SURVEYING WI-FI SECURITY

Presentation of Wi-Fi Security Measures, Varius Wi-Fi Attacks and a Classification Survey of Wi-Fi Networks in Thessaloniki

George E. Violettas, Tryfon L. Theodoroy, Konstantinos Chalkias and George Stephanides
Dept. of Applied Informatics, University of Macedonia, 156 Egnatia Str, Thessaloniki, Hellas, Greece

Keywords: Mac Spoofing, War Drive, Wi-Fi Security, wireless intrusion, WEP Attacks, WPA Attacks.

Abstract: This paper is a study of the use and possible flaws of the two basic cryptographic protocols (WEP, WPA) in Wi-Fi Networks. It presents some very easy to implement methods to gain malicious access to such networks by disclosing the network secret key, using Windows Operating Systems, like Win XP. It also describes the shutter of the myth saying that the MAC Address filtering is a safe practice for securing a wireless network. There is a field research, in which we show the distribution of wireless networks according to the security protocol implemented (if any) at a major city centre in Greece. Unfortunately, according to our results, only 8% of the wireless networks are using a fairly safe cryptographic scheme, 48% is not using any security at all, while the rest is using the totally unsecure WEP encryption.

1 INTRODUCTION

Along with the quick spread of the Wi-Fi networks, came the need for insuring the integrity and the security of the transmitted information. Special techniques were invented for this purpose, since the existing ones could not fill the gap. Those techniques were based on already known methods and algorithms, some of those very successful in other areas of cryptography.

In order to encrypt and protect the transmitted information, the Wi-Fi Networks used a specially invented technique, called WEP, which inherited the weaknesses of the algorithm used (RC4) (Ohrtman & Roeder, 2007). Today this protocol is considered to be tottaly unsafe; still WEP encryption is used in the majority of wireless networks. In the following sections we show that intruding to WEP protected networks is not only possible from Linux OS operated machines, but it can happen from a computer running a common used Windows OS.

We also claim that the WEP's succesor, WPA, is fairly safe, only when all the security measures are kept, mainly the length and the complexity of the selected security key. However, it is a fact that WPA protocol is vulnerable to "Denial of Service (DoS) attacks, due to a fundamental securiy countermeasure implemented by the protocol.

Moreover, we provide proofs that the MAC filtering protection of a wireless (and a wired one consequently) network is not secure.

Furthermore, there is a field research. The center of Thessaloniki, a Greek city with more than one million citizens, has been scanned for the presence of wirelless networks. These networks were categorized based on the location (with the aid of simultaneously GPS collected data) and the type of security implemented. Briefly speaking, the results show that the vast majority of Wi-Fi networks are either using weak encryption or they are not protected at all.

In parallel, in order to analyze the above results, we collected related data from the technical support center of the largest network and tellecommunications operator in Greece, OTE S.A.

We would like to state here, that it is very difficult to find the right word(s) to describe an attack to a wireless network, usually an illegal act in most of the European countries. Nevertheless, we hope that by propagating the followings, we are contributing to raise the (very weak) security of this kind of networks.

E. Violettas G., L. Theodoroy T., Chalkias K. and Stephanides G. (2008).
SURVEYING WI-FI SECURITY - Presentation of Wi-Fi Security Measures, Varius Wi-Fi Attacks and a Classification Survey of Wi-Fi Networks in Thessaloniki.
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 96-101
DOI: 10.5220/0002027900960101

2 WI-FI SECURITY

In order to secure a wireless network, one can transmit the confidential data after applying a cryptographic protocol on it, so no one else can understand the ciphertext, apart from the one knowing the ciphering method and the cipher key (Bauer, 2002). This technique, as far as it concerns the wireless communication, is divided into two major categories:

2.1 WEP (Wired Equivalent Privacy)

The WEP protocol is based on the RC4 Algorithm. This algorithm has several flaws, as it was invented for different purposes (Ohrtman & Roeder, 2007). The use of that protocol is strongly discouraged (Microsoft, 2008).

