ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2006. Nr. 7(71)*
ELEKTRONIKA IR ELEKTROTECHNIKA

TELECOMMUNICATIONS ENGINEERING
T 180
TELEKOMUNIKACIJŲ INŽINERIJA

Security State of Wireless Networks

A. Vindašius
Department of Telecommunications Engineering, Vilnius Gediminas technical university,
Naugarduko str. 41, LT-03227 Vilnius, Lithuania, phone: +370 5 274 49 77, e-mail: antanas@cc.hut.fi

Introduction

IEEE 802.11 standard wireless local area networks became inseparable part of both private and corporate networks. The main factors resulting great interest in unlicensed band wireless networking equipment – functionality, convenience and low cost. However, mass deployment of wireless networks faces many security issues, which tends to be unique and less understandable since most of this kind of threats doesn't exist in wired networks at all. Many serious problems concerning privacy and private network separation arise, since data is being transmitted trough freely accessible wireless medium.

It's been a long time since first publications showed up announcing WEP encryption vulnerability [1] and other various security gaps, which gave a boost for development of effective wireless network hacking tools.

IEEE developed standard for enhanced security IEEE802.11i [2] addresses many of those known vulnerabilities and have advanced solutions for many wireless security gaps, yet implementation of the standard seems to be sluggish and extremely late. Thus many wireless network users and administrators are still satisfied with old vulnerable encryption, using mistakenly assumed security methods or none at all. The basic concepts regarding wireless security has to be fully understood by anyone who deploys a wireless access point, since usually wireless network is deployed as an extension of wired local network and pose security threat to all inside network.

This paper presents results and analysis of passive 2,4 GHz band scanning in Vilnius in order to discover wireless IEEE 802.11b/g standard networks and identify the main parameters which show the general view of security state of wireless networks. The aim of research is to obtain data, showing the link layer encryption used, network exposure and other wireless network configuration characteristics.

Related work

The passive scan of IEEE 802.11 frequency bands and looking for possible security holes became popular since late 2000, when popularity of 802.11equipment started to grow dramatically. It was done by computer enthusiasts, usually without any evil intentions, only in order to locate, identify, map, get main security parameters from as many wireless devices as possible. This kind of activity is known worldwide by the name "wardriving".

Wardriving inspired the development of tools, which allow to find, identify access points, analyze and decrypt encrypted data packet flows. They are freely available as open-source scripts [3] and require only basic computing and wireless networking experience.

Many of various internet sites, inspirited by wardriving hobbyist communities provide some scanning experiences, network detection and security vulnerability discovery tips, sometimes some scan results [4]. Only very few publications showed up regarding wireless security evaluation, obtained by wardriving as a scan method, mainly presenting statistics as percentage of encrypted IEEE 802.11 networks.

The first "worldwide wardrive" was carried out in 2002 and took place in many American cities including Boston, San Diego and Des Moines as well as in Norway, Barcelona and Johannesburg. Totally 32 areas in nine countries was surveyed. The first survey found 9374 wireless access points, more than 30% of which did not have basic encryption turned on [5]. "Seattle WiFi Map Project" provides AP location maps (data last updated in 2005), showing 45% of WEP enabled networks. The results were published in [6]. The similar test, discovering 802.11b/g networks was performed in Perth, Australia in 2004 [7]. There was discovered over 700 infrastructure networks while driving 26 km path through city. The results show roughly half of the networks WEP encryption activated, 15% of SSIDs set to default.

The results vary due to different methodology and city regions scanned (business, residential); the separation of different encryption types was not supplied in any case.

Methodology of research

The objectives of the analysis was to discover approximate density of IEEE802.11 standard wireless equipment in several areas of Vilnius operating in 2,4 GHz band, to derive data of hardware settings used. The main objective was security state evaluation based on

information which can be gained during passive raw data packet collection.

The area in centre of Vilnius, small and medium business locations and few dense residential regions have been chosen for research (Fig.1). Passive scan of 2,4 Ghz frequency band was performed using a laptop running Linux and equipped with b/g standard Intel Pro/Wireless 2200BG card and build-in antenna. Hence, all this kind of low cost hardware is widely available for anyone. No high gain antenna or any other professional radio equipment was employed.

