IEEE International Conference on Communications 2013: IEEE ICC'13 - 3rd IEEE International Workshop on Smart Communication Protocols and Algorithms (SCPA 2013)

Using Multiscale Traffic Analysis to Detect WPS Attacks

Ivo Petiz, Eduardo Rocha, Paulo Salvador, António Nogueira
DETI, University of Aveiro/Instituto de Telecomunicações, Campus de Santiago, 3810-193 Aveiro, Portugal
Email: {petiz, eduardorocha, salvador, nogueira}@ua.pt

***Abstract*—The worldwide adoption of the IEEE 802.11 standard as the solution to provide efficient network coverage with high data-rates raised several security concerns. In a first stage, Wired Equivalent Privacy (WEP) was used to protect wireless networks from intrusions, whose main motivations ranged from simply getting free Internet access to the perpetration of complex attacks in order to retrieve confidential information. However, due to multiple technical flaws, this approach was not sufficient, leading to the emergence of the Wi-Fi Protected Access (WPA) and WPA2 technologies, which provided more secure mechanisms at the cost of requiring more complicated configuration tasks. In order to create a simple configuration interface, the Wi-Fi Alliance proposed a simple configuration approach: the Wi-Fi Protected Setup (WPS), which is used by major network products manufacturers and provides a much easier configuration setup, although in a less efficient security environment. Actually, this implementation is vulnerable to brute force attacks, which are very quick to execute, have little complexity and are difficult to detect. After cracking WPS, attackers can access to WPA/WPA2 login information and illicitly connect to the target wireless network. There are several technical requirements and legal constrains that limit access to the contents of wireless frames, thus preventing their deep analysis. This paper presents a method to detect attacks over WPA-enabled routers with Wi-Fi Protected Setup, based only on the amount of generated traffic. The detection methodology uses a monitoring station that exclusively analyzes traffic flows from the router: by monitoring traffic and using a multiscale analysis procedure, the approach is able to accurately identify each intrusion attempt.**

***Index Terms*—Traffic identification, wavelet transform, scalogram, Wi-Fi, WPS.**

I. Introduction

With the increasing demand for Internet connectivity, several approaches were adopted to enable simple and efficient Internet access. Currently, almost all Internet Service Providers (ISP) provide wireless routers to their clients of home and small office (SOHO) environments. Modern wireless routers facilitate the setup of domestic wireless networks, covering the user home or office area. However, the range of these wireless networks usually extends much further than the intended area, physically allowing unauthorized entities to access the users data traffic while being simultaneously difficult to identify who is using (or watching) the connections. To address this issue, wireless security mechanisms became more complex in the last years in order to prevent an abusive use by undesired users and attackers. One of the first proposed solutions was Wired Equivalent Privacy (WEP) [1], which proved to be inefficient [2] and was replaced by the more efficient Wi-Fi Protected Access (WPA) and WPA2 [3] protocols.

More secure protocols require more complex configurations, which is a problem for common Internet users, causing them to deactivate wireless security in order to avoid sophisticated setups. The Wi-Fi Protected Setup (WPS) [4] was created to simplify the wireless setup process, providing a PIN with 8 digits that can be introduced in the user's computer in order to establish the connection. WPS assures consumers that the Wi-Fi devices they purchase can be easily configured with the security features that are commonly enabled on their networks, besides assuring that the addition of new WPS devices to already established networks can be easily made. However, this simple method also brings new security concerns.

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

Reaver is a very simple and easy to use software that allows a user with a rudimentary knowledge about computers and networks to get access to wireless networks [6]. This recently released software is a brute force attack program that exploits the WPS vulnerabilities by allowing users to repeatedly send PINs in order to hit the right one. Each PIN consists of a 7 digit number, with the eighth digit corresponding to the parity number. With a minimum of 3 seconds per attempt, it is possible for the attacker to gain access to the WPA/WPA2 phrase pass in a few hours, much faster than traditional brute force and dictionary attacks, and without being necessary to capture any traffic from WLAN connected users. 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 WPS PIN continues to be the same. If the PIN has been changed, the attacker can always launch a new brute-force attack in order to crack again the new PIN.

In order to efficiently detect this type of attacks, it is

978-1-4673-5753-1/13/$31.00 ©2013 IEEE

necessary to access the contents of wireless frames and analyze them. Capturing, decoding and analyzing all wireless frames requires equipment with high processing capabilities. Moreover, the analysis of any layer of the frame data/headers is often limited by legal constrains. Therefore, in this paper we propose a method to detect the brute force WPS attack based on the analysis of low level statistics (the frame counting process) 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 legitimate traffic and of other network attacks.

