Evaluation of the WPA2-PSK wireless network security protocol using the Linset and Aircrack-ng tools

Evaluación de seguridad en protocolo de red inalámbrico WPA2-PSK usando las herramientas Linset y Aircrack-ng

Avaliação de segurança em protocolo de rede sem-fio WPA2-PSK usando as ferramentas Linset e Aircrack-ng

Alberto Acosta-López*
Elver Yesid Melo-Monroy**
Pablo Andrés Linares-Murcia***

Fecha de recepción: 13 de septiembre de 2017
Fecha de aprobación: 27 de diciembre de 2017

Abstract

Due to the emergence of new techniques and technologies of intrusion, the wireless network protocols have become obsolete; for this reason, this research seeks to violate and evaluate the security of the WPA2 protocol that is widely used by the Colombian service providers. The first section of this paper introduces the WPA2 protocol by describing its operation and the potential attacks it may suffer; the second part details the methodology used to collect the tests data and to carry out the evaluation necessary for the preparation of this article. In addition, we present the Linset and Aircrack-ng tools for auditing wireless networks that were selected to assess the security of the protocol. Finally, we show the results and conclusions.

Keywords: data security; information security; intrusion detection; wireless security.

Resumen

Debido al surgimiento de nuevas técnicas y tecnologías de intrusión, los protocolos de redes inalámbricas quedan obsoletos; para ello se busca vulnerar la seguridad del protocolo WPA2, que es ampliamente usado por los proveedores de servicios colombianos. En la primera parte, el artículo hace una introducción del protocolo WPA2, describiendo su funcionamiento y los ataques de los cuales puede ser objeto; en la segunda parte se muestra la metodología que se usó para recolectar pruebas y realizar la evaluación necesaria para la elaboración de este documento. Se presentan las herramientas para auditoria de las redes inalámbricas Linset y Aircrack-ng, las cuales fueron seleccionadas para la evaluación de seguridad del protocolo. Finalmente, se muestran los resultados y las conclusiones.

Palabras clave: detección de intrusión; seguridad de datos; seguridad de la información; seguridad inalámbrica.

* M. Sc. Universidad Distrital Francisco José de Caldas (Bogotá-Distrito Capital, Colombia). aacosta@udistrital.edu.co.
** Universidad Distrital Francisco José de Caldas (Bogotá-Distrito Capital, Colombia). eymelom@udistrital.edu.co.
*** Universidad Distrital Francisco José de Caldas (Bogotá-Distrito Capital, Colombia). paalinaresm@udistrital.edu.co.

Resumo

Devido ao surgimento de novas técnicas e tecnologias de intrusão, os protocolos de redes sem-fio ficam obsoletos; para isso, busca-se vulnerar a segurança do protocolo WPA2, que é amplamente usado pelos provedores de serviços colombianos. Na primeira parte, o artigo faz uma introdução do protocolo WPA2, descrevendo seu funcionamento e os ataques dos quais pode ser objeto; na segunda parte mostra-se a metodologia que se usou para coletar provas e realizar a avaliação necessária para a elaboração deste documento. Apresentam-se as ferramentas para auditoria das redes sem-fio Linset e Aircrack-ng, as quais foram selecionadas para a avaliação de segurança do protocolo. Finalmente, mostram-se os resultados e as conclusões.

Palavras chave: detecção de intrusão; segurança de dados; segurança da informação; segurança sem-fio.

Cómo citar este artículo:
A. Acosta-López, E. Y. Melo-Monroy, and P. A. Linares-Murcia, "Evaluation of the WPA2-PSK wireless network security protocol using the Linset and Aircrack-ng tools," *Rev. Fac. Ing.*, vol. 27 (47), pp. 71-78, Jan. 2018.

I. Introduction

Cyber-attacks are a growing trend in modern Colombian society. These attacks impact users with information on the Internet [1] because the information traffic generated when files are moved from a computer or cell phone to the Internet, always creates an encryption that allows hiding information frames and packages necessary between the modem and the sending device. For this reason, it is necessary to know how such information packages, which contain important information for the security of our data, are attacked.

A. What is WPA2-PSK?

Among the existent wireless networks that allow interconnecting two or more computers to transmit data, the best known are WPAN (Wireless Personal Area Network), WLAN (Wireless Local Area Network), WMAN (Wireless Metropolitan Network), and WWAN (Wireless Wide Area Network). Each network has an associated protocol and IEEE standard that allow the review and the subsequent communication in a local or global network. We will focus on the WLAN wireless network with WPA2-PSK protocol based on the IEEE 802.11i standard that was released on July 24, 2014 [3-5].

