Survey of the security risks of Wi-Fi networks based on the information elements of beacon and probe response frames

Estudio de los riesgos de seguridad de redes Wi-Fi basado en los elementos de la información de tramas beacon y probe response

H. I. Reyes-Moncayo; L. D. Malaver-Mendoza; A. L. Ochoa-Murillo

***Abstract*— Wi-Fi networks have become prevalent in homes, businesses, and public places. Wi-Fi is one of the most common means that people use to access digital services like Facebook, WhatsApp, Instagram, email, and even payment platforms. Equipment for deploying Wi-Fi networks is affordable and its basic features are easy to manipulate. In many cases Wi-Fi users do not even have to buy any communication equipment, since Wi-Fi routers are installed by internet service providers (ISP) in the premises of their customers. Wi-Fi equipment, owned either by end users or ISP companies, should be configured as securely as possible to avoid potential attacks. The security capabilities and features of Wi-Fi routers and access points are inserted into beacon and probe response frames. Potential attackers can use sniffing tools like Wireshark to capture these frames and extract information about security features to discover vulnerabilities. In order to assess the security risks of Wi-Fi networks we conducted a survey in which we used Wireshark to capture the traffic from several Wi-Fi networks, and then through a filter we selected the beacon and probe response frames to analyze the security information elements carried by those frames. We came to the conclusion that despite technical recommendations, some security parameters and options are still set in a way that makes networks more prone to attacks. With this paper we want the readers to be aware of the security risks of their Wi-Fi networks, even the ones set up by their internet service providers.**

***Index Terms*— Beacon frames, IEEE802.11, RSN, Security, TKIP, Wi-Fi, Wireshark, WPS.**

***Resumen*— Las redes Wi-Fi se han vuelto prevalentes en hogares, empresas y lugares públicos. Wi-Fi es uno de los medios más comunes que las personas usan para acceder a servicios digitales como Facebook, WhatsApp, Instagram, correo electrónico e incluso plataformas de pago. El equipo para implementar redes Wi-Fi es asequible y sus características básicas son fáciles de manipular. En muchos casos, los usuarios de Wi-Fi ni siquiera tienen que comprar un equipo de comunicación, ya que los enrutadores de Wi-Fi son instalados por los proveedores de servicio de Internet (ISP) en las residencias de sus clientes. Los equipos de Wi-Fi, sean propiedad de los usuarios finales o de las empresas ISP, deben configurarse de la manera más segura posible para evitar posibles ataques. Las capacidades y características de seguridad de los enrutadores Wi-Fi y los puntos de acceso se insertan en las tramas beacon y probe request. Los posibles atacantes pueden usar herramientas de escaneo, como Wireshark, para capturar dichas tramas y extraer información sobre las características de seguridad para descubrir vulnerabilidades. Con el fin de evaluar los riesgos de seguridad de las redes Wi-Fi, se realizó un estudio en el cual se usó Wireshark para capturar el tráfico de varias redes Wi-Fi, y posteriormente a través de un filtro se seleccionaron las tramas beacon y probe response para analizar los elementos de información de seguridad llevados por esas tramas. Se concluyó que a pesar de las recomendaciones técnicas algunos parámetros y opciones de seguridad están configurados de una manera que hace las redes más susceptibles a ataques. Con este artículo queremos que los lectores sean conscientes de los riesgos de seguridad de sus redes Wi-Fi, incluso las configuradas por sus proveedores de servicio de internet.**

***Palabras claves*— beacon TKIP, IEEE802.11, RSN, Seguridad, Tramas, Wireshark, Wi-Fi, WPS.**

I. INTRODUCTION

Wi-Fi networks have become prevalent in homes, work places, malls, and other public places. Wi-Fi is currently the most common and accessible way to share internet connections. The increase in the number of smart phones and other wireless devices has motivated the deployment of Wi-Fi networks. Wi-Fi networks play an important role in the digital life of many people that rely on Wi-Fi connections due to their low cost. This low cost comes with the high cost of risking sensible data when the networks are set without taking into consideration technical recommendations.

This manuscript was submitted on February 27, 2020 and accepted for publication on September 28, 2020.

H. I. Reyes Moncayo is with the Universidad de los Llanos, Villavicencio, Meta, Colombia (e-mail: hreyes@unillanos.edu.co).

L. D. Malaver Mendoza was with the Universidad de los Llanos, Villavicencio, Meta, Colombia. He is now with Pragmatic SAS, Bogotá, Colombia (e-mail: lui.malaver@unillanos.edu.co).