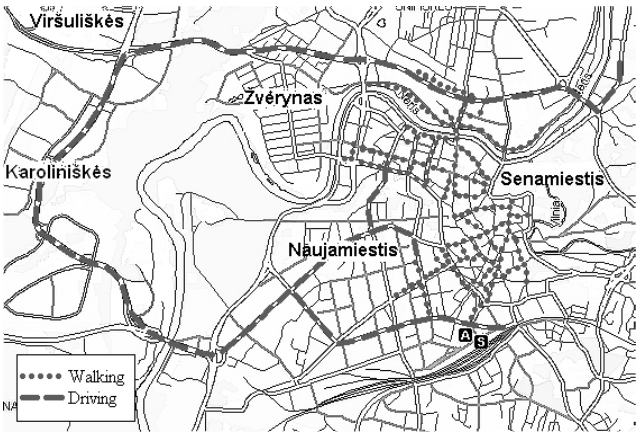

Fig. 1. Scan locations in Vilnius

Multifunctional wireless security audit tool "Kismet" [8] was used for access point detection, identification and captured packet collection. Wireless card was set to monitor mode trough all scanning process. Any kind of active network analysis, connect request, disassociation broadcasting or other penetration activity was not performed. Passive encryption breaking was not performed as well. The scanning was performed in two sessions, which took place on two different (one working and one holiday) days, approximately 5 hours duration each session.

The obtained hardware configuration data and collected data packets have been used for analytical purposes only, none of the data or access point location and characteristics have been disclosed.

Totally 632 wireless networks were discovered during scanning process. This number includes only unique AP, ad-hoc or probe networks, as the list was filtered for duplicate Basic Service Set Identification (BSSID) numbers, which could be obtained on different scan sessions. A "network" in the case of infrastructure topology means wireless AP with associated wireless clients and the single wireless link (two nodes) in ad-hoc case. Only in the case of probed network the network represents single wireless device. Thus, the network can be understood as Basic Service Set (BSS).

The total number of wireless devices discovered is not presented, since it may be extremely inaccurate due to short scanning period. This kind of results may be presented in future after long-term scanning and development of accurate algorithm for separation of wireless and wired client hardware, which both are detected as clients.

Result analysis

The collected data was processed and detected networks were classified according several criterions: network topology, physical characteristics, exposure and encryption. All discovered wireless networks were classified to ad-hoc, infrastructure or probe networks according to their connection topology. The identification can be easily made from IEEE802.11 frame header [9].

Ad-hoc network works in peer-to-peer manner. Clients connect to each other directly without any scheduling since there is no AP in such networks. Ad-hoc network detection is done through probe request and probe response packet capturing or while clients communicate with each other.

Infrastructure networks include AP as the core network device used for bridging or routing wireless clients. This type of network is detected through AP beacons, client association requests or basic data traffic.

There also are special group of probe nodes. Those include unassociated nodes, probing for AP or other node in case of ad-hoc network. Kismet detects probe networks as potential threat, since probing may be performed in order to get unauthorised access. However, usually those are just misconfigured nodes or nodes in networks with AP down.

The distribution of different network topologies can be seen in Fig. 2.

Physical characteristics – the carrier (standard) type and frequency usage was analysed.

