Annales UMCS Informatica AI 3 (2005) 305-313

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI

http://www.annales.umcs.lublin.pl/

Wireless LAN at home, in institutions and organizations

Ryszard Haraszczuk*

Software Engineering and Database Systems Division, Institute of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract

Cheap and available wireless devices are commonly used at our home and in institutions. Wireless local area networks (WLAN), new type of networks set us free from problems of changing wall socket location. That kind of LANs makes access to the Internet more comfortable. We do not have to drill holes in walls and put cables to connect another workstation to the existing network. To avoid such problems we can plug the access point install wireless cards and use the wireless LAN to connect to the Internet. It is a good idea to go this way, but there are some questions associated with that: "Are wireless networks secure?", "Don't our data be eavesdropped by intruders?". That article depicts and explains steps that should be taken to build secure wireless LAN in different places, home institutions and financial institutions with top-secret data. The currently used methods of protecting WLAN from unwanted access are presented here. The article presents also some non-standard safeguards.

1. Introduction

Recently WLAN technologies has found an important place in LAN architecture. Low costs of WLAN implementation caused that many people use them commonly. Wireless fidelity (Wi-fi) LANs are popular solutions in institutions, at schools and finally more and more often at home. Some risks are involved with implementation of WLAN solutions and not every user is conscious of those weaknesses. One of the most fundamental weaknesses is the ability to sniff packets without being discovered. That ability is caused because of type of medium that is used to transport packets. Access points propagate packets over radio waves and anybody can sniff them. Unsecured and not configured WLAN networks are common in cities. Such networks give an easy way to read data sent by open WLAN and cause loss of data. Some users can say that they do not have any valuable data and possibility of losing them is not a problem. Most of such users do not relalize that open networks make a possible for intruders to connect. Intruder can use such connection to break into the bank

* *E-mail address*: r.haraszczuk@pollub.pl

or other institutions. Innocent owner of WLAN can be punished for intruder's action. The second chapter of this paper describes commonly used methods of safeguarding WLAN. There are described ways of authorization and authentication methods used currently in WLAN. The third section of this article shows steps to deploy secure wireless network in different places depending on character of deployment place. Additionally, in the third part of paper there are proposed easy and non-standard methods of such networks protection.

2. Currently used authorization methods

There are two layers of OSI model, which give possibility of authentication implementation. The second and third layers of OSI model provide such possibility. At present there are three ways of implementing authentication in the second layer of OSI:

Open authentication – used in the case of hot spots, where everyone has the possibility of connection with the access point. Moreover, anybody is able to connect to WLAN. However, only users who pass the second authentication system are able to connect to the Internet [1].

The shared authentication; a client has got to use the key to acquire the ability of using the network. Every user of such network has the same static key that is stored on the workstation. The data sent by network configured that way are encrypted by WEP protocol.

WPA – Wi-fi protected access – authentication of clients is done by one of the EAP protocol versions. There are a few versions of EAP protocols used commonly in WLAN: EAP-TLS, EAP-TTLS, EAP-LEAP and others. Type of used EAP protocol depends on vendor of WLAN device and operating system. Advance Encryption Service (AES) or WEP with Temporary Key Integrity Protocol (TKIP) encrypts the data sent by the network configured that way.

WEP – Wired Equivalent Protocol is a wireless security protocol for the wireless Local area networks. WEP provides security by encrypting the data that are sent through WLAN. Both the Access Point and client use the same key to encrypt data. Client is able to connect to the Internet only in the case of using the correct key. Encryption of data sent by that method has some vulnerabilities. First and most obvious is that intruder can read the key from the network settings. In such a case the whole network is unsecured. Another weakness of that protocol is algorithm used to encrypt data. WEP uses RC4 algorithm to encrypt data. RC4 is a key stream algorithm. Clear data are combined with key stream by XOR operation and that way RC4 produces encrypted data. To decrypt data we need the same key stream. Combining encrypted data with the key stream by XOR operation gives clear data. The problem is that exclusive disjunction is symmetrical. When the attacker knows plain and encrypted data he can achieve key stream. Intruder can send special broadcast packets and collect encrypted data to get the key stream. When he has key stream he can see what is