2.2 WPA (Wi-Fi Protected Access)

WPA is considered to be the basis in wireless cryptography nowadays, as it is much safer than its ancestor (WEP). It is using a new algorithm (CCMP-*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) based on the AES algorithm (Ohrtman & Roeder, 2007).
WPA is divided in two basic categories:

- WPA-Personal or WPA-PSK: It is based on pre-shared keys, and consequently the efficiency of the protocol is based on the complexity of this key, and
- WPA-Enterprise: A much safer implementation requiring an 802.1x Server who is responsible of sharing different keys for each client, raising the security standards.

3 PREREQUISITES OF ATTACKING WI-FI

The requirements for attacking a Wi-Fi network are basic and minimal:

3.1 Wi-FI Card (2,4 GHz)

The most important part for that purpose is the Wi-Fi card. Just a few cards on the market are capable of completing such an assignment. Chipsets, such as the Intel (Centrino), which is integrated in the majority of laptops today, are NOT suitable for the job. One of the best cards for this kind of 'activity' is the series with an "Atheros" chipset inside from

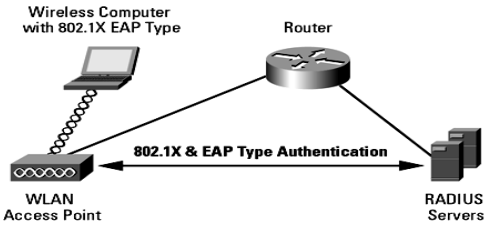

Figure 1: WPA-Enterprise, The highest type of security today. A Radius server in the corporate network handles all the users and the dynamic keys (Wi-Fi Alliance, 2003).

"Proxim" (Gold, B/G etc). Other chipsets supported are "Atheros", "Aironet" and "RTL8180" (Aircrack-ng, 2007).

3.2 Operating System

The statement which claims that attacking Wi-Fi Networks is done only under Linux OS is a myth. All the attacks described in this paper were carried out under Windows (XP). This fact makes the prospect of such attacks more terrifying, considering the worldwide spreading of Windows OS compared to Linux OS distributions.

3.3 Software to Use

One of the notorious programs for the purpose is Kismet (Kershaw, 2007). It runs under Linux OS, although it can be run under Windows OS as well, using an emulator like "cygwin" (Cygwin, 2007).

"Airsnort" is also a complete suite "*..which recovers encryption keys*.." as stated in the home page (The Shmoo Workgroup, 2008).

Pocket Warrior (Pocket Warrior, 2003) is *"...a wireless auditing software for PRISM and NDIS 5.1 compatible card that runs on PocketPC 2002"*.

In our study, we used aircrack-ng-1.0-beta2-win, found on (Aircrack-ng, 2007)**.** It is a complete suite consisting of programs for capturing Wi-Fi packets, analyzing them, examining various keys and finally finding the right encryption key. Also it includes programs for creating valid packets (packet injection) for a Wi-Fi network, in case this network is not having a associated client, and consequently is not broadcasting any packets. The latter is very "useful" for breaking into home networks, because those networks could sometimes be inactive for hours or days.

4 ATTACKING WI-FI

4.1 Attacking WEP

As mentioned above, the WEP protocol is flawless. No matter how complicated is the key used, it is possible to extract it with minimum effort. In the following pictures, we will see a network secured with this protocol. In Fig. 2, we see the typical layout of such a network.

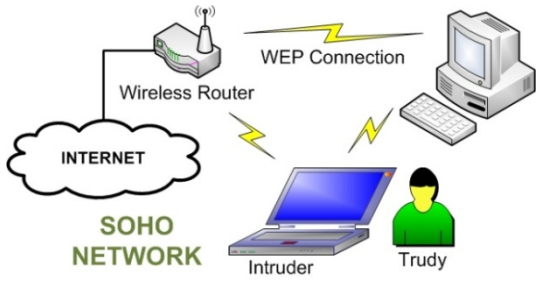

Figure 2: Small House Typical Network. One router connects wirelessly one or a few more computers to the internet. The intruder, somewhere in the vicinity is trying to breach the security of the network.