The remaining part of the paper is organized as follows: Section II presents a brief overview of some of the mostly relevant anomaly approaches that have been proposed; Section III describes the WPS security flaw and the characteristics of the brute force security attack; Section IV presents the testbed configuration that was used; Section V describes the data capture methodology and the analysis procedure that was used; Section VI provides some theoretical background on multiscale analysis and its application to the analysis of network traffic; Section VII presents the most relevant results obtained; Section VIII presents some possible application scenarios; finally, Section IX presents some brief conclusions.

II. Background on Anomaly Detection Methodologies

Solutions for identifying and mitigating IP-based attacks can be deployed at the host or network levels. At the host level, *anti-virus* applications, which rely on a database containing known patterns of attacks, can only detect attacks that are already stored, being unable to discover highly sophisticated and stealth attacks that present unknown patterns or patterns similar to legitimate applications. Besides, once a machine becomes infected, these tools are not able to detect illicit traffic since the whole network, its services and confidential data are compromised and the anomaly detection becomes unmanageable. Personal *firewalls* can also be an effective tool for preventing a computer infection by blocking traffic from unauthorized applications. However, they require an average know-how level from the user, which rarely happens, and are unable to prevent illicit traffic embedded in normal communications created by authorized applications or services.

At the network level, Intrusion Detection Systems (IDSes), such as Snort [7], and network *firewalls* appear as the most adequate approaches for guaranteeing the security of a network and its hosts. These systems operate by analyzing the traffic flowing on a network and inspecting the contents of the packets in order to find digital signatures, or patterns, that allow the unequivocal identification of security attacks. Such signatures are stored on databases that need to be constantly updated. Since IDSes usually do not analyze the traffic being exchanged between the different network hosts, they are unable to detect attacks that are launched by compromised hosts residing in the monitored network itself. IDSes can also be deployed in a distributed manner, in which several probes monitor each one of the network hosts. However, scanning every single packet and inspecting its contents, against the databases that contain all known attack patterns, is a complex and computationally intensive task. In addition, the correlations that the probes must perform in order to discover distributed and stealth attacks are extremely complex. Finally, these tools are also unable to cope with encrypted traffic and with the several existing confidentiality restrictions that prevent the analysis of the packets' contents.

Anomaly detection has been an active research field in the last years, trying to address the drawbacks associated to existing detection approaches. By performing a statistical analysis of Internet traffic and using machine learning techniques, several studies have been able to detect zero-day threats and unknown forms of attacks. For instance, in [8], the authors propose the use of Support Vector Machines (SVM) to detect anomalous behaviors. Self-Organized Feature Maps (SOFM) were used to create a profile of the normal and legitimate traffic, while TCP/IP fingerprinting is used to filter traffic that does not respect the TCP/IP standards. Finally, Genetic Algorithms (GA) are used to extract optimized information from raw Internet packets. The proposed approach managed to detect novel forms of attacks, while presenting a low False Positive rate. In a more recent work [9], authors proposed the use of machine learning (ML) techniques to exploit the correlations between packet and flow level information in order to associate packet level alarms with feature vectors extracted from flow records. Besides, authors have also proposed an architecture to deploy their approach at the network scale.

In [10], traffic classification and identification of Internet-based attacks was based on clustering techniques: by grouping the coefficients obtained from a multi-scale analysis of the traffic flows, accurate identification results were obtained. The classification of tunneled, or encrypted traffic, has been addressed in many research works. In [11], the authors proposed an approach to cope with encrypted P2P network layer tunnels. Statistical techniques were used to identify the protocols and, based on the policies of the analyzed network, devices could be advised to block, band-limit, or allow the whole tunnel. In [12], the aim was to propose generalized signatures for the identification of encrypted traffic: the authors identified 13 signatures and 14 flow attributes for SSH traffic classification, obtaining very accurate results. In [13] the size of the first few packets of an SSL connection were used to recognize the underlying application, enabling an early identification. However, it was assumed that the first bytes of a SSL connection are available for analysis, which may not always be true.

III. WPS Flaw and Security Attack

Wi-Fi Protected Setup presents two different methods to connect a user device to an access point (AP): the Push Button Configuration and the PIN methods. The Push Button Configuration method consists of pushing a physical or virtual button on both devices. A device has 2 minutes to authenticate in a wireless router, otherwise a timeout occurs and the connection fails. During these 2 minutes, any device can connect to the wireless router, whether it is a desirable or undesirable one. The PIN method can be used in two different

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

Fig. 1. PIN structure

forms: by introducing a PIN from the device into the wireless router interface or from the wireless router into the device interface. The PIN can be written in the device or wireless router or it can be dynamically generated, if requested.