WPA (Wireless Protected Access) originated in the problems detected in the WEP, a previous security system created for wireless networks [6]. WPA2-PSK (PSK acronym for Pre-Shared Key) is the evolution of the WPA protocol; it implements an algorithm based on a key of 8 to 63 characters, which is taken as a parameter, and with this value, a new key is randomly generated [6].

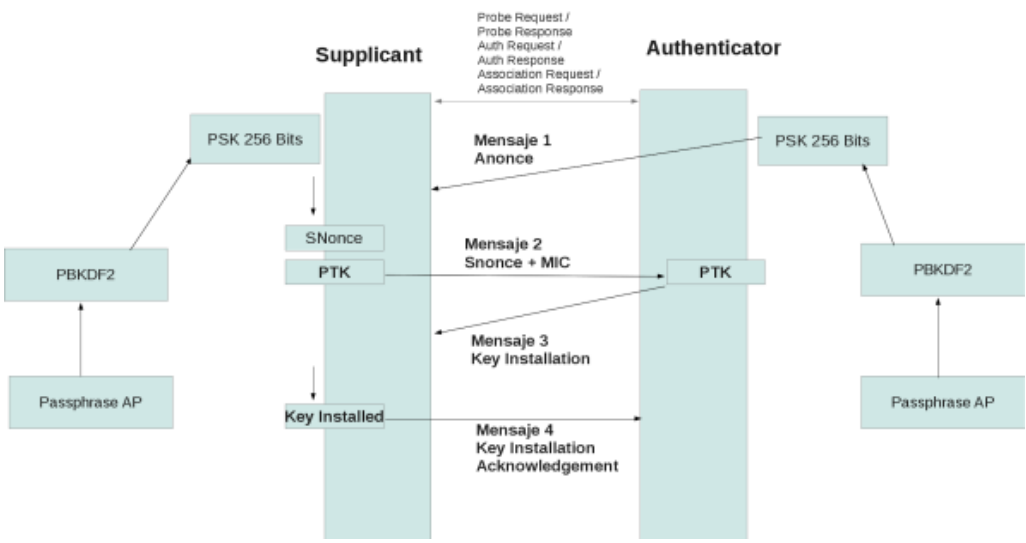

Fig.1 Operation of the protocol WPA2-PSK [6].

The operation of WPA2-PSK involves the following steps (Fig. 1):

1. The authenticator sends a message to the supplicant with a value generated randomly using its PSK key (an arbitrary value with no special meaning). This message is known as an authenticated nonce or simply nonce, because it contains a field called nonce whose value is generated randomly with the PSK key of the authenticator, as shown in Fig. 1, which was captured with Wireshark. In addition, the Replay Counter is an indicator that allows the authenticator and the supplicant to know the number of packages that have been previously sent [6].

2. The supplicant receives the message and generates another message called snonce (supplicant nonce), which is basically of the same type as the received anonce package, but contains a different nonce (an arbitrary text generated randomly using the PSK key of the supplicant) [6].

3. With the previous information, the supplicant creates the Pairwise Transient Key (PTK); this step is extremely important and, therefore, the

reader should pay more attention, because is where the "magic" of PSK and the dynamic generation of keys take place, which was implemented in the beginning to improve the security of WEP against fairly widespread attacks. PTK are the keys generated in each packet exchanged between the supplicant and the authenticator, and are generated using the Pairwise Master Key (PMK), but they are the same PSK code generated in step 1; that is, each PTK is generated dynamically by the supplicant PSK and the authenticator [6].

4. The procedure for generating the PTK key is really important, hence, its understanding is necessary. The PTK is generated by the PMK using a PTK random key generation function that takes the following parameters: 1) anonce, which is the package generated by the authenticator that contains a random text encrypted with its PSK key; 2) snonce, which is the package generated by the supplicant that contains a random text encrypted with its PSK key; 3) MAC authenticator; and 4) MAC supplicant [6].

5. The supplicant sends a packet to the authenticator with the snonce message and a MIC field (field encrypted using the Michael encryption mechanism) that allow performing an integral and consistent check of the packet; this field is generated by the supplicant using the PTK and the PMK [6].

6. With the package sent by the supplicant in step 5, the authenticator derives the PTK key, since it already knows the fields necessary to do the calculation: PMK, which is the same for both the supplicant and the authenticator, anonce, snonce, and the MAC addresses of the authenticator and the supplicant [6].

7. Once the authenticator has generated the PTK with the fields received from the previous packet (with the snonce field), it tries to generate the MIC field, since it has the same PTK and PSK as the supplicant. The MIC generated by the authenticator and the supplicant must be the same, and if that is the case, the authenticator sends a message to the supplicant of the type "Key Installation"; this message can be seen with the "Flag" of the type "Install Flag", which in turn can be seen in the third package exchanged in the authentication process [6].

