WI-FI PROTECTED SETUP VULNERABILITY IN ROMANIAN WIRELESS NETWORKS

Florin SMARANDA
University of Piteşti, Argeş, Romania
fsmaranda@yahoo.com

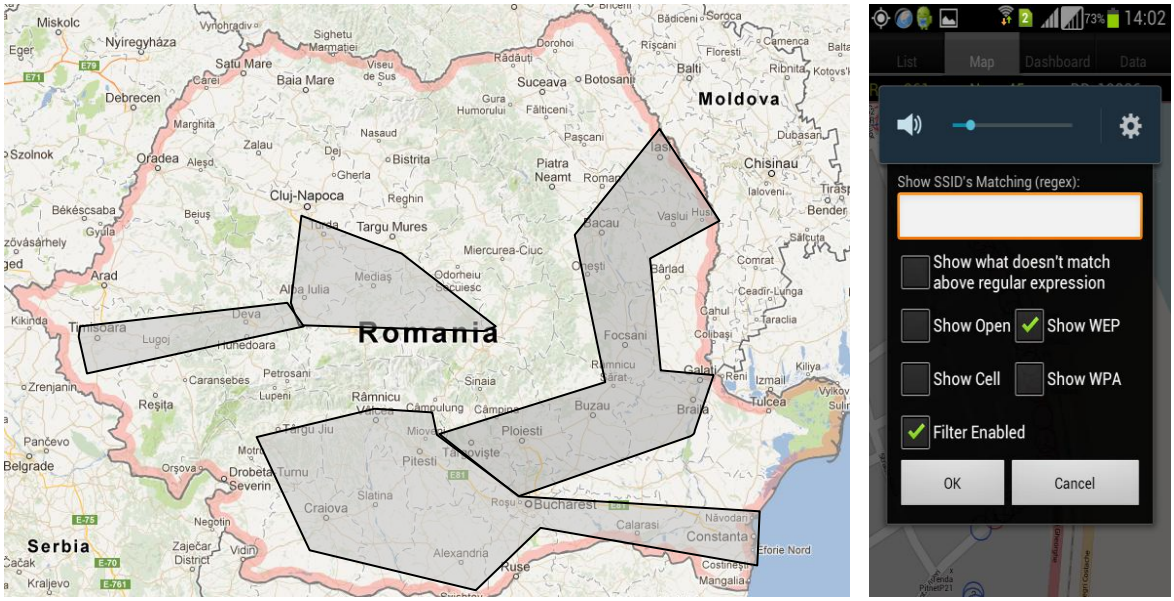
Keywords: *wireless, WPS, security, Romania*

Abstract: *This paper presents a study concerning the security of wireless networks in Romania in the context of the recently discovered vulnerability of Wi-Fi Protected Setup. A large number of wireless networks was scanned giving a good estimate at national level. The presence of the Wi-Fi Protected Setup feature is analyzed for the networks in urban and rural environment and the applicability of the solutions for the PIN acknowledgement messages problem.*

1. INTRODUCTION

Wireless networks and Wi-Fi networks in particular have changed the way people and businesses have thought about internet connectivity. The wide range of users that adopts this type of networks brings potential problems because they do not know the new security problems associated with Wi-Fi networks.

The Wi-Fi Protected Setup (WPS) vulnerability was discovered in the end of 2011 and surprised the hardware vendors that were marketing it as a important feature.



(a) *(b)*

Fig 1. Areas scanned in Romania (a) and WiGLE for Android software (b)

id	ns1:href	ns1:name	ns1:name2	ns1:description	ns1:style
red	http://maps.google.com/mapfiles/ms/icons/red-dot.png				
yellow	http://maps.google.com/mapfiles/ms/icons/yellow-dot.png				
green	http://maps.google.com/mapfiles/ms/icons/green-dot.png				
		Wifi Networks	RomTelecom-WEP-CC4	BSSID: 72:1d:67:64:cc:4c Capabilities: [WEP][ESS] Frequency: 2412	#yellow
		Wifi Networks	RomTelecom-WPA-CC4	BSSID: 72:1d:67:64:cc:4d Capabilities: [WPA2-PSK-CCMP][ESS] Frequency	#red
		Wifi Networks	TP-LINK	BSSID: 90:f6:52:3c:2d:be Capabilities: [WPA2-PSK-TKIP+CCMP][WPS][ESS]<br/	#red
		Wifi Networks	22605	BSSID: 22605_702_46027605 Capabilities: HSDPA;ro Frequency: 0	#green
		Wifi Networks	22605	BSSID: 22605_702_46027604 Capabilities: HSDPA;ro Frequency: 0	#green
		Wifi Networks	TP-LINK_130919	BSSID: 90:f6:52:49:fd:8a Capabilities: [WPS][ESS] Frequency: 2412	#green
		Wifi Networks	HG520b	BSSID: 4c:ed:de:4e:d7:c4 Capabilities: [ESS] Frequency: 2412 1	#green