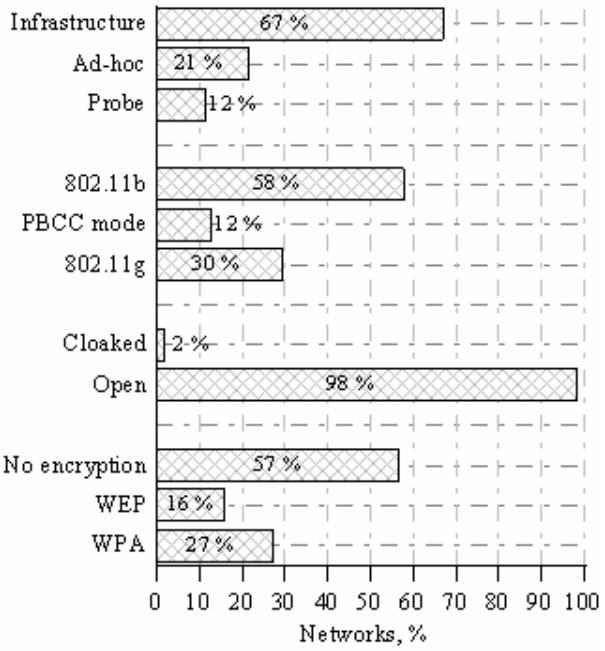

Fig. 2. Results obtained from passive scan

What kind of standard network uses can be determined from rates, the network is operating. The rates, supported by b standard are 1, 2, 5,5 and 11 Mbps, while supported rates for g standard are 6, 9, 12, 18, 24, 36, 48, 54 Mbps. According to the retrieved rate values, the network of interest can be identified as 802.11b or 802.11g.

During result analysis, non-standard rate of 22 Mbps have been noticed. After some research on various vendor wireless product specifications it was discovered, that some vendors utilize this rate using Packet Binary Convolutional Coding (PBCC) mode in their 802.11b devices. This mode is proprietary and is not supported by the 802.11b specification. That is why the separate group of 802.11b "PBCC mode" in Fig. 2 was distinguished.

Another physical characteristic, which can be determined by any data traffic activity of the network, is frequency channel, the network is operating in. The frequency usage data in Fig. 3 are based on infrastructure and ad-hoc networks only, as probe networks are performing scan in all frequency spectrum

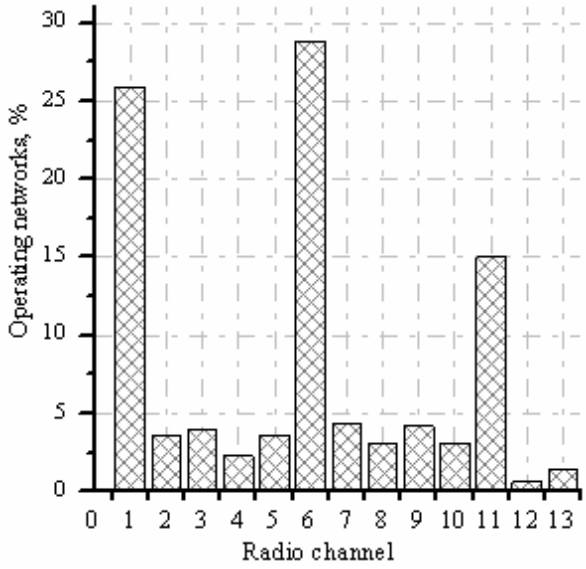

Fig. 3. The frequency channels used in discovered infrastructure and ad-hoc networks

Note, that strong tendency is to use channels 1, 6 and 11. The research on most popular vendor product specifications show, that major part wireless APs include 1st (f.e. Zyxel, SMC), 6th (f.e. Lucent, Linksys, Netgear) or 11th (f.e. DLink) channel as the default. Therefore, the motivation to set scanning or hacking tools to spend more time on those channels while hopping through whole spectrum is well-founded.

Each interface is identified in link layer by hardware MAC address. The first six bytes of MAC address represent network hardware vendor. This information can be used for vendor-specific vulnerabilities exploit or simply for checking whether the default configuration is used on wireless device. The full list of vendor's identification numbers can be found on official IEEE Registration Authority page [10]. The distribution on different vendors showed strong correlation against frequency used, i.e. the major part of networks were operating in default preconfigured frequency. The results, showing different vendor distribution is not presented as it is not the aim of this analysis.

The classification according to exposure of network was also made. The only criterion was the SSID visibility. All networks with freely visible SSIDs goes to group "open" (Fig. 2) and those with masked SSID – to group "cloaked". The major part of SSIDs were discovered having information about network equipment vendor, model or worse – the location or owner of the AP. SSID name does not make the attack harder or easier, but helps a lot to identify the network, which can be one of the most time consuming tasks for attacker.