A. L. Ochoa Murillo was with the Universidad de los Llanos, Villavicencio, Meta, Colombia. She is now with Sophos Solutions, Bogotá, Colombia (e-mail: Andrea.ochoa@unillanos.edu.co)

Wi-Fi routers are affordable and some users do not even have to purchase one because their internet providers install them as part of their service. It is a common practice that the only configuration parameters modified on the Wi-Fi routers, at the time of installation and during their operative life, are the name of the network, technically known as SSID (Service Set Identifier), and the password, leaving the other parameters untouched. Using the factory default configuration ignoring security parameters might open the door to attackers, which with little effort and free tools can get access to the Wi-Fi networks. Our survey demonstrates that security recommendations issued by reputable organizations, such as the Wi-Fi alliance and the United States Computer Emergency Readiness Team (US-CERT) are neglected in a high percentage of Wi-Fi networks.

This paper is organized as follows: We start by giving a brief overview of Wi-Fi security, its beginnings, evolution, and the last significant update, WPA3. Then, we explain how information security is embedded in beacon and probe response frames. In the next section, we explain the security risks made visible by the WPS (Wi-Fi Protected Setup), RSN (Robust Security Network), and WPA (Wireless Protected Access) information elements. In the next section, we present a real-life survey where we captured Wi-Fi traffic from different networks at different locations in Villavicencio, Meta, Colombia; we explain how we extracted the data from the aforementioned information elements. Following the presentation of the survey, we present and discuss the results explaining the security risks and how to mitigate them. Finally, we make conclusions.

II. Wi-Fi Security Overview

The security of Wi-Fi networks can be seen as pre-RSN (Robust Security Network) and RSN. RSN is specified by means of the IEEE 802.11i amendment issued in 2004. Before IEEE802.11i the options to offer confidentiality were reduced to WEP (Wired Equivalent Privacy) and the authentication was either open or by means of a shared key. These security methods were soon broken, forcing the Wi-Fi-alliance to come up with the IEEE 802.11i amendment. IEEE 802.11i established the RSN age of Wi-Fi networks introducing several methods for authentication, confidentiality, data integrity, key management, and access control as shown in Fig. 1 [1].

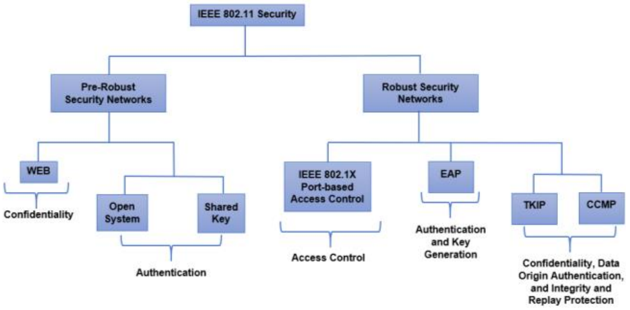

IEEE 802.11 Security
Pre-Robust Security Networks
Robust Security Networks
WEB
Confidentiality
Open System
Shared Key
Authentication
IEEE 802.1X Port-based Access Control
Access Control
EAP
Authentication and Key Generation
TKIP
CCMP
Confidentiality, Data Origin Authentication, and Integrity and Replay Protection

Fig. 1 Taxonomy of Wi-Fi security [1].

The RSN methods shown in Fig. 1 are better known as WPA (Wireless protected access) and WPA2, each one having two levels: personal and enterprise. WPA and WPA2 personal are intended for use in SOHO (Small Office Home Office) and home networks, whereas WPA and WPA2 enterprise are for medium and large-scale networks. The main difference between the personal and enterprise levels lies in the authentication method: The personal level uses pre-shared key authentication (PSK), whereas the enterprise one uses IEEE802.1X authentication. RSNs are established through RSN associations (RSNAs), security relationships based on the IEEE802.11i 4-way handshake that allows for the protection data frames and enhanced security. Security features enabled by RSNs are: enhanced user authentication mechanisms, cryptographic key management, data source authentication and integrity, data confidentiality, protection against replay. Pre-RSN networks, like WEP, used only one key or a small number of keys for all the devices, and lacked a standard mechanism to distribute keys. RSN introduced two key hierarchies: the pairwise key hierarchy for protecting unicast traffic, and the group key hierarchy for protecting broadcast and multicast traffic. The keys are for securing the traffic through three services: encryption, authentication, and integrity. IEEE802.11i defines that pairwise keys can be installed through two mechanisms:

Pre- Shared Key (PSK): A PSK is a static key given to the access point (authentication server -AS) and the stations (STA) through a secure mechanism. The PSK should be loaded into the devices before the association stage. The IEEE standard does not specify how to generate or distribute the PSK; therefore, organizations should review their PSK implementation to detect vulnerabilities. For big organizations the PSK distribution might be infeasible.