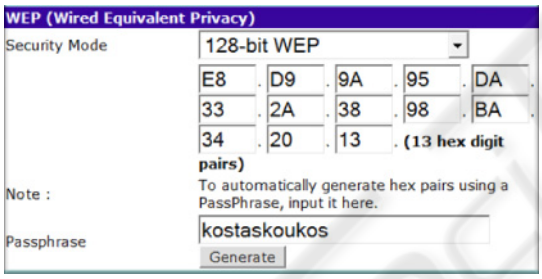

Figure 3: Typical configuration of a SOHO router. The specific image displays the particular page where to set the kind of security for this Wi-Fi device. The security is set to WEP, with 128-bit security.

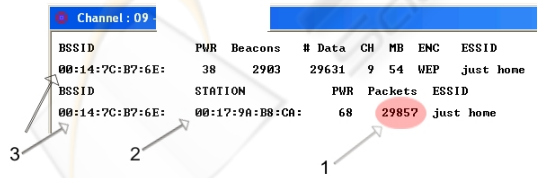

Figure 4: BSSID (2) (3): MAC Address's of the Access Point. PWR: signal level. BEACONS: base announces of the Access Point. DATA (1): the packets in question. ENC: Encapsulation. Security implemented (WEP, WPA, etc). ESSID: the network name (e.g. SSID). STATION: the MAC Address of the connected station. It can be used later on, in case the network administrator has implemented the MAC Address filtering. This kind of security is very leaky, as it is very easy to fake a MAC Address.

The device under "attack" was a WiFi-router "OfficeConnect" model, made by "*3COM*". In Fig. 3, we present the relevant page for creating the WEP key in such a device.

Additionally, we have to consider that when a user wants to extract the produced key to store it in a flash drive or elsewhere, she needs to copy each pair of the hexadecimal number separately. It is less possible that anyone will ever bother to change that key once it is produced. For our experiments, the key for the network was chosen on purpose to be a word not existing in the English or in the Greek dictionary.

The first step is to look for Wi-Fi networks in the area. The next picture depicts the discovery of the network in question:

As soon as the target is found (or chosen), there are two actions to take:

- First step for attacking WEP

We have to record an efficient amount of Wi-Fi packets (red oval in Figure 4). The exact number is not accurately set, but usually a number between 500.000 and 700.000 packets is enough. This number can be collected in about 10 to 20 minutes from a network with medium traffic (3-5 clients).

- Second step for attacking WEP

As soon as the number of packets needed is collected, the program for finding the WEP key is launched through a windows interface with few parameters to be set. The next Figure shows the program in action, checking various letters and finally finding the WEP key.

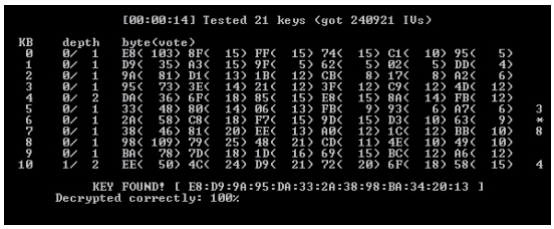

Figure 5: "aircrack-ng" in action. The program is inspecting various combinations of characters and it finally finds the right key (KEY FOUND).

In the first line we can see that a number of 240,921 packets (IV's) was enough to find the key. As seen in the last two lines the key was found within seconds. The hexadecimal key represented in this example, is identical with the one provided at the Figure 3 ("kostaskoukos").

4.2 Attacking WPA

Unlike WEP, WPA is not vunerable to such attacks

(Ohrtman & Roeder, 2007). It implements a different algorithm so it has none of the weaknesses of its ancestor. It has only a serious weakness which has to be taken under serious consideration (Kang & al, 2004).

The initial key called PTK, used to commence the handshake protocol is vunerable to dictionary attacks. As soon as this key (PTK) is collected, it can easily be deciphered as it holds a little extra info, only *2.5n + 12* bits, where *n* is the length of the key the user entered. The packet, which contains the key in question, is the "association" packet. In order to get upper hand on this packet, one needs to wait until a new station connects to the network or somehow force an already connected station to disconnect, so that station will obviously try to reconnect. As soon as that station tries to reconnect, the "association" packet is captured (Andrew Vladimirov, 2006).

