ISSN 1870-4069

Cryptography in Wireless Network Penetration Testing

Claudio Casado[1], Cristian Barría[2], Lorena Galeazzi[3]

[1] Universidad Mayor, Santiago, Chile
[2] Pontificia Universidad Católica de Valparaíso, Valparaíso, Chile
[3] Instituto Profesional DuocUC, Santiago, Chile
[1] claudio.casadob1@mayor.cl, [2] cristian.barria@ucv.cl
[3] l.gale.ava@gmail.com

Abstract. At present, wireless accesses are experiencing exponential growth worldwide, not being unrelated to various attacks on the integrity, availability and confidentiality of information; Resulting in the implementation of security measures. Based on the above, the protection of the data is of transcendental importance and together with this the implementation of cryptographic systems at the level of organizations and end users. This is why the present research exposes the different variables that must be considered during security tests to obtain information, and with the purpose of achieving a contribution to protection methodologies that are incorporated in the different components of the wireless networks.

Keywords: wireless, pentesting, criptography.

1 Introduction

Based on the internet service exposure, this has been a key role in the technological growth of telecommunications, increasing its development curve, thanks to the ability to entertain the user to maintain an uninterrupted connection, where society demands the creating new systems that satisfy their demand and needs, directing technological progress towards the transfer of information independent of physical media such as cable. The foregoing is reflected in figures for wireless technology growth at the national level, where in recent years internet access points have grown by 45.3% between 2014 and 2016, reaching 73.8% of the population, playing at the same time in a more important activity in the activity of the common things, to the economic transactions and the private and public communications [2].

In spite of the above, the suppliers of the item have focused their efforts on improvements and advances oriented to functionalities and quality of the connections, without considering the security that should have the devices that are part of the network [3].

Along with the growth of the above-mentioned technology, there is a similar growth in the associated security incidents. Under an international context, between 2016 and 2017, the concerns of companies in Latin America on information security issues have increased by an average of four percentage points [4].

On the other hand, at the level of end users, the gap between them and the security that revolves around the technology in question reaches worrying levels, since, according to the company Norton, only 48% of users are able to determine if a wireless network is secure. Within the same study, 35% of users have at least one unprotected device connected to their network [5]. Cyber-attacks and espionage activities in the network, massive interception of telecommunications networks, disruption of the internet service, espionage and attacks against critical infrastructures and governmental entities, have set the guidelines in this area [2].

In view of the above, the existence of studies that support Information Security Management Systems (ISMS) with accurate data to obtain a baseline assessment of the risk associated with the null or inadequate implementation of the different methods is problematic. cryptographic devices that provide security for wireless networks. As a consequence, it is sought, as a contribution, to propose a risk assessment associated with the aforementioned variable that will serve as a basis to support both security testing and the preparation of security plans in support of ISMS. The second section presents related works that explain the current encryption mechanisms and the variables that could imply a risk for the network. In the third section, a risk analysis based on OWASP methodology is carried out. Finally, in the fourth section, we present the conclusions, analyzes and future work that emerge from the results of the risk analysis.

2 Related Work

The main characteristic of wireless networks is the ability to generate a connection between a transmitting device and a receiving device, taking into account the only condition in which it must be within the transmission range of the signal remittent. The independence based on its wireless structure provides the end users mobility, faculty responsible for the momentum in the vertiginous growth of this technology [6].

Given the above, one of the biggest problems to be considered is security in Wi-Fi networks where Detect, isolate and prevent malicious acts that, if realized, would cause much greater effects on the network is the goal. It is thus that the most important actions to take into account to safeguard the security of a network and its information, are the identification and authentication of users in addition to the classification of the risks associated with these characteristics [7].

In response to the need to provide user identification and authentication to wireless networks, the Institute of Electrical and Electronic Engineers (IEEE) implements the 802.11 standard in 1999, which registers remarkable advances as time passes and technology advances. only in the frequencies that it uses and its maximum speed of transmission, but in the mechanisms of encryption that it uses to grant security to the moment a user wants to enter the network [6].

Some of the most important security mechanisms involve encryption and key management mechanisms to achieve the aforementioned security features [8] [3].

The cryptographic mechanisms of the IEEE standard mentioned above are: WEP, WPA and WPA2, in chronological order of implementation. The former proved, through numerous investigations, to be extremely vulnerable as it uses RC4 encryption, with public key transmitted in clear text and does not offer end-to-end security.