sent over WLAN. WEP has an initial vector (IV) that was added to avoid weaknesses of RC4 algorithm. The initial vector was proposed to generate different encrypted data from the same plain data. Unfortunately, the initial vector is sent as the field in packet so there is no problem to read it. The vulnerabilities of WEP protocol mentioned earlier persuade producers to work on new protections. Manufacturers added to WEP ability of dynamically changing keys. Temporary Key Integrity Protocol (TKIP) responsible for controlling and automatic key changes was proposed. To raise security WLAN devices additionally got the ability to authenticate by EAP protocol. Those two changes Wi-fi alliance announced as Wi-fi Protected Area (WPA). Currently we have two versions of WPA.

WPA 1.0 – Wi-fi Protected Access version 1 – Uses dynamically changing key protocol – TKIP, to ensure more security of two keys used to encrypt data. One for data sending over broadcast and the other for data sending between station and gateway. Authentication is done by EAP protocol. Additionally, from protect before replay attacks Message integrity check is added to the packet. MIC is calculated before the packet is encrypted and put inside the packet before it is sent. Access point decrypts packet and rejects packets with bad value of MIC. Unfortunately, data are still encrypted by WEP protocol.

WPA 2.0 – Wi-fi Protected Access version 2 – also uses TKIP to ensure dynamically changing keys. That version of WPA specification has MIC to protect network from packet injection attack. The second version of WPA has a stronger encryption algorithm. It uses Advanced Encryption Service (AES) to encrypt and decrypt data. Both AES and RC4 are symmetrical algorithms. That algorithm is more complicated and that is why it gives more security to WLAN. AES due to its complexity needs faster processors to encrypt data. Old WLAN devices cannot use that encryption method because of greater requirements of encryption algorithm.

Both versions of WPA can work in two modes. The first designed for home users and the other one for institutions:

WPA-PSK – that mode is designed for home users who do not have the authentication server. It is often named as WPA-Personal [3]. Key used to authenticate at Access Point is statically kept on the workstation. That key is used in the process of generating Primary Master Key (used to encrypt the data sent between workstation and gateway), and Group Master Key (used to encrypt the data sent to broadcast).

WPA-EAP – that mode is designed for institutions. Every user of WLAN has its own key. It is often named as WPA-Enterprise [3]. Authentication is made by Radius server (Remote Authentication Dial-In User Service). Radius stores users names and keys. Access Point is Network Access Server (NAS) between the authentication server (RADIUS) and the station (STA). That mode resolves a problem of one shared key for the whole institution. When one key is stolen only

the device using that key is compromised. Other connections use a different key and are secure.

The above mentioned authentication methods used the second layer of 7 layer OSI model. As mentioned before there is also ability to authenticate clients over the third layer of OSI. Authentication in that layer is based on IP addresses. An example of such authentication scheme is Virtual Private Networks. Commonly we have several protocols supporting building VPN's. VPN can be established over IPsec protocol or over SSH protocol or SSL protocol. Protocol used to build VPN depends on type of software and operating system.

3. Customization

We can adjust the ways of authentication described in the previous section to security level used in our home or institution. Applying a high secure model can cause a waste of time and financial sosts. Security level should be adapted to value of stored data and dangers that can come into institution or home. Wireless devices implement some safeguards that are easy to pass over. We should remember that sometimes even the easiest safeguards could stop some intruders. We should not omit any of those easy safeguards. Below there are described steps to implement secure WLAN in different places.

3.1. Wireless LAN at home

Home WLAN is made of access point and sets of computers with wireless cards connected to the Internet service provider wall socket or modem. The example of home network is shown in Figure 1.