Authentication, Authorization, and Accounting Key (AAAK): Also known as a Master Session Key (MSK), the AAAK is loaded into the AP during the RSNA establishment by means of an Extensible Authentication Protocol (EAP). The AAAK changes each time a user starts a session, authenticates to the WLAN and lasts until the key lifetime expires or the user re-authenticates. EAP operates directly over data link layers, such as IEEE802.3 and IEEE802.11 [2]. IEEE802.11i defines three components: the supplicant, the authenticator, and the authentication server (AS). The supplicant is a piece of software run by the clients wanting to associate with the access point. The authenticator is the access point. The authentication server contains and validates the authentication information. EAP passes authentication information between the supplicant and the AS. The authenticator, the access point, is an intermediary between the supplicant and the AS [3].

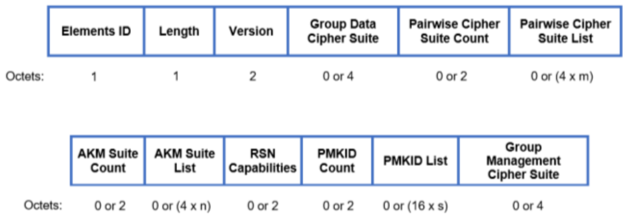
An improvement to IEEE802.11i, is WPA3. WPA3 introduced in 2018 uses the most advanced cryptographic methods [4]. WPA3 is compatible with WPA2, disallows outdated legacy protocols, such as WEP and TKIP, and mandates the use of protected management frames (PMF). PMF, optional in WPA2, prevents attacks that use disassociation and de-authentication frames, explained later in this paper. Currently, WPA3 is optional for certified Wi-Fi devices, but when the market grows and consolidates, it will become mandatory. Like WPA2, WPA3 comes in two versions: WPA3-Personal and WPA3-Enterprise.

WPA3-Personal uses Simultaneous Authentication of Equals (SAE), defined in the standard IEEE 802.11-2016 [5], instead of PSK used by WPA2-Personal. SAE is robust against offline dictionary attacks where the adversary tries to steal network passwords by testing possible passwords without interacting with the network. This capability provides the users with more robust password-based authentication even when they use simple passwords; therefore, users can choose passwords easier to remember. Additionally, WPA3-Personal provides forward secrecy (FS); which means that data are protected even if a password is compromised after the data has been transmitted. With FS a unique session key is created each time a user stars a session; therefore, if a key is compromised, it will only affect the data exchanged using that particular key.

WPA3-Enterprise builds upon WPA2 and introduces the following features: 256-bit Galois/Counter Mode Protocol (GCMP-256) for authenticated encryption; 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384) for key derivation and confirmation; Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve for key establishment and authentication; and 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) for robust management protection. WPA3-Enterprise also offers 192-bit, an optional feature more secure than the current 128-bit encryption [6].

III. Security Information Embedded In Wi-Fi Frames

Beacon and probe request frames contain security information that the wireless stations need to know prior to establishing RSN associations (RSNA) with the access points. One of the pieces of information contained in those frames is the RSN (Robust Secure Network) information element, RSNIE. Fig. 2 shows the RSNIE [5]. The element ID field, whose value is 48, differentiates the RSNIE from other elements contained in the frame. The length indicates the number of bytes that come after it. The version indicates the version number. In an RSN several cipher suites are used. The field *group data cipher suite* indicates the encryption algorithms used to protect multi-cast data frames. The field *pairwise cipher suite list* tells which algorithms are used to protect unicast frames. The field *AKM* (authentication key management) suite list indicates if the authentication method is either PSK or EAP. The fields *PMKID count* and *PMKID list* only travel within association and re-association request frames. PMKID is the unique key identifier used by the AP to keep track of the PMK (primary master key) being used for the client. Of special interest is the *RSN capabilities* field, which indicates the requested and advertised capabilities. This field indicates whether or not the access point requires and is capable of protecting management frames. Other subfields of *RSN capabilities* have replay counters to prevent replay attacks to multi-cast and uni-cast frames. When the management frames are being protected, the field *group management cipher suite* indicates the cryptographic algorithms used to protect multi-cast management frames; the unicast management frames are protected with the same algorithms used to protect unicast data frames.

