Detection of WPS Attacks Through Multiscale Analysis

Ivo Petiz*, Eduardo Rocha*, Paulo Salvador*†, António Nogueira*†
*Instituto de Telecomunicacoes, Aveiro
†DETI, Universidade de Aveiro
{petiz,eduardorocha,salvador,nogueira}@ua.pt

***Abstract*—The wide spread adoption of 802.11 networks as the solution for providing an efficient network coverage with high data-rates raised several security concerns. In a first stage, WEP was used for protecting user's wireless networks from intrusions. Such intrusions' purposes could be simple free Internet accesses or more complex attacks to access confidential information. However, due to multiple technical flaws this approach was not sufficient which lead to the emergence of WPA and WPA2 technologies. WPA and WPA2 allow more secure networks but require more complicated configuration tasks.**

With the objective of creating a simple configuration interface, the Wi-Fi Alliance came up with a simple configuration approach: the Wi-Fi Protected Setup (WPS). WPS is present in major vendors products, providing a much easier configuration setup but a less efficient security environment. This less secure implementation is vulnerable to brute force attacks, that can be quick to execute, with little complexity and difficult to detect. After cracking the WPS, attackers can access to WPA/WPA2 wireless passphrase and consequently, illicitly connect to users' wireless networks.

Accessing and analyzing the content of the wireless frames is limited by technical requirements and legal constrains. Therefore, this paper presents a method to detect attacks on WPA routers with Wi-Fi Protected Setup based only on the amount of traffic generated. We propose a monitoring station which exclusively analyzes traffic flows from the router. By monitoring the traffic and using a multiscale analysis we are able to accurately identify this type of intrusion attempt over other traffic.

I. Introduction

With the increasing demand for Internet connectivity, several approaches were adopted for enabling a simple and efficient Internet access. Currently almost all (Internet Service Providers) ISPs provide wireless routers for homes and small office (SOHO) environments to their clients. Moreover, all network equipments manufacturers offer a wide-range of wireless routers. Modern wireless routers facilitate the setup of domestic wireless networks covering the users' home and office environment. However, the range of the wireless networks extend much further than the users' environment. Therefore, wireless routers physically allow the wireless access of unauthorized entities to the users data traffic, while it becomes difficult for users to know who is using (or watching) their connections. To address this issue, in the last years, wireless security became more complex in order to prevent an abusive use by undesirable users and attackers. One of the first proposed solutions was WEP security [1], which proved not so efficient [2] and was replaced by more efficient protocols, like WPA and WPA2 [3].

More secure protocols, such as WPA and WPA2, need more complex configurations which, for the common Internet user, could be a big problem, what sometimes led users to deactivate wireless security in order to avoid complicated setups. Wi-Fi CERTIFIED Wi-Fi Protected Setup (WPS) [4] was then created in order to simplify wireless setup, providing a PIN with 8 digits that could be introduced in user's computer and the connection would be established. Despite this simple method facilitates less expert users brings big security issues. WPS helps assure consumers that the Wi-Fi devices they purchase can be easily configured with security features enabled on their Wi-Fi networks, and that they can add new Wi-Fi Protected Setup devices to established networks with greater ease.

Wi-Fi Protected Setup is a certification program designed to support Wi-Fi CERTIFIED 802.11 products including consumer electronics and phones, as well as computers and routers. It applies to 802.11 devices for home and small office, including those that communicate through 802.11a/b/g/n, as well as multiple-band devices and those designed to operate Wi-Fi Direct™ features. The Wi-Fi Alliance [5],certified the first products with Wi-Fi Protected Setup in January of 2007. Since then, new features have been introduced to make the setup and configuration of security features even easier to use. In the past year alone, more than 1,000 products, including home access points, gateways and handsets have passed the testing necessary to be identified as Wi-Fi CERTIFIED Wi-Fi Protected Setup [4].

A very simple and easy to use software, which allows a user with not so much knowledge about computers and networks to get access to wireless networks, was recently released. This software, named Reaver [6], is a brute force attack program that exploits the WPS vulnerability by allowing users to subsequently send PINs trying to hit the right one. This PIN consists of a 7 digit number with a eighth digit corresponding to the parity number. With a minimum of 3 seconds per attempt it is possible to attacker to gain access to the WPA/WPA2 phrase pass in a few hours, much faster than traditional brute force and dictionary attacks, not being necessary capture any traffic from WLAN users connected. This type of attack is hard to detect and difficult to prevent. Event if the owner of an attacked wireless network changes the WPA/WPA2 phrase pass, the attacker can get the new phrase pass once again if the PIN from WPS continues the same. If the PIN has been changed, the attacker can always launch a

new brute-force attack in order to crack again the PIN.