If we introduce the wireless router PIN in the user device when using the PIN method, it is possible, on common wireless domestic routers of the main vendors, to make various attempts before the MAC address of the attacker device becomes blocked. Besides, some wireless routers do not even block these devices, allowing a continuous brute force attack to be executed without any restrictions. Most of the wireless routers using WPS have the PIN feature enabled by default, without the possibility of disabling it. The importance of this flaw ca be better understood if we look to the PIN structure, shown in Figure 1: since the PIN consists of only 8 digits, where the eighth digit is a check-sum bit, the number of attempts that are necessary to find the PIN is equal to, at most, 10^8. However, the attack can be optimized because the authentication proceeds by verifying the first 4 digits and then, if those first 4 digits are correct, discovering the last 4 digits. Therefore, in the worst case we need to try 10^4 numbers to find the first part of the PIN and, then, make other 10^3 attempts to find the last part: since the last digit is the check-sum and can be calculated by the attacker, a total number of 11000 attempts in the worst case are necessary to find the correct wireless router PIN and get the WPA/WPA2 phrase pass.

IV. Testbed Configuration

The testbed hardware consists of two laptops, named machine 1 and machine 2, and a domestic wireless router, as illustrated in Figure 2. Machine 1 was used as the attacker and machine 2 was the responsible for capturing the traffic sent by the router. The tested router is a Thomson TG784 model, Wi-Fi Certified and having 802.11b/g operating by default with WPS. Both machines 1 and 2 are laptops running Linux Ubuntu 11.10 and equipped with an Atheros wireless card in order to use the monitor mode, because it is necessary to make the attack and capture the corresponding traffic.

Reaver 1.4 [6] is used to exploit the previously described security flaw, after configuring the interface in monitor mode using *airmon-ng*, an application from the *aircrack-ng* suite software. In order to capture the router traffic, machine 2 was also configured in monitor mode, running Tshark in promiscuous mode.

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

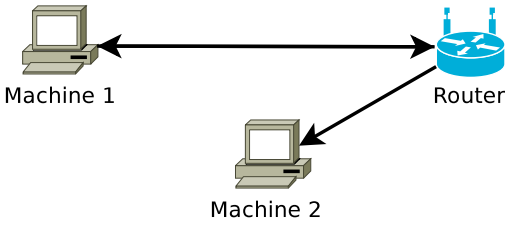

Fig. 2. Testbed configuration

V. Data Capture and Analysis

In order to allow the detection of potential WPS attacks based on the analysis of the router responses, we have collected all traffic sent by the wireless router.

The WLAN cards of both machines 1 and 2 were configured in monitor mode, using the *"airmon-ng start wlan0"* command. For each Reaver attack configuration, the minimum capture duration was equal to 6 hours. Captures were made using Wireshark in promiscuous mode, filtering traffic in order to only analyze packets from router to machine 2. After the tests, all captures were divided into 5 minutes files, a size that was considered the ideal duration to predict security attacks, since it allows to obtain the maximum accuracy in the minimum period of time, approaching the intended (almost) real time detection methodology.

Several captures, with different parameters, were made in order to simulate the different responses from routers of various vendors. Note for example that some routers, in order to prevent this kind of attacks, restrict the number of attempts an attacker can execute before blocking its MAC address. This situation can be avoided using a delay after a certain number of PIN attempts. The different experiments that were made are:

- Regular attack, no changes to the Reaver's default configuration.
- "–delay=2", sets the delay between attempts to 2 seconds.
- "–delay=5", sets the delay between attempts to 5 seconds.
- "–recurring-delay=$\langle 5 : 120 \rangle$", waits 120 seconds after 5 attempts.
- "–recurring-delay=$\langle 10 : 60 \rangle$", waits 60 seconds after 10 attempts.

In order to differentiate between the recurring-delay and the simple delay options, the simple delay will be called lag. All captures were made in the first half of the attack period. A capture made in the second part of the attack will necessarily have more packets exchanged and will present slightly different results.

We analyzed the number of captured bytes and packets per sampling interval. The sampling interval was set to 0.1 seconds and all collected flows were analyzed over 5 minutes intervals. In order to compare the WPS attack traffic with regular Internet traffic, several traffic captures corresponding to some of most used Internet applications, like Facebook, Gmail, Youtube and online news, were also made. These captures were obtained and processed using exactly the same methodology that was applied to the WPS captures. Captures

were made from machine 2 and only low level statistics were collected.