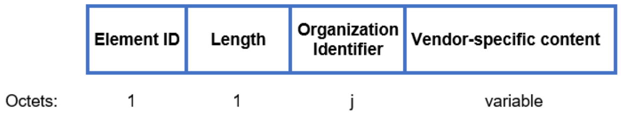


	Elements ID	Length	Version	Group Data Cipher Suite	Pairwise Cipher Suite Count	Pairwise Cipher Suite List
Octets:	1	1	2	0 or 4	0 or 2	0 or (4 x m)

	AKM Suite Count	AKM Suite List	RSN Capabilities	PMKID Count	PMKID List	Group Management Cipher Suite
Octets:	0 or 2	0 or (4 x n)	0 or 2	0 or 2	0 or (16 x s)	0 or 4

Fig. 2 RSN Information Element (RSNIE).

Some beacon and probe response frames also have vendor specific elements. These elements carry information not defined in the standard; they are organized in a format that helps to prevent interoperability issues. The format for this element is in Fig. 3. One common vendor specific element is the Microsoft Corp. element type WPS, which indicates if WPS is enabled in the access point. WPS (Wi-Fi Protected Access) is a method created by the Wi-Fi alliance to facilitate the connection to home networks to inexperienced users. Another vendor specific information element is the WPA information element from Microsoft, which repeats some of the fields carried by the RSNIE.



	Element ID	Length	Organization Identifier	Vendor-specific content
Octets:	1	1	j	variable

Fig. 3 Vendor specific element

IV. Security Risks

The information provided by the RSNIE and some other vendor specific elements makes evident the risks under which Wi-Fi networks operate. Starting with the field RSN capabilities, if protection of management frames is not required, a door is open for de-authentication and disassociation attacks, which aim at disconnecting legal users by sending forged de-authentication and disassociation frames. With tools such as Scapy [7], it is possible to forge the aforementioned frames with the source MAC address equal to the BSSID (Basic Service Set ID), so that the client stations see the frames as legitimate and proceed according to the type of frame: de-authentication or disassociation. By default, management and control frames are not protected; therefore, it is not necessary for the attacker to know any password. Just with the BSSID and the MAC address of the client to be attacked, the attacker can forge the frames to make the target client disconnect from the AP. BSSID and client MAC addresses are easily obtained by means of free tools like Wireshark [8]. These attacks are used not only for disconnecting users, but also to force them send authentication and association frames again, so they can be captured and analyzed to extract passwords.

The fields containing cipher suite information let the potential attackers know if the network uses TKIP encryption, AES encryption or both. TKIP was an intermediate algorithm between WEP and WPA2 -AES. TKIP was intended as a software update to improve the safety of 802.11 hardware operating with WEP. Beck and Tews [9] in 2009 demonstrated that it is possible to inject frames with custom payload in a network protected with MIC (message integrity check), used by TKIP for integrity protection. AES, introduced through WPA2, required new hardware and promised to be at the moment a definitive solution to the vulnerabilities of TKIP; however, in 2017 Vanhoef [10] discovered vulnerabilities in the WPA2 standard itself and was able to decrypt frames from WPA2 networks. Since those vulnerabilities belong to the standard, any WPA2 device is affected disregarding its configuration. To be protected against the KRACK attack, the devices must be patched [11].

TABLE I
SAFETY RISKS AND POSSIBLE SOLUTIONS

Attack	Field of beacon frame and its unsecure value[a]	Possible Solution
Deauthentication attack	RSN Capabilities: Management Frame Protection Required: False	Use of protected management frames through IEEE802.11w
Disassociation attack	RSN Capabilities: Management Frame Protection Required: False	Use of protected management frames through IEEE802.11w
WPS attack	Wi-Fi protected setup state: Configured	Disabling WPS in the AP
Injection of frames with custom payload	Cipher Suite: TKIP	Disabling TKIP and using only CCMP(AES)
KRACK attack	None: since the attack takes advantage of a WPA2 weakness	Patching the device

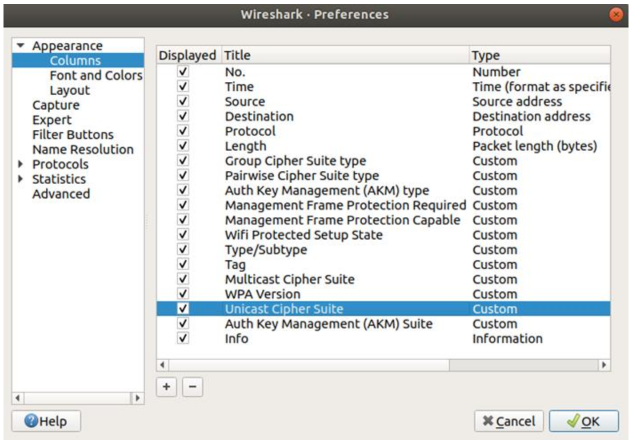
[a] This column shows the fields of beacon frames and the values of these fields that facilitate attacks. This also applies to probe response frames.