In order to efficiently detect such attacks is necessary to access and analyze the content of the wireless frames. Capturing, decoding and analyzing all the wireless frames requires the usage of equipment with high processing capabilities. Moreover, the analysis of any layer of the frames data/headers is often limited by legal constrains. Therefore, in this paper we propose a method to detect the presented brute force WPS attack, based on the analysis of low level statistics (frame count) of the traffic sent by an attacked router. A multiscale decomposition and analysis of the collected traffic is performed and the obtained decomposition coefficients are then compared with the ones of regular legit traffic and other network attacks.

II. WPS Flaw and Attack

Wi-Fi Protected Setup presents two different methods to connect user's device to an access point, which is the Push Button Configuration method and the PIN method. The Push Button Configuration method consists in push a button on both devices, the button could be physical or virtual. A device has 2 minutes to authenticate in wireless router or will be presented a timeout and the connection will fail. In this 2 minutes any device could connect to wireless router, a desirable or undesirable one. The PIN method could be used by two different forms, by introducing a PIN from device in wireless router's interface or a PIN from the wireless router in the device's interface. PIN could be written in the device or wireless router or is possible to be a generated dynamically if requested.

In the case of using PIN method, by introducing the wireless router's PIN in the user's device, it is possible, to most of the vendors' wireless domestic routers, to make various attempts before the MAC address of the attacker's device becomes blocked. More concerning is the fact some wireless routers do not even block these devices, making possible a continuous brute force attack without any restrictions and of the wireless routers using WPS has the PIN feature enabled by default, without the possibility of shutting down. This flaw is even bigger looking at the PIN structure, shown in Figure 1, since the PIN consists only of a 8 digit number where the eighth digit is the check-sum. The number of attempts to find the PIN should be at most 10^8, but the attack can be optimized because the authentication proceeds by verifying the first 4 digits and then, if the first 4 digits are correct, there are only the last 4 digits left to discover. Therefore, in the worst case we need to try 10^4 numbers to find the first part of the PIN and then another 10^3 attempts to find the last part, once the last digit is the check-sum and can be calculated by attacker, what will give a total of 11000 attempts in the worst case to find the correct wireless router's PIN and get the WPA/WPA2 phrase pass.

III. Testbed Configuration

The lab hardware consists of two laptops named as machine 1 and machine 2 and a domestic wireless router as seen in

1	2	3	4	5	6	7	8
1^{st} Part				2^{nd} Part			CS

Figure 1. PIN Description

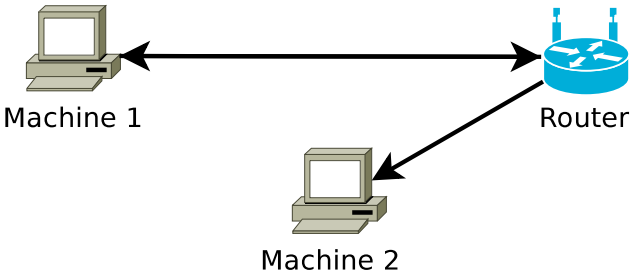

Figure 2. Lab configuration

Figure 2, working as a wireless router. Machine 1 was used as the attacker and machine 2 was the responsible for capturing the traffic sent by the router. The tested router was a Thomson, model TG784, is Wi-Fi Certified and 802.11b/g operating by default with WPS. Both machine 1 and machine 2 are laptops running Linux Ubuntu 11.10 and equipped with an Atheros wireless card, in order to make use of monitor mode, what is necessary to make the attack and capture the traffic.
To exploit this flaw is used Reaver 1.4 [6], after configuring the interface in monitor mode, using airmon-ng, from aircrack-ng suite software. To capture the traffic from router, machine 2 was configured in monitor mode to, running Tshark and configured in promiscuous mode.

Several attacks were launched using the several Reaver options, ranging interval between pin attempts and delay after a certain number of attempts, in order to simulate different types of WPS restrictions, as happens with the different kinds of routers, from the different vendors. It was used only traffic from the first part of attack, when an attacker tries to discover the first 4 digits of the PIN, since an continuously running system will always detect the beginning of the attack.

IV. Data Capture and Analysis

The collected traffic consisted of the traffic sent by the wireless router, in order to enable the detection of potential WPS attacks based on the analysis of the router responses to these attacks.