WPA has implemented an extra security measure, described as follows: As soon as the WPA implementing station "senses" a station trying to connect for 3 times in a row with the wrong key phrase, it shuts down completely for 2 minutes. This can be used also for Denial of Service – DoS Attacks (Aslam, 2006) (Geier, 2003). Because of the above security measure of the WPA protocol, the dictionary attack cannot happen against the real transmitting station (Access Point) and thus it can only take place off line.

In the following picture we set an access point (3COM) implementing the WPA protocol, with the passphrase "dimitris".

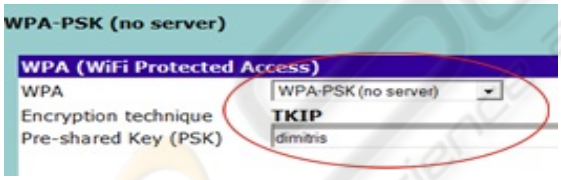

Figure 6: Setting the WPA-PSK key.

We need to state here that the passphrase "dimitris" has been chosen on purpose. In the on-line Oxford dictionary (AskOxford, 2008) the word "dimitris" did not exist, although the word did exist in the dictionary used for the attack (as almost all the rest of the words of eight characters long). As seen in the next image, the passphrase was found after approximately 15 minutes.

If we want to avoid the brute force attack, the length of the passphrase has to be at least 20 characters long, with suggested length at least 33 characters (Lisa Phifer, Core Competence Inc, 2004).

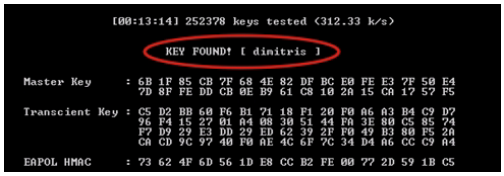

Figure 7: Finding the WPA key in seconds.

5 MAC ADDRESS SECURITY

Somehow the Mac Adress filtering is considered solid and inpenetrable. No one seems to know why this statemet has not been shuttered, although there are several references for the opposite from authorities like (Wi-Fi Alliance, 2003).

In order to attack "Mac Address Security", we used one of the many programs freely avaliable on the internet, called MacMakeup (Gorlani, 2008). That program can very easily alter the Mac Adress of any network card. The program is very simple as demonstrated in the image below:

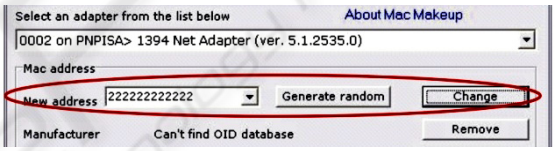

Figure 8: Changing the Mac Address of a specific Network Card (NIC) to the desired one 22:22:22:22:22:22.

After resetting the specific wireless card, it has the new Mac Adress (Fig below):

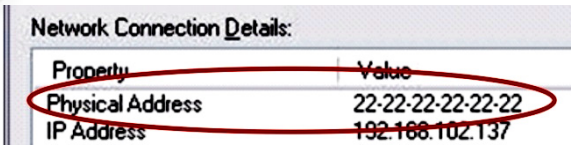

Figure 9: Finding the WPA key in seconds.

As it has been referred in section 4, when someone is attacking a WEP protected network, she is able to get the Mac Adresses of both the Access Point the client(s), respectively. Thus, even if the Access Point implements the Mac Address filtering, the attacker can easily change her computer's Mac Address, to the one belonging to the accosiated client. The Access Point then is "obliged" to accept this "legal" client.

6 WI-FI SURVEY

In a study about security, it is very critical to study

as well, what are the practices used and what is generally happening in the real world today.

6.1 "War Driving"

The definition of the term "War driving" is: someone with a laptop and a GPS is wandering around, looking for Wi-Fi networks (Andrew Vladimirov, 2006). As soon as the particular area is mapped, the weak security networks are targeted and potentially hacked by the "War driver".