The second is more secure than WEP because it was created as a corrective measure within the 802.11i update of the IEEE standard given the insecurity presented by its predecessor. WPA includes integrity control to the messages it manages. It uses Michael encryption algorithm (MIC) and TKIP (Temporal Key Integrity Protocol). Finally, WPA2 was created to convince its predecessor as a secure encryption mechanism, being more robust, efficient and complex to break than WEP and WPA since in addition to the features incorporated in the latter, it includes 4 Ways Handshake and CBC-MAC encryption algorithm, in addition to CCMP-AES as security protocol [8, 3]. As a means of authentication, enterprise networks use the EAP framework (with different versions of it, such as LEAP, PEAP, EAP-TTLS, EAP-TLS, EAP-FAST, EAP-MD5) Pre-Shared Key (PSK). Both features are present in both WPA and WPA2. The encryption mechanisms described above are still in force today, but these are the ones that predominate in the default configurations in WEP, which, despite their validity as a crypto-do mechanism, does not guarantee the minimum of security that justifies its activation by default, making it tend to be considered obsolete. Details on the operation and characteristics of the above are summarized in Table 1 [8].

Table 1. Encryption protocols in wireless networks and their characteristics.

Characteristics	WEP	802.11i	
		WPA	WPA2
Security Protocol	RC4	TKIP	CCMP
Cipher	RC4	RC4	AES
Key Length	40 or 104 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24 bit IV	48 bit IV	
Key Generation	Concatenation	Two phase mixing function	Not needed
Data Integrity	CRC-32	Michael	CBC-MAC
Header Integrity	None	Michael	CBC-MAC
Replay Protection	None	Packet Number	
Key Management	None	EAS-based	
Authentication	Open or shared key	802.11x or PSK	
Wi-Fi Alliance Certificate (WPS)	Active/No Active		

Although WPS is not a feature of encryption mechanisms, it affects the security they seek to provide, since in their desire to facilitate the installation and configuring of known devices on the network, it leaves aside, without compensation, the security provided by the encryption techniques associated with authentication [9].

Once the characteristics associated to the different cipher-do mechanisms have been described, a more specific description of the variables that represent, today, a security risk given by these mechanisms (see Table 2).

Table 2. Definition of variables.

	Variable	Description
WEP	Key	Corresponds to the key of access to the network defined by the administrator of this one [3]
	Keystream	Corresponds to the result of the XOR binary operation between a WEP key and a given Initialization (IV) Vector [6]
WPA	PSK	It corresponds to the authentication process for a specific client or device. It is known as four-way handshake since it uses 4 validations of the authentication [3]
	EAP-Handshake	It works in conjunction with WPA-PSK to add a secure "wrapper" to the information that travels between the AP and the client when performing a four-way handshake [3, 8].
	TKIP Encryption	Encryption type that allows to deliver confidentiality to data packets traveling through the network [7]
WPA2	4-way Handshake	Authentication process used by this protocol [10].
WPS	PIN	Functionality present in APs using the eight-digit PIN exchange with client device for easy connection, installation and configuration [9].

3 Risk Analysis

As defined by the Open Web Application Security Project (OWASP) in its risk analysis methodology, it is calculated according to the following equation [11]:

$$Risk = Likelihood * Impact. \tag{1}$$

The first step to carry out this methodology is to identify the variables that could represent a risk. Secondly, an estimate must be made of the probability that exploitation of such risk will be effective based on the identified vulnerabilities. Finally, one must determine the impact that the exploitation of each of the vulnerabilities can have. To analyze qualitative variables OWASP recommends the assignment of values between one and ten that allow to establish ranges that define if a vulnerability and / or associated risk correspond to High, Medium or Low. The methodology in question recommends the use of sub-factors to establish a more accurate quantitative assessment based on qualitative variables [11].

For the calculation of the risk (R) associated to a variable, in the present work it is considered the use of two sub-factors for the calculation of the probability of occurrence. These are the popularity of the attack (P) and its simplicity (S) where its average multiplied by the impact factor (I), results in the desired estimate. Given the above, the equation for risk analysis would be the following:

$$R = \left(\frac{P * S}{2}\right) * I. \tag{2}$$

Given the above (equation 2), the measurement levels for probability and impact are defined by associating at low level the values from one to less than four, as mean scores between one and less than seven, and finally as high ones that go from seven to ten. Given the variables and methodology defined above, each of these is valued for subsequent risk analysis. A risk weighting will be performed for each of the malicious acts, extracting in turn an overall risk average pertaining to each of the cryptographic variables reviewed in this work: WEP, WPA / WPA2, WPS [3, 12]. Table 3 shows the results of the risk analysis carried out for each type of attack.

Table 3. Risk weighting for attacks associated with cryptographic variables.