VI. Multi-Scale Analysis based on Wavelet Scalograms

Our traffic analysis approach relies on a wavelet decomposition based on the Continuous Wavelet Transform (CWT). In this way, it is possible to analyze the stochastic traffic process in both time and frequency domains. Wavelet transforms are widely used in many different fields, such as image analysis, data compression and, more recently, traffic analysis. The CWT of a process $x(t)$ can be defined as [14]:

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

where $*$ denotes the complex conjugation, $\frac{1}{\sqrt{|s|}}$ is used as an energy preservation factor, $\psi(t)$ is the *mother wavelet* and τ and s are the translation and scale parameters, respectively. The first parameter is used to shift 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 one 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:

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

The volume bounded by the surface of the scalogram is the mean square value of the process. The analysis of the scalograms enables the discovery/identification 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 the existence of a high-frequency component. In addition, assuming that the process $x(t)$ is stationary over time, several statistical parameters can be obtained, such as the standard deviation:

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

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 $\mathbf{T}$.

VII. Results

In order to validate the proposed classification approach, several traffic measurements were performed, as described in section IV. The analyzed traffic was collected 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 is not connected to the wireless network, it does not have access to layer 3 traffic information. Consequently, the number of captured bytes per sampling interval (0.1 seconds) layer 2 metric was considered for analysis. The same metric was also used in the different captures corresponding to legitimate Internet applications, in order to enable a direct comparison with the WPS attack case. All captures were made at Machine 2, accessing only to layer 2 traffic.

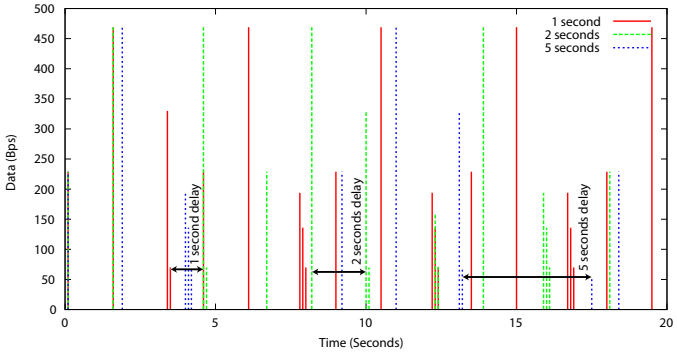

Fig. 3. Data (bytes per second) corresponding to three different delay values between PIN attempts

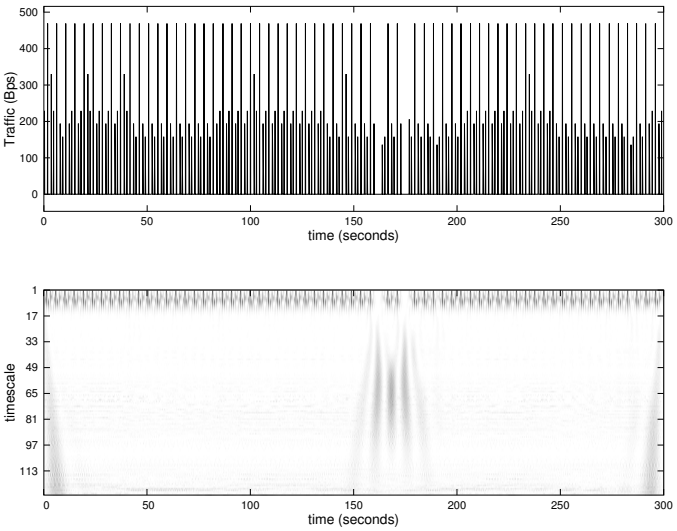

Fig. 4. Scalogram of the bytes per 0.1s process - 5 minutes capture

From Figure 3, it is possible see that there is a clear distinction between the traffic processes corresponding to different delays between PIN attempts. All data flows start at 0 seconds, being easy to identify the different lags between PIN attempts. At 20 seconds, the capture corresponding to 5 seconds delay exhibits only 2 complete PIN attempts, whereas the capture corresponding to a 1 second delay has completed 5 cycles and the capture corresponding to 2 seconds delay has almost completed 5 attempts.