If WPS is enabled, there is another door open [12]. WPS uses a PIN as a mechanism to provide the client with connection information such as the WPA password. The client simply needs to provide the PIN number to gain access to the authentication credentials. Through freely available tools, such as Fern Wi-Fi Wireless Cracker [13] and Reaver [14], the WPS PIN can be obtained in 4 to 10 hours [12].

Table I summarizes the security risks that potential attackers can discover through the information embedded in beacon and probe response frames; it also suggests the solutions to ameliorate or eliminate the risks.

V. REAL LIFE SURVEY

We conducted a survey wherein we captured Wi-Fi traffic at different locations in the City of Villavicencio. The goal of the survey was to analyze the information embedded in beacon and probe response frames in order to discover security risks. To conduct the survey, we used Wireshark installed on an Ubuntu 18.04 machine. We set the Wi-Fi interface to monitor mode, so we were able to capture all the details of the IEEE802.11 frames. We captured Wi-Fi traffic from 150 access points at different places of Villavicencio. We combined all the capture files into a single one for analysis purposes. The default Wireshark view has few columns such as source, destination, protocol, and info. To conduct the analysis, we added to the Wireshark view the necessary columns, Fig. 4. After having all the necessary columns, we filtered the capture to visualize only the beacon and the probe response frames, we finally exported the results to a .csv file and did the data wrangling in Pandas. The whole process is illustrated in Fig. 5.



Displayed	Title	Type
☑	No.	Number
☑	Time	Time (format as specifie
☑	Source	Source address
☑	Destination	Destination address
☑	Protocol	Protocol
☑	Length	Packet length (bytes)
☑	Group Cipher Suite type	Custom
☑	Pairwise Cipher Suite type	Custom
☑	Auth Key Management (AKM) type	Custom
☑	Management Frame Protection Required	Custom
☑	Management Frame Protection Capable	Custom
☑	Wifi Protected Setup State	Custom
☑	Type/Subtype	Custom
☑	Tag	Custom
☑	Multicast Cipher Suite	Custom
☑	WPA Version	Custom
☑	Unicast Cipher Suite	Custom
☑	Auth Key Management (AKM) Suite	Custom
☑	Info	Information

Fig. 4 Wireshark columns used to conduct the survey.

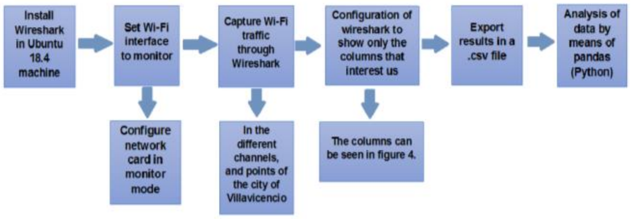

Install Wireshark in Ubuntu 18.4 machine
Set Wi-Fi interface to monitor
Capture Wi-Fi traffic through Wireshark
Configuration of wireshark to show only the columns that interest us
Export results in a .csv file
Analysis of data by means of pandas (Python)
Configure network card in monitor mode
In the different channels, and points of the city of Villavicencio
The columns can be seen in figure 4.

Fig. 5 Wi-Fi frame capture and analysis.

VI. RESULTS AND DISCUSSION

We summarized the results in the following pie charts. The survey tells us that although vulnerabilities of some Wi-Fi protocols and features have been reported, in many cases they are ignored and no corrections have been implemented. We observed that WPS is still used in a significant percentage of the observed networks. WPS vulnerabilities were reported back in 2011 [12]. Fig. 6 shows that WPS is enabled in 43.9% of the access points, disabled in 5.7%, and not supported in 50.4%. That means in half (50.4%) of the access points the manufacturers did not installed support for WPS; however, in the other half (43.9% plus 5.7%) that supports WPS, this protocol is enabled in most of the APs; 43.9% out of 49.6%, which is 88.5% of the APs that support WPS. This situation could be easily solved by accessing the administration web page of the AP and disabling WPS; however, in many cases access to the AP administration is blocked to the users, since the ISPs are the owners of these devices; therefore, they are the ones that should disable this functionality. According to our results, some internet providers are either unaware of the WPS vulnerability or just indifferent to it.