8. The supplicant sends to the authenticator a "Key Install Acknowledgment" message, which simply confirms that, in this session of package exchange, the same PTK generated in the client and the AP were used. This package contains a "Key ACK" field with a value of zero, indicating that it is the last message sent in the authentication process between the supplicant and the authenticator [6].

Once the function of the WPA2-PSK protocol is understood, we can perform different types of attacks to detect its vulnerabilities.

B. Types of attack

Modems that create wireless networks for their users are vulnerable to several types of attack. The most common attacks are the following:

1. *SYN saturation attack*: flood network traffic. In other words, a single individual makes a large number of requests to the server, in this case the modem, which denies access to the rest of its users [7].

2. *DoS attack*: It is a denial of service attack [8].

3. *DDoS attack:* it is an extension of the DoS attack, but it attacks from different connection points [8].

4. *Identity theft:* Phishing is based on social engineering that focuses on the fact that humans make the greatest errors [8].

5. *Attack by intermediary:* It diverts packet information by changing it and returning altered information, or just checking what information is being handled by the target user [8].

II. Methodology

A. Software

1) WIFISLAX. Operating system based on Linux that can be used as a live cd or boot access on a USB; it was designed by www.seguridadwireless.net, and was adapted for Wireless [9]. This OS is an audit tool for wireless networks that contains a set of tools to function.

2) Linset. Application to audit wireless networks that does not use decryption dictionaries to obtain the access code to the network. With this tool, the cooperation of the user, who is unaware of the attack, is of vital importance, which implies that the user has little or no knowledge of computer security. Linset creates a fake AP with the same ESSID, as the one we are attacking and without any type of encryption; in addition, it authenticates the APs of the legitimate clients, preventing them to authenticate, and making them access the AP created by this tool and enter the password of the network [10].

3) Operation. This tool attack the modem, allowing network users to connect, and then, creating a fake network to which users will connect and provide the network password. Once the password is obtained, the fake network is closed and the modem operation is released.

4) Aircrack-ng. Complete suite of tools that audit wireless Wi-Fi networks. This tool focuses on different areas of security in wireless networks: packet-monitoring, attack, testing, and cracking [11].

5) VMware Workstation PRO (trial version). This tool is one of the industry standard products to run multiple operating systems as virtual machines on a single PC. Thousands of IT professionals, developers, and businesses use Workstation Pro and Workstation Player to improve agility, productivity, and security [12].

6) Windows 8 Pro (trial version). New operating system created by Microsoft. In this case, we will use Windows pro test version for the development of this research.

B. Hardware

Modem ZTE ZXV10 W300E (for home network use)

Desktop computer corei7 16 RAM

Network adapter TP-LINK WN725 (Does not support monitoring)

Network adapter TP-LINK WN722N (Supports packet monitoring)

C. Methods

The modem was configured to generate a wireless network called Security, use the WPA2-PSK protocol, and generate the password for accessing the newly created network. In this case, the network was called PruebaArticulo, and the password was @Prueba@.

We performed the audit using *attack by intermediary* and *DoS attack* (for using decryption dictionaries known as brute force), and run ten tests for each technique.

First, we carried out a brute-force attack, that is, an information package was captured with the wireless network encrypted access key. Afterwards, we carried out an impersonation attack, in which a third network that impersonates the original network is created, while the victim sends the password of his/her wireless network. In both attacks, we evaluated anonymity and waiting time to obtain access.

III. Results

This study allowed us to understand better the use of the audit tools. The focus of our analyses was to highlight the vulnerabilities of the security protocol; for this, we studied the following items: time to obtain the password, method, and visualization of the attack (Table 1).

Table 1

Comparative table between the Linset and Aircrack tools

	Linset	Aircrack
Method	Create an alternate network to capture the access key	Use repositories of dictionaries to make the comparison
Time	The time it takes to obtain a password is related to the lack of technical knowledge or ignorance on the part of the user	The time depends on the type of password security this can last from one to six months
Viewing the network client	It can be perceived by the network client	The network client is not aware of the attack of which he is being victim
Avoidable attack	The attack can be avoided	The attack can not be avoided

Table 2 shows the length (hours) of each of the 10 tests conducted with the Aircrack tool; whereas Table 3 shows the length (minutes) of the attacks with the Linset tool.

Table 2

Length (in hours Approx.) of an attack with Aircrack

Nø Test	Time (Hours)
1	11
2	15
3	10
4	12
5	24
6	16
7	17
8	12
9	14
10	21

Table 3

Length (in min Approx.) of an attack with Linset

Nø Test	Time (Minutes)
1	14
2	7
3	15
4	5
5	11
6	9
7	5
8	7
9	14
10	11

The network attack using Linset was one of the most effective; however, this is not because of the results, but because of the lack of defense methods. Therefore, as long as the attacker has a good network card, the attack is imminent and difficult to avoid if the user is unaware of it.