The amount of traffic per 0.1 seconds for a 5 minutes capture and the corresponding scalogram are shown in Figure 4. It is possible to note an almost constant rate of peaks,

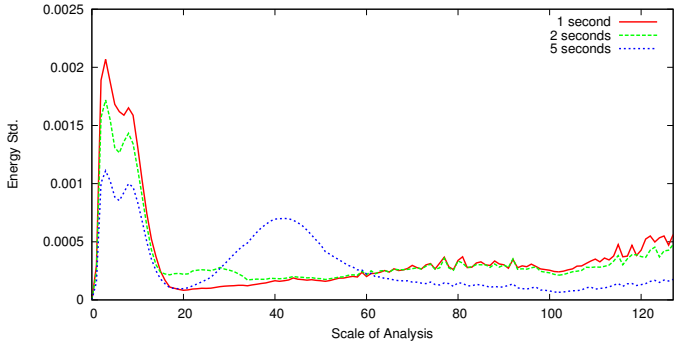

Fig. 5. Comparison of the energy standard deviation for three different delay values between PIN attempts

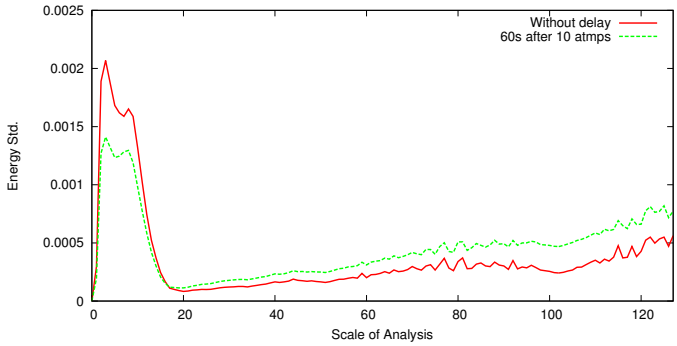

Fig. 6. Comparison of the energy standard deviation considering a delay of 60s after 10 attempts and no delay

except around 160 seconds where the rate decreases for more or less 15 seconds, resuming then to the initial rate. Figures 5 and 6 present the comparisons between the standard deviation of the energy corresponding to different security attack configurations.

In Figure 5, we compare the results obtained for the default configuration with an 1 second delay, 2 seconds delay and 5 seconds delay between attempts. Despite different configurations, the three scenarios present similar curves that can be identified using a multi-scale analysis based on wavelet scalograms.

Figure 6 corresponds to another configuration option, where an additional delay is introduced after a set of attempts (e.g. 10 attempts). When compared to the default configuration (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 the curves corresponding to legitimate typical Internet applications and services like Facebook, Youtube, Gmail and Online News, as shown in Figure 7. These differences will enable an accurate identification of this type of security attack.

The probability that a given flow traffic belongs to WPS attack, π_{wps}, can be calculated from:

$$\pi_{wps} = \frac{2E - \sum_{z=1}^{Z} \|P_z - t_z\|}{2E} \quad (4)$$

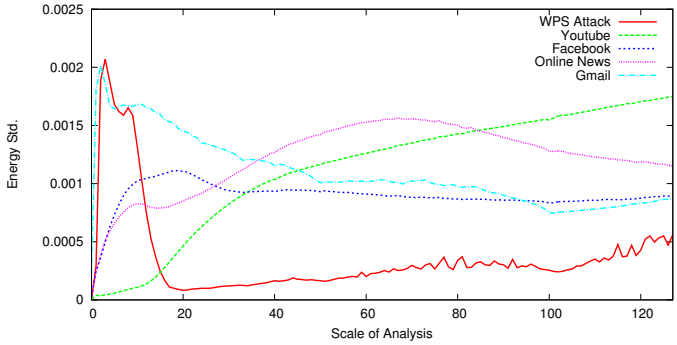

Fig. 7. Comparison of the energy standard deviation corresponding to a WPS attack and to some legitimate Internet services

Application	**Percentage of matching to WPS**
Standard WPS Attack	100%
WPS Attack with 2 seconds delay	91.40%
WPS Attack with 5 seconds delay	76.56%
WPS Attack with 60 seconds delay after 10 attempts	73.44%
Gmail	11.72%
Online News	3.13%
Facebook	9.38%
Youtube	7.03%

Fig. 8. Classification results

where E is the number of scales, Z is the maximum number of zones, P_z is the number of points of the training traffic flows located in zone z and t_z is the number of points of the testing traffic flows located in zone z. So, the probability of a WPS attack is calculated based on the distance to a pre-established pattern, that is, our WPS attack detector uses a proximity analysis based on the concept of "zone". Traffic flows with wavelet decomposition curves similar to previously analyzed WPS training flows will have high probability values of belonging to WPS attacks. The number of zones should be carefully defined: if this number is too high, the system will become more rigorous, reducing the number of false positives, but can also consider some "exotic" WPS attack configurations as non WPS attacks, thus reducing the system efficiency; on the other side, reducing the number of zones will increase the number of false positives. The considered number of zones was equal to 80, since this was the value that gave to best classification results for WPS attacks, considering traffic flows from WPS attacks and also from frequently used licit applications.