Fig. 2 Sample KML file with results with WPS feature detected

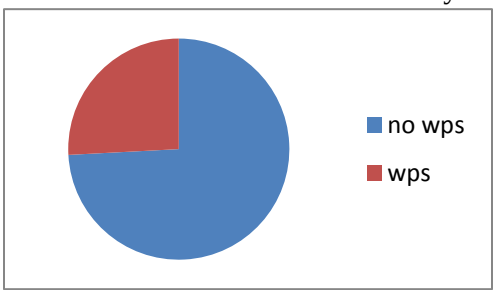
This paper focuses on the detection of Wi-Fi Protected Setup (WPS) characteristic in Romanian wireless networks, the presence of the vulnerability and the user adoption of solutions for removing this vulnerability. The wireless security scans performed for this study were made in Romania in rural and urban areas, covering over 40000 networks in the areas marked in Fig 1. In order to have the GPS location of the discovered WPS Access Points (AP), the software used for scanning was WiGLE.Net for Android [1] that easily allows the detection of the WPS feature and exports the data in multiple formats such as CSV and KML (used by Google Maps - sample output in Fig 2). WiGLE for Android also has a multiple detection avoidance feature implemented so that the same network does not show multiple times in the exported results

2. EARLY SECURITY THREATS FOR WIRELESS NETWORKS

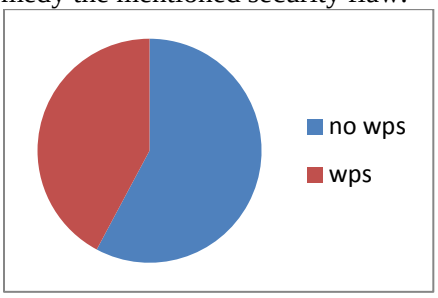
There are many threats for wireless networks, some general and some specific. The most common attacks (for both wired and wireless) involve social engineering, where the attacker does not use specialized IT skills. The dictionary attack is frequently used because people tend to put to their networks passwords that are easy to remember such as the name and easy keyboard combinations (1234, qwerty, etc.). Many recent attacks are also based on the execution of code (such as JavaScript) on the client's computer with full security permissions because people may unknowingly agree to it [2]. The specialized attacks involve the vulnerabilities of WEP security protocol used mostly in older wireless network cards. More recently the exploit of the WPA short packet spoofing and the Wi-Fi Protected Setup (WPS) problem in generating PIN acknowledgement messages have brought back the question of wireless security.

3. CURRENT SECURITY THREATS TO WIRELESS NETWORKS IN ROMANIA

In Romania most Wi-Fi solutions are of 802.11n type, and many of these devices have been marketed since 2007 with the WPS feature. This feature was created in order to bring enhanced security to users that do not understand the steps required to create a secure connection. Because of hasty and incorrect implementation, this feature led to the discovery in December 2011 [3] of an exploit that reduces the number of tries for an attacker that searched the pre-shared key of the WPA/WPA2 network. As a response, in early 2012 most producers that had devices vulnerable to this attack offered solutions or produced firmware updates that remedy the mentioned security flaw.



(a)



(b)

Fig 3. Wi-Fi Protected Setup (WPS) in rural (a) and urban (b) areas

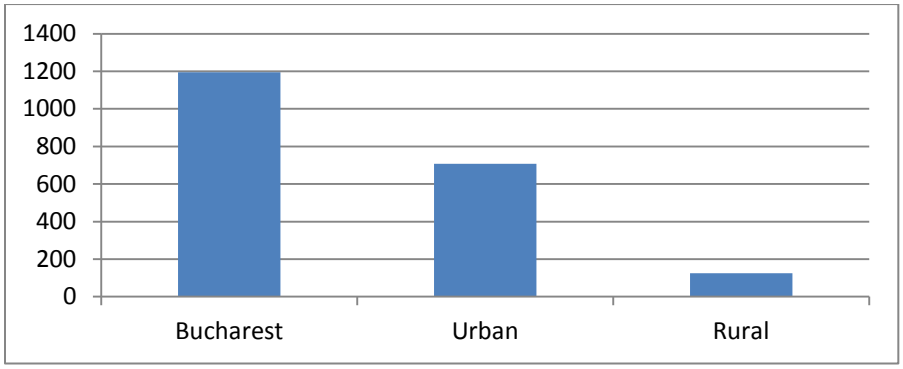


Fig 4. Wi-Fi Network density in Romania in rural, urban areas and in the capital Bucharest

While scanning for the WPS feature in Romania, the results presented in Fig. 3 were found.

The percentage of WPS enabled solutions is high in cities (38%) and lower in rural areas (26%). This is due to the fact that there is a large number of 802.11n devices in the total number of scanned networks. In order to put this into a correct perspective, network density must be taken into account.