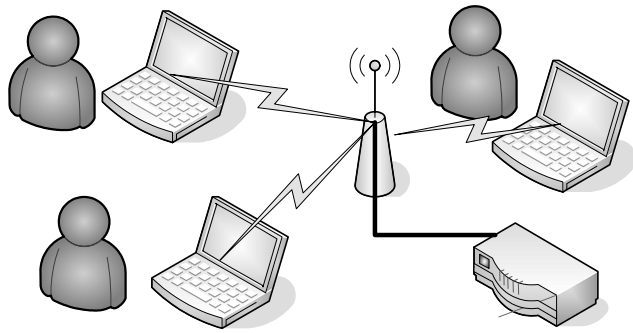


Fig. 1. WLAN network at home

A private user is thrown back on standard safeguards offered by wireless devices because of the modest budget allocated to implement WLAN. That is why all of the safeguards delivered with wireless device should be turned on during implementation of wireless network at home. Below there are described standard safeguards that can be turned on during the setup process. First of all

the home user should change default network Service Set Identifier (SSID). Secondly propagating of network SSID should be turned off. Does anything exist if it is not seen? Disabling SSID propagation protects from intruders. That protection is easy to pass through by sniffing network and reading SSID from packets. That is why the home user should define media access control addresses (MAC address) allowing to communicate with the access point. Advanced intruders can sniff packets sent by such a network and achieve MAC addresses that are allowed to communicate with the access point.

The home user should also set up WLAN with the support for Wi-fi protected access. Older devices, which do not support that mode, can achieve that ability by upgrading firmware. It seems to be reasonable to use devices with WPA 1.0 at home due to high costs of devices equipped with WPA 2.0. Buying devices with support of WPA 2.0 is good when the home user builds a new WLAN network. Such a user should turn on the data encryption by AES.

Home users can reduce the range of WLAN by limiting power propagated by the access point. Limiting transmit power is a non-standard safeguard. Home users quite often omit that safeguard. After limiting power the home user should examine a new range of such network and affirm whether radio waves are not propagated outside the building. The example of configured WLAN is in Figure 2.

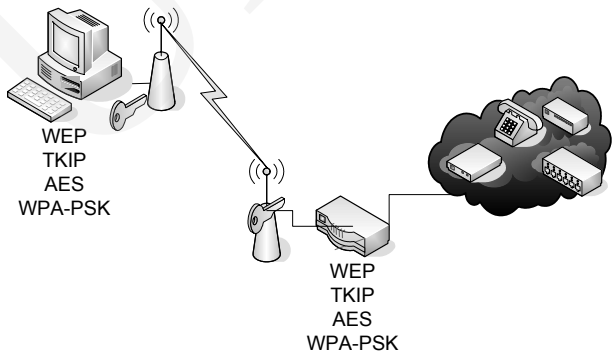


Fig. 2. Secured home WLAN

Limiting time of WLAN device work is another safeguard. The home user can use time switcher to achieve that. This is the second non-standard safeguard that can raise security of home wireless network. The user can define hours in which WLAN will work. For example, during the night between ten p.m. and six a.m. the access point can be turned off. Figure 3 shows such a switcher. Another kind of switcher is a remote switcher. It can also be used to raise the security level. This type of remote switcher enables turning off unplugging the AP whenever it is wanted.

Fig. 3. Time switcher and remote switcher

3.2. Wireless LAN in institutions

Before installing wireless LAN in institutions security policy should be created or a section of wireless LAN in existing policy should be added. That section should forbid installing any access points and ad-hoc networks in institutions without IT staff knowledge. Security policy should fix hours in which WLAN devices operate. Type of data encryption used in network should be specified. The company security set should describe configuration of access points, wireless cards and operating systems. Company department responsible for installing and managing WLAN devices should be pointed to [3].

Additionally, security policy should fix procedures taken before any WLAN hardware is connected to the existing network. For e.g. registering MAC address of wireless card, setting up operating system, turning on encryption etc.