For both machines, WLAN cards were configured in monitor mode with the "airmon-ng start wlan0" command. For each Reaver attack configuration, the minimum capture duration was 6 hours, made using Wireshark in promiscuous mode, filtering the traffic to obtain just packets from router to machine 2. After the tests all captures were divided in 5 minutes files, size chosen by us trying to find the ideal duration, in order to predict attacks, with a maximum accuracy near real time.

Several captures, with different parameters, were performed in order to simulate the different responses from routers of

various vendors. For example, in order to prevent these kind of attacks, some routers restrict the number of attempts the attacker could execute before blocking the MAC address of the attacker. This can be avoided by using a delay after a certain number of PIN attempts.
- Regular attack, no alterations to the Reaver's default configuration.
- "–delay=2", set the delay between attempts in 2 seconds.
- "–delay=5", set the delay between attempts in 5 seconds.
- "–recurring-delay=$\langle 5 : 120 \rangle$", wait 120 seconds after 5 attempts.
- "–recurring-delay=$\langle 10 : 60 \rangle$", wait 60 seconds after 10 attempts.

To differentiate recurring-delay option from simple delay option it will be called lag to simple delay.
All captures were made in the first half of the attack period. A capture made in the second part of attack will necessarily have more packets exchanges and will present slightly different results.

We analyzed the number of captured bytes and packets per sampling interval. This interval was set 0.1 seconds and all collected flows were analyzed over 5 minutes intervals.

In order to compare the WPS attack with regular Internet traffic was also made traffic captures from some of most used Internet applications like Facebook[7], Gmail[8], Youtube[9] and online news. These captures follow the same method as the WPS. Captures were made from machine 2 and only low level statistics were collected.

V. Multi-Scale Analysis based on Wavelet Scalograms

In this section we present our traffic analysis approach which is based on a wavelet decomposition through the Continuous Wavelet Transform (CWT). In this manner, we can analyze any process in both time and frequency domains. Therefore, this tool is widely used in many different fields such as image analysis, data compression and, more recently, in traffic analysis. The CWT of a process $x(t)$ can be defined as [10]:

$$\Psi_x^{\psi}(\tau, s) = \frac{1}{\sqrt{|s|}} \int_{+\infty}^{-\infty} x(t)\psi^*(\frac{t-\tau}{s})dt \qquad (1)$$

where $*$ denotes the complex conjugation, $\frac{1}{\sqrt{|s|}}$ is used as an energy preservation factor, $\psi(t)$ is the *mother wavelet* while τ and s are the translation and scale parameters, respectively. The first parameter is used for shifting the mother wavelet in time, while the second parameter controls the width of the window analysis and, consequently, the frequency that is being analyzed. By varying these parameters, a multi-scale analysis of the entire captured process can be performed, providing a description of the different frequency components present in the decomposed process together with the time-intervals where each of those components is located. A Wavelet Scalogram can be defined as the normalized energy $\hat{E}_x(\tau, s)$ over all possible translations (set $\mathbf{T}$) in all analyzed scales (set $\mathbf{S}$), and is computed as:

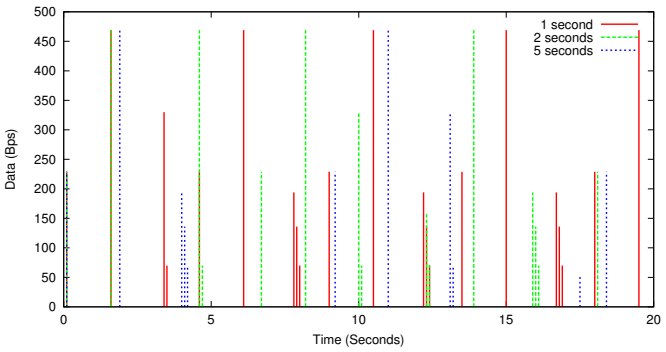

Figure 3. Data per second from 3 different delays configurations

$$\hat{E}_x(\tau, s) = 100 \frac{\left|\Psi_x^{\psi}(\tau, s)\right|^2}{\sum_{\tau' \in \mathbf{T}} \sum_{s' \in \mathbf{S}} \left|\Psi_x^{\psi}(\tau', s')\right|^2} \qquad (2)$$