Imitating the above on Sunday 28 of February 2008, we drove at the center of Thessaloniki town for around 4 kilometers. Our equipment was: a laptop with a Wi-Fi card, and a GPS device preferably connected to the laptop. The software needed for the job is the notorious (Netstumbler, 2008). We managed to connect the software with the GPS used (a PCMCIA card of NaviGPS). The only disadvantage of the particular software for our research is that: it reports all networks with security enabled as WEP enabled networks, even if they are WPA protected. So in order to separate the networks based on security implemented, we used a mobile phone (HTC 3300) with a GPS embedded. The software we found out that distinguishes between WEP & WPA protection was Airomap (Airomap, 2007).

The outcome of our "tour" was a map (Figure 10) created in Google Maps with the data collected.

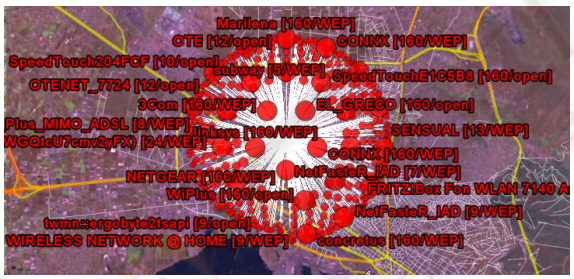

Figure 10: Wireless networks discovered during the survey, at the centre of Thessaloniki – Greece.

7 RESULTS OF WAR DRIVING

The results of the research were very disappointing. We discovered approximately 490 wireless networks in an area of about 0,750 Km^2. According to our results, only the 8% of the networks discovered used the WPA protocol. The 44% of the networks, used the flawless WEP protocol, and the rest 48% of them did not use any encryption at all.

Inside the 48% of the networks discovered not to use any encryption algorithm, those with RADIUS server or hotspot implementations are also included. In fact, the latter does not mean that such networks are protected. The information transmitted is defenseless, and consequently compromised by anyone with a "sniffing" program like Ethereal (Ethereal, 2007). In addition, there are many networks whose SSID is the default one of the specific device, along with the channel number (e.g. 9% of the total networks discovered, have the SSID: CONNX, channel 6. This is the default SSID of the AP sold by the National Network and Telecommunications Operator, OTE S.A.). This repeated occurrence means that many people bought an Access Point from the local store, plugged it in, did not even bother to read the manual, connected their laptop and forgot about it. Unfortunately, these same people do send their credit card number to their bank's secure site, through this totally unsecured channel.

Table 1: Wireless Networks categorized according to security protocol implemented.

Type of Security	Perrcentege (%)
WPA	8%
WEP	44%
OPEN (No security)	48%

A similar work in Hong Kong (PISA & WTIA, 2005), shows that the above problem is spread worldwide. The 61% of the AP discovered on that survey had the WEP/WPA protection turned off.

8 USER-BEHAVIOUR STATS

Motivated by the above disappointing results, we collected and then examined technical information from OTE S.A.. In fact, as one of the authors has been working on the internet technical support department of OTE S.A., we extracted data from user-calls reporting problems with their Wi-Fi network and reliability. The above survey has been conducted from April 1st to May 15th 2008. Some of the most interesting results include the following: from the 355 users whose problem has been recorded,

- 10.7% used WPA (75% of them are companies and only 25% of them are single users)
- 28.7% had never used wireless connection; however their Access Point was turned on using the default settings.
- 41.6% keep the default router's settings
- 10.9% claim that they do not require encryption (they want to freely share it)

- 39.1% do not change the router's settings after resetting the router
- 11.8% reported low bandwidth, because someone else was maliciously sharing their Wi-Fi internet connection.

9 SUGGESTIONS

Although, when one uses all the security measures and the perquisites a wireless network is practically impenetrable. Those basic measures are:

- WPA protocol should be used, WPA-2 is preferable,
- The network secret (passphrase) has to be changed frequently,
- The passphrase should not exist in a dictionary and it should be at least 20 characters long. As an extra security measure the passphrase should contain some symbols (like @#$%^&) or/and some capital letters,
- MAC Address Security & filtering should be used only as a complimentary and an extra security measure. If used as a standalone security measure is useless as it can be penetrated in seconds with not much of an effort.

