 802.11 wireless ... Retrieved December 1, 2020, from https://www.researchgate.net/publication/262458771_Basic_security_measures_for_IEEE_80211_wireless_networks

Sheldon, F. T. (n.d.). (PDF) The Insecurity of Wireless Networks. Retrieved December 1, 2020, from https://www.researchgate.net/publication/260635283_The_Insecurity_of_Wireless_Networks

Srikanth, I. V. (2019). Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3). Retrieved December 01, 2020, from https://www.researchgate.net/publication/334445004_Review_on_Wireless_Security_Protocols_WEP_WPA_WPA2_WPA3

Srinivasan, A. (n.d.). VOUCH-AP:priVacypreservingOpen-access 802 ... Retrieved December 3, 2020, from https://cis.temple.edu/~jiewu/research/publications/Publication_files/Srinivasan_IJSN_2018.pdf

Tasoluk, B., & Tanrikulu, Z. (2011, March 02). A Weakest Chain Approach to Assessing the Overall Effectiveness of the 802.11 Wireless Network Security. Retrieved December 01, 2020, from https://arxiv.org/abs/1103.0464

Wisniewski, C., Wisniewski, C., Says:, J., Says:, L., Says:, K., Says:, C., . . . Mitchell, D. (2011, February 11). Dear Starbucks: The skinny on how you can be a security hero. Retrieved December 01, 2020, from https://nakedsecurity.sophos.com/2010/11/09/dear-starbucks-the-skinny-on-how-you-can-be-a-security-hero/