The volume bounded by the surface of the scalogram is the mean square value of the process. The analysis of these scalograms enables the discovery of the different frequency components, for each scale (frequency) of analysis. For instance, the existence of a peak in the scalogram at a low frequency indicates the existence of a low-frequency component in the analyzed time-series while a peak in the scalogram at a high-frequency corresponds to an existing high-frequency component. In addition, assuming that the process $x(t)$ is stationary over time, several statistical information, such as the standard deviation, can be obtained:

$$\sigma_{x,s} = \sqrt{\frac{1}{|\mathbf{T}|} \sum_{\tau \in \mathbf{T}} (\hat{E}_x(\tau, s) - \mu_{x,s}), \forall s \in \mathbf{S}} \qquad (3)$$

where $\mu_{x,s} = \frac{1}{|\mathbf{T}|} \sum_{\tau \in \mathbf{T}} \hat{E}_x(\tau, s)$, and $|\mathbf{T}|$ denotes the cardinality of set $\mathbf{T}$.

VI. Results

In order to validate the proposed classification approach, several traffic measurements were performed as described in section III. The analyzed traffic was collected by using a promiscuous monitoring probe that captures all traffic sent from the wireless router of a 802.11 wireless network that was assembled at our networks laboratory. Since our monitoring probe does not connect to the wireless network, it does not access layer 3 traffic information. Consequently, the layer 2 metrics considered for analysis were the number of captured bytes per sampling interval (0.1 seconds). The same method was also used in Internet applications captures, in order to

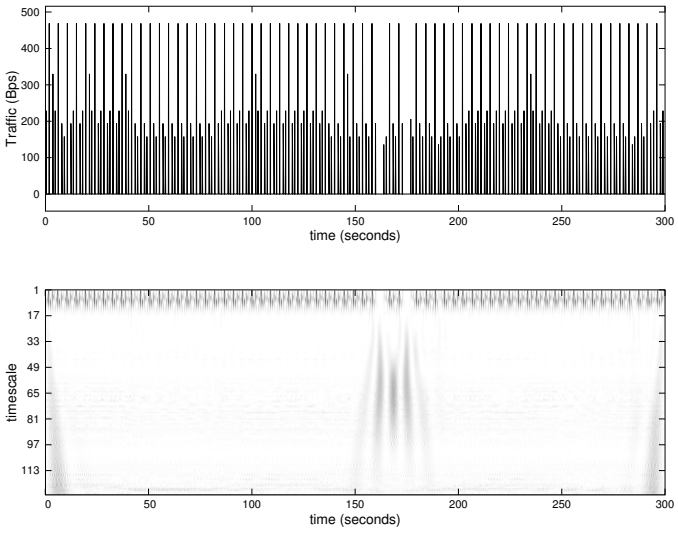

Figure 4. 5 minute capture bytes per 0.1 second scalogram

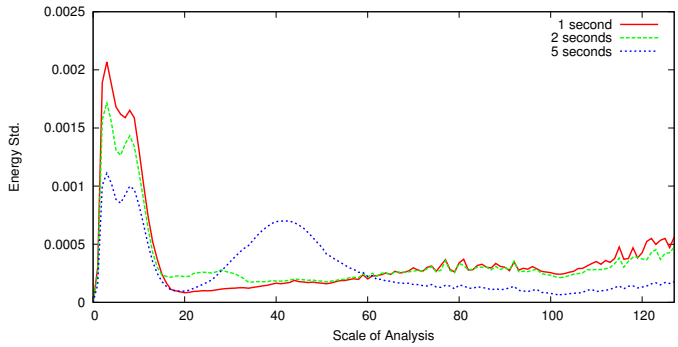

Figure 5. Comparison of 3 different delay intervals

compare with the WPS attack. The captures were made in Machine 2, only accessing layer 2 traffic.

In Figure 3 is possible to distinguish from the different PIN attempts' delays. All PIN attempts' data flows start at O seconds and it is possible to identify the different lags between PIN attempts. At 20 seconds, capture with a 5 seconds delay only had made 2 complete PIN attempts whereas the 1 second delay attempt has completed 5 cycles and 2 seconds attempts made almost 5 attempts.