Fig. 2 also shows the number of discovered wireless networks according to type of encryption (if any). The key length or precise cipher algorithm are not categorized as it requires deeper analysis of every network and possibly active penetration. The results shown here, only basically distinguishes no encryption, WEP based encryption (both 40 and 104 bit) and WPA based encryption (any algorithm). WPA standard [11] specifies advanced authentication algorithm, which solves known WPA vulnerabilities.

The data collected does not inform of any higher layer security implementations, such as VPN tunnelling or application layer end-to-end encryption. It does not show that networks with WEP or WPA are more secure either. WEP has been proved to be insecure, some versions of WPA as well. Thus, the encryption in link layer lets to make only general findings about overall network security. The detailed analysis of packets in higher layer (using Ethereal [12]) from few randomly chosen unencrypted networks indicated no higher layer encryption.

The IP addresses can be sniffed by capturing ARP (Address Resolution Protocol) packets, which are broadcasted in the entire network and inescapably are transmitted through AP. In such way even IP addresses of the node in wired part of network, which never communicates through wireless, are discovered. The large quantity of captured ARP packets with MAC addresses of Ethernet interfaces (the MAC addresses can be verified in [10] as well) strongly indicates that there is direct access to wired network though AP.

Not only imperfect technical security methods degrade the security level of wireless networks. Often the basic wireless issues are misunderstood by those who install wireless access points into their networks. The lack of basic knowledge in network architecture and wireless networking, leads to insecure wireless network deployment. Probably the most dangerous network topology is the one with wireless access point installed inside the local network as trusted node leaving the router and firewall behind. Attacker gets directly to local network leaving all security enforcements useless. Leaving AP with the default configuration unchanged and encryption disabled are common network administrator mistakes.

Any corporate network administrator would never allow a stranger to plug his laptop into local network switch, but they are offering to do so by means of providing unprotected wireless access.

Conclusions

The passive scan in few business and residential areas in Vilnius was performed. From the data collected the following inferences can be made:

1. The major part of discovered wireless access points were configured predictably, with many default settings. Predictable access point configuration and disabled

encryption pose security threat not only to wireless, but also to wired part of the local network.

2. 57 % of discovered wireless networks had no encryption enabled, the higher layer protocol analysis of randomly chosen networks showed, that no higher-layer encryption was employed either. 16 % of networks use WEP which have been proved insecure. Only 27 % of the networks had WPA enabled. This part of networks can be considered more or less secure, but no straight inferences can be drawn as there are some vulnerable WPA versions.

3. Large number of captured ARP packets (with MAC addresses of Ethernet interfaces) shows, that APs often are deployed as trusted node in wired local networks and pose security threat to all inside network.

4. All the information obtained with low-cost widely available equipment, none of the professional hardware or software was used. Unauthorised access to major part of wireless networks can be gained by anyone slightly experienced and concerned.

5. For basic wireless access point security, AP should not be left with factory defaults or installed as trusted node in local network; configuration should include WPA or WPA2 link layer encryption (with encryption keys resistant to dictionary attacks if preshared key mode is used). Higher layer security should be used for sensitive data.