3.3. Setting up wireless LAN

IT department responsible for wireless LAN should have in-depth knowledge about all the security settings available in WLAN devices. Wireless LAN should not be connected directly to the wired network. All traffic between wireless and wired network should come through the firewall. All the safeguards delivered with wireless device should be turned on in the process of installing wireless network in institutions. The default network SSID should be changed to the maximum available length. What is more, the network SSID should not be propagated. Default passwords and IP of device should be changed. IP of device should use different address scheme and different class of network address. Access points should be placed out of reach to prevent from reconfiguring or resetting by unauthorized people.

Authentication by WPA protocol with the Radius server should be implemented to achieve the high security level. Using the Radius server gives more flexibility and simplicity in managing users' names and passwords. It also helps to manage MAC addresses of trusted wireless cards. It short period of time should be fixed for key change in the case of using the first version of WPA protocol.

Additional security can be achieved by setting up monitoring access points. That type of access points scans all the radio channels to detect rouge access

points set by intruders or frustrated employees. Monitoring the access point can also inform about off-hours traffic, unencrypted traffic, ad-hoc networks, and improper configuration of access points.

Example of configured and properly implemented networks is in Figures 4 and 5.

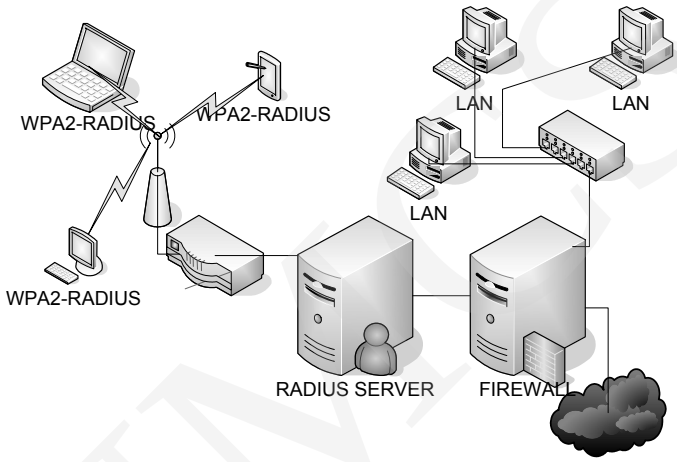
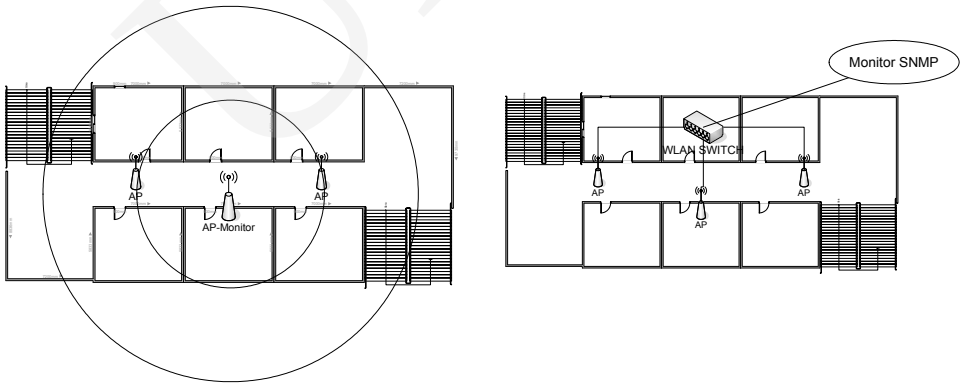


Fig. 4. WLAN in institution



(a) (b)

Fig. 5. Monitoring WLAN in institutions a) wireless monitor b) wired monitor

Setting up authentication with the Radius server is difficult but in the future it will give possibilitz of easy management of wireless users.

Limiting wireless LAN range can be achieved by directional antennas placed in corners of building. That is another kind of non-standard safeguard. Power of propagating access points should also be adjusted to the range of those antennas. Position of those antennas should be experimentally assigned. A new range of wireless network should be examined after the process of placing antennas.