Figure 8 shows the results obtained by the proposed WPS attack detector. Distinct results were obtained for different WPS attacks, but for all cases the identification accuracy was higher than 70%, which can be considered a good result. Regarding licit applications, Gmail is the application that presents the highest matching probability to a WPS attack, but even in this case the probability was less than 12%, which is a clear sign that Gmail flows can not be confused with WPS flows.

VIII. Application Scenarios

This type of security attack can obviously be avoided by disabling the WPS feature. However, if WPS is considered as a fundamental feature, some measures should be adopted by vendors to prevent brute force attacks: introducing or increasing the delay after a certain number of PIN attempts, rising the time needed to perform an attack; reducing the number of PIN attempts on a restricted time window; creating a MAC black list that will be used to block all MAC addresses with more than a reasonable number of PIN attempts in a reduced period of time.

Thus, even if it would be impossible to avoid the attack, it could be possible the detect it. By building an attack detector, implemented in software or hardware, relying on the proposed multi-scale analysis based on wavelet scalograms, it would be possible to protect a corporate network from these brute force WPS attacks. Any wireless card could capture traffic from a domestic router to the different users and, from its analysis, detect if there is any anomalous data flow coming from a possible WPS brute force attack. A hardware based solution, implemented on a small device using a micro board with a specific wireless card that supports the monitor operation mode, would allow to monitor a simple network of a group of separate networks. This solution could be applied to bigger scenarios, like an entire building with several different networks from the same or from different providers, where the device could check the integrity of all networks security without needing to be connected to any one of the networks.

Whether the solution is implemented in software or hardware, the principle is the same: the system has to capture all traffic for a small period of time, separate it (by destination MAC address), perform a wavelet decomposition to any suspicious traffic using the CWT, identify the WPS attack based on the profile of the energy curve.

IX. Conclusions

Nowadays, wireless networks are widely used to provide efficient and easy to use Internet access. Internet users use these networks to access important on-line services, such as home banking or on-line shopping. Users trust in these connections by using protocols like WPA or WPA2, which provide a high level of security. Flaws such as the one detected in the WPS feature compromise the security of wireless networks and the confidence of users on-line communications and transactions. This paper proposed a method for the detection of malicious attacks to domestic routers taking advantage of the WPS flaw. Using exclusively layer 2 traffic statistics and resorting to the Continuous Wavelet Transform, the paper proved that it is possible to identify this type of security attack: in fact, the traffic frequency components generated by this type of interaction can be easily differentiated from traffic flows generated by other legitimate 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 *IEEE Symposium on Security and Privacy*, may 2006, pp. 15–400.

[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/

[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] (2011, March) Snort home page. [Online]. Available: http://www.snort.org/

[8] T. Shon and J. Moon, "A hybrid machine learning approach to network anomaly detection," *Information Sciences*, vol. 177, no. 18, pp. 3799–3821, September 2007.

[9] N. Duffield, P. Haffner, B. Krishnamurthy, and H. Ringberg, "Rule-based anomaly detection on IP flows," in *IEEE INFOCOM*, April 2009, pp. 424–432.

[10] E. Rocha, P. Salvador, and A. Nogueira, "Detection of illicit traffic based on multiscale analysis," in *17th International Conference on Software, Telecommunications Computer Networks*, September 2009, pp. 286–291.

[11] T. Yildirim and P. Radcliffe, "A framework for tunneled traffic analysis," in *The 12th International Conference on Advanced Communication Technology*, vol. 2, Feb. 2010, pp. 1029 –1034.

[12] R. Alshammari and N. Zincir-Heywood, "Generalization of signatures for SSH encrypted traffic identification," in *IEEE Symposium on Computational Intelligence in Cyber Security*, april 2009, pp. 167 –174.

[13] L. Bernaille, R. Teixeira, I. Akodkenou, A. Soule, and K. Salamatian, "Traffic classification on the fly," *SIGCOMM Comput. Commun. Rev.*, vol. 36, pp. 23–26, April 2006.

[14] 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.