IV. Discussion

Although companies in Colombia like Digiware are dedicated to computer security, no system is 100 % safe. What is really important for an adequate protection of our data is education; however, how do we obtain this knowledge? Are the supplier companies willing to give us basic training to at least change the password of our wireless network? The truth is that the knowledge we have today is quickly becoming obsolete, particularly in technology; what before lasted a little over a year, nowadays only last for weeks or sometimes days. In the current information age, it is necessary to have a minimum of security in our data, which is why a question arises: who will train us for this?

This article presents two tools to evaluate the security of our wireless networks, and the way the WPA2 security protocol works. Additionally, we provided elementary knowledge about the different types of attacks that currently affect wireless networks. Evidently, besides computer viruses, the attacks to the network infrastructure are problematic because they allow access to the users' sensitive data.

V. Conclusions

Linset employs more advanced techniques than Aircrack, seeking the ingenuousness of the user to appropriate the network´s password. It also uses a technique of alternative creation of networks contrary to Aircrack, which collects identification packages; in terms of time, Aircrack method is more expensive than Linset. Aircrack attacks on vulnerable networks are totally unavoidable, therefore, it would be necessary to find a solution. The delay time that the Linset tool has against Aircrack is limited with respect to time: A Linset attack is limited by the user´s patience who usually does not tolerate more than 15 minutes without giving up the password. An Aircrack attack is limited by the power of the attacking machine; depending on the capacity of the machine, the search can take from days to weeks or even up to one month.

Depending on the management of the company, it is necessary to train the employees to identify the attacks on the networks, and thus avoid providing relevant information so the attacker can access the network. A mechanism to increase the security of entry to a private Wi-Fi network is the authentication through the devices Mac addresses. This mechanism not only allows the known devices to access, but also provide a degree of security.

Author contributions

Alberto Acosta supervised the study. Pablo Linares was the rapporteur of the project, made the first tests, and created the base methodology. Elver Melo helped validating the results and complemented the technical and bibliographic data for the realization of the practice.

Acknowledgments

The authors acknowledge the collaboration and funding from the research group TRHISCUD (Treatment of clinical historical information –Universidad Distrital) of the Engineering School at the Universidad Distrital Francisco José de Caldas. We plan to continue with this collaboration in future studies.

References

[1] D. Lemos, "El secreto en la nube," [Online]. Available: http://www.digiware.net/?q=es/blog/el-secreto-de-la-nube [Accessed Apr. 30, 2017].

[2] R. Juan, "Redes inalámbricas Principales protocolos," 2011. [Online]. Available: http://deredes.net/redes-inalambricas-principales-protocolos/ [Accessed Apr. 28, 2017].

[3] A. Hassan Adnan, "A comparative study of WLAN security protocols: WPA, WPA2," in *International Conference on advances in Eletronical Engineering (IEEE)*, Dhaka, Bangladesh, 2015.

[4] Intel, "Wi-Fi diferentes protocolos y velocidades de datos," 2017. [Online] Aviable: http://www.intel.la/content/www/xl/es/support/articles/000005725/network-and-i-o/wireless-networking.html [Accessed May. 20 2017].

[5] IEEE "802.11-2016 - IEEE Standard for information technology," 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7786995/ [Accessed May 21, 2017].

[6] J. Ruz Maluenda, B. Riveros Vasquez, and A. Varas Escobar, "Redes WPA/WPA2," [Online] Available: http://profesores.elo.utfsm.cl/~agv/elo322/1s12/project/reports/RuzRiverosVaras.pdf [Accessed May. 20, 2017].

[7] Ciberseguridad wikia, "Ataques TCP/IP," 2013. [Online] Available: http://es.ciberseguridad.wikia.com/wiki/Ataques_TCP/IP [Accessed May. 24, 2017].

[8] S. Dietrich, D. Dittrich, and P. Reiher. Denial of Service. *Attack and Defense Mechanisms*. NJ: Prentice Hall. 2004.
[9] Wifislax "Presentación," [Online] Available: http://www.wifislax.com [Accessed Jun. 4, 2017].
[10] A. Maroto, "Crackeando Redes Wi-Fi: WPA y WPA2 –PSK," 2016 [Online] Available: http://www.tic.udc.es/~nino/blog/lsi/reports/wpa.pdf [Accessed Jan. 20, 2017].
[11] Aircrack-ng, "Introduction," [Online] Available: http://www.aircrack-ng.org/doku.php [Accessed Mar. 27, 2017].
[12] VMware, "Workstation pro," [Online] Available: http://www.vmware.com/co/products/workstation.html [Accessed Mar, 30 2017].