10 CONCLUSIONS

Although we do have today the means to secure a wireless network, only a very small percentage (8%) of the Wi-Fi implementations today, are using a strong cryptographic security (WPA). Combined with the availability of the attacking tools for Windows Operating Systems, makes the possibility of such a network to be compromised, almost a certainty.

The 92% of the wireless networks implemented today, are not using any serious security, although the wireless security nowadays is reliable. The vast majority of wireless networks today (54%) are using obsolete methods like WEP to secure the transmitted data, setting at risk the transmitted information.

REFERENCES

Aircrack-ng. (2007). Retrieved from http://www.aircrack-ng.org/doku.php

Aircrack-ng. (2007). *Is my card compatible with airodump /aireplay ?* Retrieved from aircrack documentation: http://www.wirelessdefence.org/ Contents/Aircrack ORIGINAL.html#q080

Airomap. (2007). Retrieved 01 29, 2008, from http://www.divideconcept.net/index.php?page=airosuite/index.php

Andrew Vladimirov, K. V. (2006). *Wi-Foo: The Secrets of Wireless Hacking* .

AskOxford. (2008). Retrieved 02 23, 2008, from Oxford Online Dictionary: http://www.askoxford. om/ results/?view=dict&freesearch=dimitris&branch=13842570&textsearchtype=exact

Aslam, B. I. (2006). 802.11 Disassociation DoS Attack and Its Solutions: A Survey. *Mobile Computing and Wireless Communication International Conference, 2006.* Amman: Nat. Univ. of Sci. & Technol.

Bauer, F. L. (2002). *Decrypted Secrets.* Springler.

Brad, A. (2008). *802.11 Attacks*. Retrieved 04 16, 2008, from Foundstone Professional Services: http:// www.foundstone.com/us/resources/whitepapers/802.11%20Attacks.pdf

Cygwin. (2007). Retrieved from http://www.cygwin.com/

Ethereal. (2007). Retrieved 11 17, 2007, from http:// www.ethereal.com/

Geier, J. (2003, May 1). *Tutorials*. Retrieved 01 2008, from Wi-Fi Planet: http://www.wi-fiplanet.com/ tutorials/article.php/2200071

Gorlani, M. (2008). *Mac Makeup*. Retrieved from http:// www.gorlani.com/publicprj/macmakeup/macmakeup.asp

(2004). Analysis and Countermeasure on Vulnerability of WPA Key Exchange Mechanism. In Y. S. Kang, & e. al, *Information Networking* (pp. 915-924). Berlin: Springer Berlin / Heidelberg.

Kershaw, M. (2007). *Kismetwirless*. Retrieved from Kismet: http://www.kismetwireless.net/

Lisa Phifer, Core Competence Inc. (2004, 11 17). Using WPA without enterprise AAA.

Microsoft. (2008). *What are the different wireless network security methods?* Retrieved 01 2008, from Windows Help and How-to: http://windowshelp.microsoft.com/Windows/en-US/Help/b385cc8a-af25-489e-a82e-decf6df26b681033.mspx#EZB

Netstumbler. (2008). Retrieved from http:// www.netstumbler.com/

Ohrtman, F., & Roeder, K. (2007). *Wi-Fi Handbook.* McGraw-Hill.

PISA & WTIA. (2005, April). *Wireless LAN War Driving Survey 2004-05*. Retrieved 03 2008, from http:// www.hkwtia.org/wtia/WLAN%20War%20Driving%20Report%20(2004-5).pdf

Pocket Warrior. (2003). Retrieved 2008, from http:// pocketwarrior.sourceforge.net/

The Shmoo Workgroup. (2008). Retrieved from http://airsnort.shmoo.com/

Wi-Fi Alliance. (2003, Febrouary 6). Retrieved 01 16, 2008, from Enterprise Solutions for Wireless LAN Security: http://www.securitytechnet.com/resource/ hot-topic/wlan/Whitepaper_Wi-Fi_Enterprise2-6-03.pdf