Protocol	Variable	Attack	P	S	I
WEP	WEP Key Recovery	FiOS SSID WEP Key Recovery	9	10	8
		Neesus Datacom 21-bit attack	8	9	8
		Dictionary Attack	4	10	8
		Cryptographic Attack	7	5	8
		Using Aircrack-ng (Client Attached)	7	5	8
	Keystream Recovery	Chop-Chop Attack	4	4	7
WPA	Breaking Authentication WPA-PSK	Obtaining the Four-Way Handshake	7	4	9
		Cracking the PSK	7	4	9
		Decrypting WPA-PSK Captures	6	4	6
	Obtaining the EAP-Handshake	Attacking LEAP	4	6	8
		Attacking PEAP & EAP-TTLS	7	4	9
		Attacking EAP-TLS	1	1	10
		Attacking EAP-FAST	5	5	9
		Attacking EAP-MD5	4	7	7
	Braking Encryption TKIP	Beck-Tews Attack	4	4	8
WPA2	4-way Handshake	KRAK Attack	3	2	7
WPS	WPS Attack	Brute-force Hack	10	10	10

Once the previous tabulation has been performed, the calculation of the weighted general risk is performed for each of the encryption methodologies, as shown in Table 4.

Table 4. Likelihood and Impact Weighting for WEP, WPA, WPA2 and WPS.

WEP			WPA			WPA2			WPS		
Likelihood		Impact	Likelihood		Impact	Likelihood		Impact	Likelihood		Impact
P	S	I	P	S	I	P	S	I	P	S	I
6,5	7,2	7,8	5	4,3	8,3	3	2	7	10	10	10
6,8		7,8	4,7		8,3	2,5		7	10		10

After the previous tabulation was carried out, the calculation of the general risk weighted for each cryptographic variable according to the methodology proposed by OWASP (Table 5).

Table 5. Matrix for obtaining real risk for each cryptographic variable.

		Overall Risk Severity		
Impact	High	Medium (WPA2)	High (WEP y WPA)	Critical (WPS)
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Low	Medium	High
	Likelihood			

4 Conclusions and Future Work

It can be concluded from the present work that although cryptography and encryption mechanisms seek to grant users authentication in a network, they will not fully comply with this role if the security configurations necessary to reduce the risk present in this type of technologies. Factors such as the obsolescence of some of these mechanisms, make a network insecure despite having the technology and corresponding updates to achieve this goal. The deactivation of WPS and the use of WPA2 within the configurations of the router are good basic and recommended minimum practices to mitigate the present risk in a network.

Although a risk analysis applied in an organization considers more sub-factors of analysis specific to the business context, through the present work we seek to contribute with a risk analysis that serves as a basis for the generation of con-science about the null or incorrect application of security on a network infrastructure. This allows both to support strategies and methodologies for performing security tests on this type of technology, and to support ISMSs through clear information that serves as a basis for the development of plans and policies for associated good safety practices to the protection of wireless networks.

As future work, it is proposed to carry out similar work to quantify the risk associated with other variables present in the wireless networks, further reinforcing the contribution to the problem raised in this research, supporting both the ISMS and the associated pentesting methodologies.

References

1. Salvetti, D.: Redes Wireless. 1era Edición, Buenos Aires: Fox Andina, Dalaga (2011)
2. National Security Council of Chile: National Cybersecurity Policy (NSP) for 2017–2022. https://www.ciberseguridad.gob.cl/media/2017/05/NCSP-ENG.pdf
3. Cache, J., Wright, J., Liu, V.: Hacking Wireless Exposed: Wireless Security Secrets & Solutions. McGraw Hill (2010)
4. Laboratorios ESET: ESET Security Report Latinoamérica (2017)
5. Symatec Corporation: Norton Cyber Security Insights Report (2016)

6. Wadhwa, U.: Wireless Network Security: Tough Times. In: International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 1022–1025 (2015)
7. Troya, A., Astudillo, J., Romero, C., Sáenz, F., Díaz, J.: Vulnerability Detection in 802.11i Wireless Networks Through Link Layer Analysis. In: IEEE Latin-América Conference on Communications (LATINCOM) (2014)
8. Hassan Adnan, A., Abdirazak, M., Shamsuzzaman Said, A., Anam, T., Zaman Khan, S., Mahmudur Rahman, M., Musse Omar, M.: A comparative study of WLAN security protocols: WPA, WPA2. In: International Conference on Advances in Electrical Engineering, Nº 3, pp. 165–169 (2015)
9. Instituto Nacional de Ciberseguridad de España: Qué es WPS Pin y por qué debes desactivarlo. Oficina de Seguridad del Internauta (2014)
10. Vanhoef, M., Piessens, F.: Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys. USENIX, vol. XXV, pp. 673–688 (2017)
11. OWASP Foundation: About The Open Web Application Security Project (2018)
12. Gonzalez-Pérez, P., Sanchez-Garcés, G., Soriano de la Cámara, J.M.: Pentesting con Kali. 0xWord (2013)