The amount of traffic per 0.1 seconds for a 5 minutes capture and its scalogram is shown in Figure 4. It is possible to note a rhythm almost constant, except near 160 seconds, where the rhythm is broken for 15 seconds, and resumes to the initial rhythm. In Figures 5 and 6 are presented the comparisons between different attacks configuration's scenarios. In Figure 5 we compare the default configuration with an 1 second delay, 2 seconds delay and 5 seconds delay between attempts. Despite different configurations the 3 options show similar curves that can be identified using a multi-scale analysis based on wavelet scalograms. Figure 6 presents another configuration option where an additional delay is introduced after a ser of attempts (e.g. 10 attempts). When compared to the default configuration

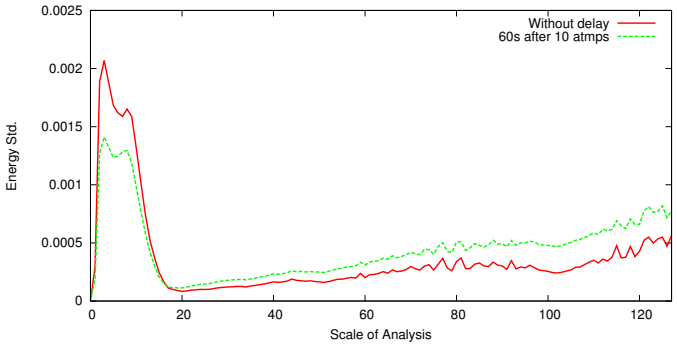

Figure 6. Comparison between different delay intervals

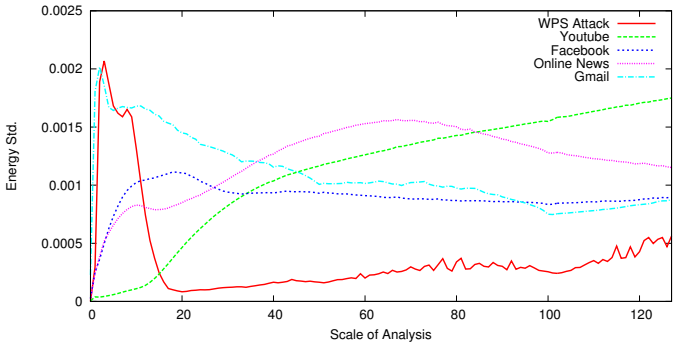

Figure 7. Comparison between WPS attack and some Internet services

(no additional delay) the analysis reveals a very similar curve. The WPS attack, when analyzed using a multi-scale analysis based on wavelet scalograms, shows a very characteristic curve, quite different from other Internet applications and services like Facebook, Youtube, Gmail and Online News, as shown in Figure 7, what makes it possible to identify using this methodology.

VII. Conclusion

Wireless networks are now widely used for providing an efficient and easy to use Internet access. Internet users use such networks to access important on-line services such as home banking, on-line shopping and to transfer important data. Users trust in these wireless connection by using secure protocols like WPA or WPA2 that provide a high level of security. Flaws such as the one detected in WPS feature compromise the security of wireless networks and compromise the security and confidentiality of the user's on-line communications and transactions.

In this paper, we proposed a method for the detection of malicious attacks to domestic routers based on Wi-Fi Protected Setup flaw. Making exclusively use of layer 2 traffic statistics and resorting to Continuous Wavelet Transform, it is possible to identify an attack. Indeed, the frequency components generated by the mentioned attacks can be easily differentiated from flows generated by other legit Internet applications like email, video streaming or social networks.

REFERENCES

[1] "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 802.11-1997*, 1997.

[2] A. Bittau, M. Handley, and J. Lackey, "The final nail in WEP's coffin," in *Security and Privacy, 2006 IEEE Symposium on*, may 2006, pp. 15 pp. –400.

[3] "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 Amendment 6: Medium Access Control (MAC) Security Enhancements," *IEEE Std 802.11i-2004*, 2004.

[4] "Wi-fi protected setup white paper," Tech. Rep., January 2007. [Online]. Available: https://www.wi-fi.org/knowledge-center/white-papers/wi-fi-certified-wi-fi-protected-setup%E2%84%A2-easing-user-experience-home-a-0

[5] (2012, September) Wi-fi alliance. [Online]. Available: http://www.wi-fi.org/

[6] (2012, September) Reaver WPS - Brute force attack against wifi protected setup. [Online]. Available: http://code.google.com/p/reaver-wps/

[7] (2012, September) Facebook. [Online]. Available: https://www.facebook.com

[8] (2012, September) Gmail. [Online]. Available: https://mail.google.com

[9] (2012, September) Youtube. [Online]. Available: http://www.youtube.com

[10] J. Slavic, I. Simonovski, and M. Boltezar, "Damping identification using a continuous wavelet transform: application to real data," *Journal of Sound and Vibration*, vol. 262, no. 2, pp. 291 – 307, 2003.