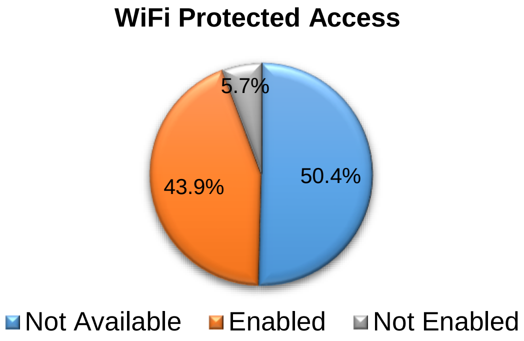


Fig. 6 Wi-Fi Protected Setup Statistics

Fig. 7 shows that 87.8% of the APs lack the management frames protection capability, whereas 5.7% of the APs have this capability. 6.5 % of the APs did not add the RSN information element to the frames; therefore, for these APs no information is available regarding the protection of management frames.

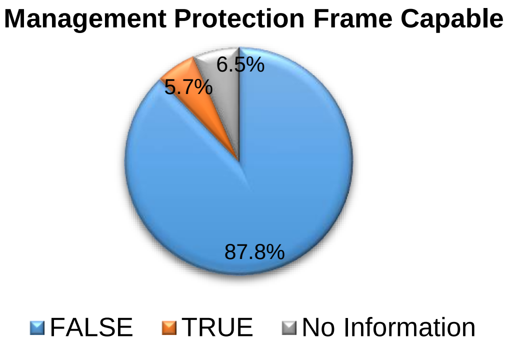


Fig. 7 Management Protection Frame Capable Statistics.

Fig. 8 shows that 93.5% of the APs do not require the protection of management frames. 5.7% of the APs have the PMF capability; however, none of them require the management frames to be protected; therefore, they accept protected and unprotected management frames. The consequence of setting PMF to required is that only PMF capable stations can associate to the AP. The RSNIE is missing in 6.5% of the frames; therefore, information about the PMF requirement is not available

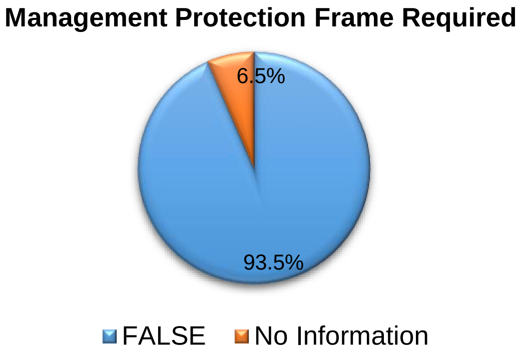


Fig. 8 Management Protection Frame Required Statistics

Information about the pairwise and groupwise ciphers, and the authentication management keys is carried by the RSNIE or the WPA information element. Depending on the AP, the beacon and probe response frames can carry both information elements, just one, or none. In our study we found all these cases. The beacon and probe response frames with WPA information element come from APs in transition to RSN. If the frames have only RSNIE, the APs are IEEE802.11i complaint. If none of the aforementioned information elements are present, the APs probably are very old; that is the case for 4.1% of the Aps. Fig. 9 shows the percentages for the types of pairwise traffic ciphers. 45.5% of the APs use only AES, the recommended practice; however, 47.2% use both TKIP and AES, and 3.3% use only TKIP. Supporting TKIP is not a good practice, due to the vulnerabilities already reported; even the Wi-Fi Alliance on a technical note discouraged the use of TKIP in 2015 [15]. Although WPA2 has been broken recently, it is still safer than TKIP [16]. Let us not forget that TKIP was a temporary mechanism, introduced in 2004, to solve the vulnerabilities of WEP without changing the hardware; nowadays when the vast majority of hardware has been upgraded, it is surprising TKIP is still in use, ignoring the recommendation of the Wi-Fi alliance [15].

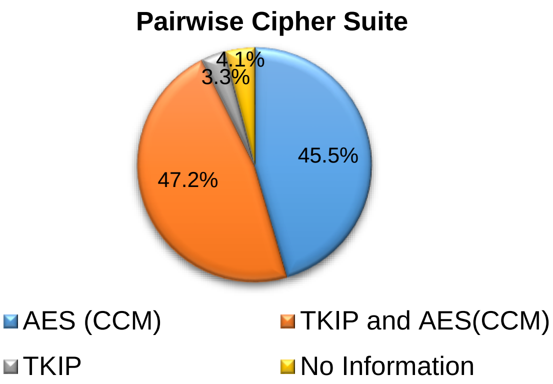


Fig. 9 Pairwise Cipher Suite Statistics

We have a similar situation with the groupwise ciphers: 50.4 % of the AP use only TKIP, while 45.5% use only AES, figure 10.