When the range of WLAN goes beyond the building, positions of antennas should be changed. The example of limiting wireless range is presented in Figure 6.

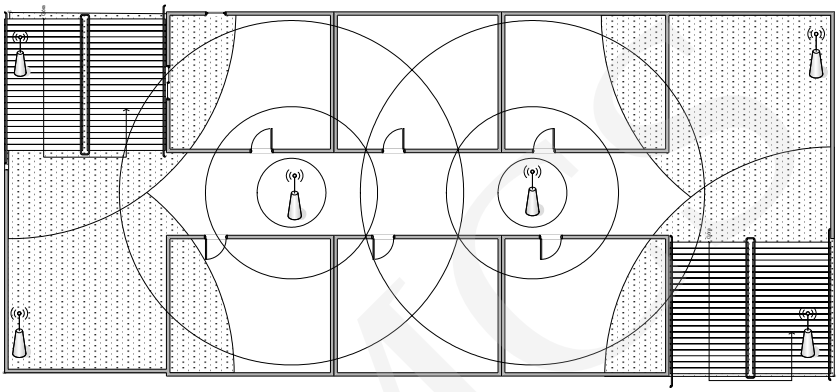


Fig. 6. Limiting WLAN range by set a of antennas

3.4. Wireless LAN in organization with top-secret data

Implementing wireless LAN int such places is not recommended. Institutions with top-secret data and financial institutions should avoid using WLAN. Only in the case of architectural restrictions in historic buildings wireless networks can be used. Implementing such networks in those places need to set up all the safeguards mentioned before. Security policy should be created. All the wireless device safeguards should be turned on. Additionally, it is recommended to set up a virtual private network for the users with wireless workstations. Currently VPN gives the higher security level of WLAN. Firewall should allow traffic only from VPN-workstation to VPN gateway. The example of such secured network is shown in Figure 7.

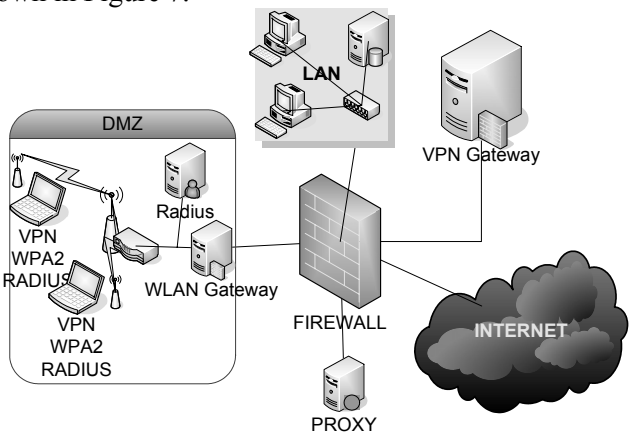


Fig. 7. WLAN in organization with top-secret data

4. Conclusion

Wireless networks are a very convenient solution. They free us from sets of cables. It is a good idea to install wireless LAN in institutions and at home.

This article points to some additional risks of wireless LAN. It gives some ideas of protecting such networks. The article shows safeguards implemented in 802.11i standard. There are described different types of protection build in it. Standard and easy to pass through safeguards are also mentioned. The third paragraph has also a few non-standard safeguards connected with limiting transmit power. The article describes two different methods of limiting transmit power, one by limiting output power of access point. That method is easy and available for home users. The second one is that the range of wireless LAN by placing different types of antennas. It is obvious that properly configured wireless LAN is secure. Currently there is no reason not to trust WLAN security.

The main purpose of this article is to show different safeguards used at home, in institutions and places with too secret data.

References

[1] Regan K., *Wireless LAN Security: Things you should know abort WLAN security*, Elsevier Science Ltd., (2003).

[2] Wi-Fi Alliance. (2003). Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. Retrieved March 1, 2004 from http://www.wifialliance.com/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf.

[3] von Solms B., Marais E., *From secure wired networks to secure wireless networks – what are the extra risk?*, Elsevier Science Ltd., (2004).