References

1. **Newsham T.** Cracking WEP Keys, Presented at Black Hat USA 2001 conference. – Las Vegas, USA, 2001, July 11–12.
2. **IEEE**, ANSI/IEEE Std 802.11i, 2004 Edition. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements. – New York: IEEE Standards Board, 2004.
3. **Vladimirov A., Gavrilenko K. V., Mikhailovsky A. A.** Wi-foo. The secrets of wireless hacking. – Addison Wesley, 2004.– P. 28–41.
4. **Welch D.** Wireless Security Threat Taxonomy // Proceedings of the 2003 IEEE Workshop on Information Assurance. – West Point, NY, 2003 June.
5. **Brewin B**. Worldwide 'war drive' exposes insecure wireless LANs // ComputerWorld. – 2002 Sept.
6. **Heim K**. Seattle's packed with Wi-Fi spots // The Seattle Times. – 2005, Feb. 18.
7. **Yek S., Bolan C.** An analysis of security in 802.11b and 802.11g wireless networks in Perth,W.A // Australian Computer, Network & Information Forensics Conference 2004. – Perth, Western Australia, 2004, Nov. 25.
8. **Kershaw M.** Kismet Wireless, internet access: http://www.kismetwireless.net.
9. **IEEE**, ANSI/IEEE Std 802.11, 1999 Edition. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. – New York: IEEE Standards Board, 1999.
10. **IEEE Registration Authority.** Organizationally Unique Identifier, internet access: http://standards.ieee.org/regauth/oui/oui.txt.
11. **Wi-Fi Alliance,** internet access: http:// www.wi-fi.org.
12. **Ethereal.** Software manual, internet access: http:// http://www.ethereal.com.

Submitted for publication 2006 05 09

A. Vindašius. Security State of Wireless Networks // Electronics and Electrical Engineering. – Kaunas: Technologija, 2006. – No. 7(71). – P. 19–22.

Mass deployment of wireless networks faces many security issues, which tends to be unique and less understandable since most of this kind of threats doesn't exist in wired networks at all. Many serious problems arise concerning privacy and private network separation, since data are being transmitted trough shared and freely accessible wireless medium. The main security problems and vulnerabilities concerning wireless networks are shortly addressed. This paper presents results and analysis of passive 2,4 GHz band scanning in Vilnius in order to discover wireless IEEE 802.11b/g standard networks and identify the main parameters which show the general view of security state of wireless networks. The data obtained from analysis indicates that main security threats are experienced by wireless networks due to disabled link layer encryption. The other problem is considering access points as trusted nodes in wired local area networks. Ill. 3, bibl. 12 (in English; summaries in English, Russian and Lithuanian).

А. Виндашюс. Безопасность беспроводных сетей // Электроника и электротехника. – Каунас: Технология, 2006. – № 7(71). – С. 19–22.

Пользующиеся сегодня большой популярностью беспроводные сети сталкиваются с множеством вопросов безопасности, которые вообще не существуют в проводных сетях. Из-за того, что пакеты с данными передаются через свободно используемый и общий всем эфир, возникает серьёзная проблема изолирования отдельных подсетей. Коротко описаны возможные способы нарушения безопасности беспроводных сетей. Проведённое в Вильнюсе исследование просканированной частотной полосы в 2,4 GHz показывает общий уровень защиты частных беспроводных сетей, использованное в них шифрование, основные особенности конфигурации беспроводных точек доступа. Собранные данные показывают, что чаще всего проблема безопасности возникает при использовании точек беспроводного доступа как надёжных зон и не использование шифрования канального уровня. Ил. 3, библ. 12 (на английском языке; рефераты на английском, русском и литовском яз.).

A. Vindašius. Bevielės prieigos tinklų saugumas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2006. – Nr. 7(71). – P. 19–22.

Eksploatuojant bevielius tinklus susiduriama su daugybe saugumo klausimų, kurių daugelio laidiniuose duomenų perdavimo tinkluose apskritai nekyla. Kadangi duomenų paketai perduodami beviele, visiems bendra ir laisvai prieinama terpe, iškyla didelė atskirų tinklų izoliavimo ir privatumo problema. Trumpai aptariami bevielių vartotojų tinklų saugumo pažeidžiamumo klausimai. Atlikti pasyvaus 2,4 GHz ruožo skenavimo Vilniaus mieste tyrimai rodo bendrą privačių bevielių tinklų saugumo lygį, naudojamą šifravimą, pagrindinius bevielių prieigos taškų konfigūracijos ypatumus. Surinkti duomenys rodo, kad dažniausiai bevielių tinklų saugumo problemų iškyla traktuojant bevielius prieigos taškus kaip patikimas zonas bendroje tinklo topologijoje bei nešifruojant kanalinio lygmens. Il. 3, bibl. 12 (anglų kalba; santraukos anglų, rusų ir lietuvių k.).