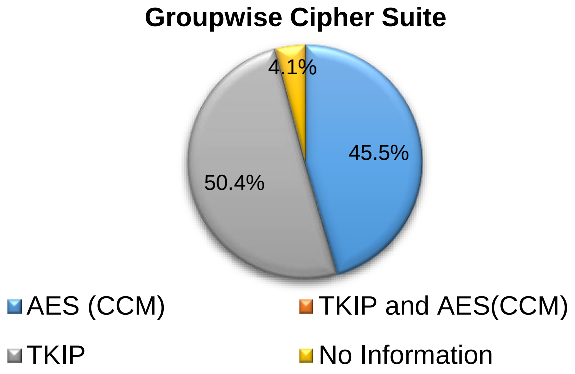


Fig. 10 Groupwise Cipher Suites Statistics.

Disabling TKIP can be done easily via the administration graphical interface of APs. As in the WPS case, the final users have no access to that interface. According to the Wi-Fi alliance's 2015 technical note, already mentioned, TKIP should be disabled by default in Wi-Fi certified devices, and access to any TKIP option should not be available in the main administrative graphical interface, but only through a secondary interface in the case that access for legacy devices, only TKIP, is required; however, vendors, installers of Wi-Fi devices, and ISPs still enable TKIP.
In our survey, PSK was the only authentication management key mechanism that we were able to observe: 95.9% of the APs use PSK, the other 4.1% don't transmit RSNIE; therefore, they are not IEEE802.11i complaint, Fig. 11

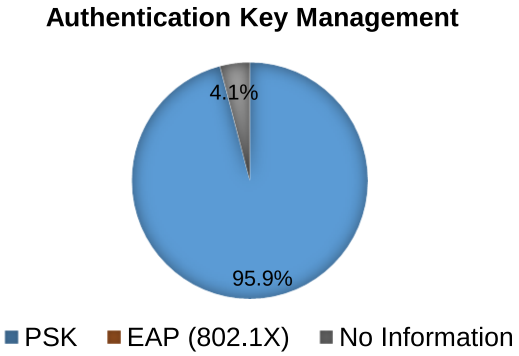


Fig. 11 Authentication Key Management Statistics.

We have commented on known vulnerabilities and how to reduce the risk by doing simple changes to the configuration of access points and Wi-Fi routers. Unfortunately, none of these recommendations can prevent the KRACK attack, which takes advantage of IEEE802.11 standard flaws and is not preventable by changing the configuration of devices [10]. We can protect devices from the Krack by means of patches. A list with patches available for devices from several vendors is available in [17]. Considering that the Wi-Fi Alliance will not enforce the use of WPA3 for certifying devices in the near future, WPA2 will still be present in our lives for some more years; therefore, it is necessary to protect our current WPA2 devices as much as possible.

VII. Conclusions

We have used Wireshark to capture Wi-Fi traffic at different locations in the city of Villavicencio in Colombia. We have focused our work on analyzing some information elements, carried by beacon and probe response frames, which contain data indicating security features and capabilities. In our analysis we found that a significant percentage of networks operate ignoring the latest recommendations and still use insecure protocols, whose vulnerabilities were reported around a decade ago. WPS is still broadly used putting in risk home networks; something that can be easily solved by just disabling the WPS option in access points and Wi-Fi routers. TKIP, whose use has been discouraged by the Wi-Fi Alliance, is still in use despite of the fact that AES, more robust cipher, is available in all the Wi-Fi devices manufactured and certified as of 2004. Although one technical reason for keeping TKIP is to allow legacy devices, pre-RSN, to connect to Wi-Fi networks, the good practice is to have separated networks for those legacy devices, where additional security measures are in place. What we observed is that TKIP and AES devices share the same networks making the latter vulnerable to the weaknesses of the former. As in the WPS case the solution is to disable TKIP through the web interface of the affected devices. The protection of management frames is neither available nor enabled in most of the devices we observed. The solution to this security flaw could be a simple configuration task, but it also might imply a software or hardware update. Protection against the KRACK attack implies patching the devices, when the patch is available, or buying new equipment. The internet service providers, who install Wi-Fi routers as part of their service, and internet subscribes that deploy their own Wi-Fi networks should be more aware of the risks that come with the convenience of Wi-Fi.

References

[1] S. E. Frankel, B. Eydt, L. Owens, and K. K. Scarfone, "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i | NIST," *Special Publication (NIST SP) - 800-97*, Feb. 2007. DOI: 10.6028/NIST.SP.800-97

[2] J. R. Vollbrecht, B. Aboba, L. J. Blunk, H. Levkowetz, and J. Carlson, "Extensible Authentication Protocol (EAP)." [Online]. Available: https://tools.ietf.org/html/rfc3748. [Accessed: 26-Mar-2019].