The network density presented in Fig 9 is an estimate for the scanned areas and is very high in cities (1194 networks/km2 in Bucharest and 708 networks/km2 in other urban areas) compared to rural areas (124 networks/km2 in rural areas - higher if closer to cities and lower if they are in remote areas) therefore the numbers prove that it exists a higher chance to find a vulnerable AP in urban areas compared to rural even if the percentage is smaller in cities.

Because of the extended time necessary to perform a successful WPS attack, a reduced number of APs were tested for this vulnerability. The purpose of the performed attack was only to detect the presence of vulnerable devices, because not all devices from a vendor are vulnerable (as some are already commercialized with updated firmware). The tests determined that 3 out of the 10 tested networks were vulnerable. For an opportunistic attacker the most important issue would probably be the time needed to perform the successful attack.

However the number of WPS enabled devices commercialized before December 2011 is high and offers enough targets for a determined attacker. Also, because the APs that support WPS are still perceived as relatively new devices and the users will unlikely feel the need to upgrade the equipment anytime soon.

4. SOLUTIONS FOR WPS VULNERABILITY AND THEIR ADOPTION

A different aspect that this paper tries to determine in what measure the security of implemented wireless networks is improved after the release of software and firmware updates, because the effort of software developers often ends with the publishing of the software update. Some manufacturers were not affected because they already had mechanisms in place (such as the introduction of timeouts in case of multiple attempts to validate a personal identification number).

In the first part of 2012 many solutions became available from Access Point manufacturers that solve the WPS vulnerability. Most hardware producers recommend disabling this feature, even if it is still promoted by vendors as an advantage for new wireless products. There were some devices that even with the feature disabled in the Web interface did not disable the feature, while other manufacturers did not want to renounce to the WPS feature. Therefore firmware updates were published online and a general feeling of security was created. However end-users usually

take a long time to perform firmware updates and many are not even aware of the existence of an security update, the WPS problem still remains a threat today.

In case of software updates there are recent studies [4] that showed that almost half of the users do not update the software even if they know how and a quarter of the users do not update because they do not know how to perform an upgrade.

Firmware updates are even more problematic because of the difficulty of the process (compared to the software update) and because there is a great risk that the hardware device will fail during the update.

A study concerning the frequency of firmware update showed performed in the fall of 2012 at Pitesti University, Faculty of Electronics and Computer Technology (65 students participated in the conducted poll) showed that the number of persons that have ever performed a firmware e update is small compared to the people that have performed software updates (such as Windows, Office or Visual studio) because they are advertised as soon as they are available. Firmware updates do not have a similar mechanism for update advertisement and are rarely checked manually. The main reasons identified for not performing a firmware update are: lack of knowledge about the existence and role of the update; fear that the update will make the device inoperable (because of errors or power outages during the update process); fear that the new firmware will remove features and lead to a lengthy reconfiguration process. Therefore many 802.11n APs featuring WPS are still vulnerable to attacks even if the manufacturers have published the updates that remedy the errors.

While automatic firmware updating seems like a good option, few manufacturers have the necessary resources to develop and test the update so that the firmware changes does not lead to traffic disruption or, more importantly, local security policy modifications (such as Cisco's Connect Cloud firmware update in 2012).

5. CONCLUSIONS

The study was performed throughout 2012 as soon as the WPS vulnerability became known. Tests performed in the second part of 2012 showed that there are still vulnerable WPS enabled networks because people do not know about the vulnerability, do not know how to update the firmware or are afraid to make changes to the firmware. Even if WPS attacks are a lengthy process, the existence of vulnerable networks at almost a year after the vulnerability was presented shows that many users will remain vulnerable to these attacks.

Silently making available online solutions to remedy this vulnerability without a proper publicity campaign that makes users aware of the dangers of using outdated firmware will not reduce significantly the number of vulnerable systems. This kind of publicity is often perceived as exposing a weakness to the customers that leads to lower sales and many times efforts were made to actually hide the vulnerability then to solve it.

The solution is the automatic firmware updates, solution that already exists in the industry (most notably in mobile phones) but involves developing software and hardware solutions by the hardware manufacturers that may increase the price of the device. Some customers however may prefer this solution to increase their network security, instead of employing the services of a full network specialist.

6. REFERENCES

[1] Wireless Geographic Logging Engine, " WiGLE", Accessed September 2012, http://www.wigle.net/wiki/index.cgi?WiGLE

[2] Valeriu IONESCU, „Designing a client side data scrapper”, Universtity of Pitesti Scientific Bulletin, Series: Electronics and computers science Vol. 1 / 2011, pg. 21-24, ISSN: 1453-1119

[3] Stefan Viehböck, "Brute forcing Wi-Fi Protected Setup. When poor design meets poor implementation", 26.12.2011, Version 3, http://sviehb.wordpress.com/, Accessed 10 October 2012.

[4] Skype, "Survey Finds Nearly Half of Consumers Fail to Upgrade Software Regularly and One Quarter of Consumers Don't Know Why to Update Software", July 23, 2012, Accessed: http://about.skype.com/press/2012/07/survey_finds_nearly_half_fail_to_upgrade.html