[3] "802.1X Overview and EAP Types," *Intel*. [Online]. Available: https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-i-o/wireless-networking.html. [Accessed: 26-Mar-2019].

[4] "Security | Wi-Fi Alliance." [Online]. Available: https://www.wi-fi.org/discover-wi-fi/security. [Accessed: 26-Mar-2019].

[5] "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, Dec. 2016.

[6] M. Koziol, "Wi-Fi Gets More Secure: Everything You Need to Know About WPA3," *IEEE Spectrum: Technology, Engineering, and Science News*, 06-Sep-2018. [Online]. Available: https://spectrum.ieee.org/tech-talk/telecom/security/everything-you-need-to-know-about-wpa3. [Accessed: 27-Mar-2019].

[7] P. B. and the S. community, “Scapy.” [Online]. Available: https://secdev.github.io/. [Accessed: 30-Jan-2019].

[8] “Wireshark · Go Deep.” [Online]. Available: https://www.wireshark.org/. [Accessed: 30-Jan-2019].

[9] E. Tews and M. Beck, “Practical Attacks Against WEP and WPA,” in *Proceedings of the Second ACM Conference on Wireless Network Security*, New York, NY, USA, 2009, pp. 79–86. DOI: 10.1145/1514274.1514286

[10] M. Vanhoef and F. Piessens, “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS ’17*, Dallas, Texas, USA, 2017, pp. 1313–1328. DOI: 10.1145/3133956.3134027

[11] “KRACK Wi-Fi attack threatens all networks: How to stay safe and what you need to know,” *PCWorld*, 08-Nov-2017. [Online]. Available: https://www.pcworld.com/article/3233308/security/krack-wi-fi-security-flaw-faq-tips.html. [Accessed: 14-Feb-2019].

[12] “Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack | US-CERT.” [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA12-006A. [Accessed: 29-Jan-2019].

[13] “Fern Pro | Downloads.” [Online]. Available: http://www.fern-pro.com/download. [Accessed: 30-Jan-2019].

[14] “Google Code Archive - Long-term storage for Google Code Project Hosting.” [Online]. Available: https://code.google.com/archive/p/reaver-wps/. [Accessed: 30-Jan-2019].

[15] T. Campbell, “Technical Note: Removal of TKIP from Wi-Fi Devices,” p. 3, 2015.

[16] “WPA2 ‘KRACK’ Attack,” *SANS Internet Storm Center*. [Online]. Available: https://isc.sans.edu/forums/diary/22932/. [Accessed: 08-Apr-2019].

[17] C. Osborne, “Here’s every patch for KRACK Wi-Fi vulnerability available right now,” *ZDNet*. [Online]. Available: https://www.zdnet.com/article/here-is-every-patch-for-krack-wi-fi-attack-available-right-now/. [Accessed: 08-Apr-2019].

Hector I. Reyes Moncayo, received the Ph.D. degree in electrical engineering from the University of North Dakota, Grand Forks, USA in 2014, the MSc. degree in teleinformatics and the B.S. degree in electronics engineering from the Universidad Distrital Francisco José de Caldas in 2003 and 1993 respectively. In 2009 he received the Fulbright scholarship to pursue doctoral studies in the USA. He is with the Universidad de los Llanos, Villavicencio - Colombia, working as an assistant professor. His research interests include cognitive radio, software defined radio, wireless networks, and networking.
ORCID: https://orcid.org/0000-0002-4299-6315

Luis D. Malaver Mendoza, received the B.S degree in systems engineering from the Universidad de los Llanos in 2020. During his years as a student he participated in the networks and applications research group at the same university. He participated in an internship for the design and development of a software for managing socioeconomic benefits at the Universidad de los Llanos. As of July 2020 he is with Pragmatic SAS, Bogotá - Colombia, working as a development engineer. His research interests include communication and information security.

ORCID: https://orcid.org/0000-0002-6970-2209

Andrea L. Ochoa Murillo, received the B.S degree in systems engineering from the Universidad de los Llanos in 2019. During his years as a student he participated in the networks and applications research group at the same university. In 2018, she participated in an internship for the design and development of a software for managing the enrollment of students in the undergraduate and graduate programs offered by the Universidad de los Llanos. As of April 2019 she is with Sophos Soluctions, Bogotá - Colombia, working as a software developer. His research interests focus on telecommunications security.

ORCID: https://orcid.org/0000-0003-3959-0477