Trakia Journal of Sciences, 7, Suppl. 2, pp 134-137, 2009

Available online at:
http://www.uni-sz.bg
ISSN 1313-7050 (print)
ISSN 1313-3551 (online)

Original Contribution

THE SECURITY SUGGESTIONS FOR WIRELESS ACCESS POINTS

Deniz Mertkan Gezgin[1], Ercan Buluş[2], Halil Nusret Buluş[2]

[1]Trakya University Vocational College of Technical Science, Trakya University, 22030,Edirne, Turkey

[2]Namik Kemal University, Corlu Engineering Faculty, Computer Eng. Dept, Turkey

ABSTRACT

The usage area of wireless networks has been increased by the increase on the development of 802.11 wireless networks. As a result of this, the security on wireless networks has become more important. Various cryptographic algorithms have been developed on the subject of the security and they have been used in many wireless network applications. IEEE has started to work on security of wireless networks under the 802.11i standard. As part of these, various cryptographic algorithms have been developed and stronger algorithms take the place of inadequate ones. So providing a secure environment on wireless networks has been proposed. In this paper, the security standards used in access points which are wireless networks devices, the cryptographic algorithms used by these standards and the superiority of these algorithms are studied.

KeyWords: *Security of Wireless Networks, MAC Adress Filtering, Wep, WPA, 802.11i*

INTRODUCTION

Recently wireless networks are used widely. Being rid of cables and developments of the performances of wireless networks effect it .. The usage areas has been increased parallel of development of wireless networks and the increase on the standards. The places like offices, amusement places, hotels which have variable visitors and the places like factories, houses are places which wireless networks are locally used. In these places a device like hub in wired networks is used to access to the wireless networks, internet share or to set up a local network. These devices are named "access points". They are confused with the wireless modems which are bought or given by internet providers. Because some of the wireless modems have access points properties. In another words wireless modems used like access points exist. Access points can be used for many scenarios like repeater, bridge. These properties will be discussed. In fact the main idea in this study is the increase of usage of access points because of the increase of using wireless networks. In this case, many clients and users appear. Some of them are permitted users and some of them are attackers who want to damage the network, slow down the speed and destroy the access points. There are policies in the wireless networks to prevent this. Most important one of them is locally most used networks have recently used or developing security policies. The usage of them changes according to the security demand. The subject dealed in this study is security mechanisms and strategies used in wireless clients.

Access poInt

Access points are known as shortly AP or WAP (Wireless Access Point). Access point provides a wireless access to the wired ethernet network. Access points are connected to hub, key and wired router and send wireless communication signals. APs act like cell phone towers: pass from one location to another so wireless access goes on. They can be shown as equivalent to hubs on wired networks. AP devices have their own memories. They include a software named Firmware. This firmware can be updated according to new updates and developments. Access point devices have security protocols. Some of them are WEP(Wired Equivalent Privacy) ,WPA (Wi-Fi Protected Access) and

***Correspondence to**: *Technical Science Vocational Higher school, Trakya University, 22030, Edirne, Turkey;*
e-mail: d_m_gezgin@hotmail.com

WPA2. APs shouldn't be confused with wireless modems and routers. Mostly we use wireless modems or routers to access internet in our homes. Beside this, when wireless networks open for general use are used to access to the internet at airports, student boardinghouses, restaurants or hotels, generally access points are used

Figure 1. *Wireless Access Point*

Wireless access points basically have 3 properties. These are default mode, repeater mode and bridge mode. Access points carry the data signals to environment wirelessly by RF signals. Bridges attaches the devices that are not have wireless properties. So they help these devices used commonly. Repeaters strengthen the wireless RF signals so they increase the range.

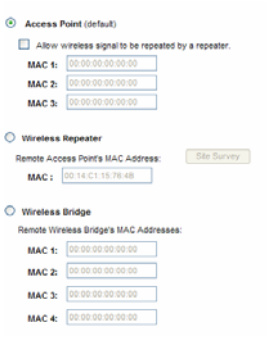

Figure 2. *Wireless Access Point Modes*

SECURITY SUGGESTIONS FOR ACCESS POINTS

Some security problems have appeared since wireless networks have become more popular. Since wireless access points or modems broadcast, all PCs that have wireless Ethernets and notebooks can see this broadcast. As a result of this, attackers who have unauthorized access to the system may cause slowing down the system speed, or may get a security password in the system. They can take knowledge about the system by listening to the RF. Some security standards and policies have been developed to prevent these attacks. In this study, security mechanisms that are included in wireless access points has been analyzed.

a) SSID (Service set identifiers) Hiding

SSID(Service set identifiers) is called as wireless network name in order to understand easily. Access point is the name of it as default but we can also give a name to it. You can see wireless networks of different names after scanning. This is called SSID. Wireless access points can broadcast in different channels. If you hide access point, unauthorized users can't send connection request to the system since they do not see the name of the access point in the wireless networks list. Specialists on this subject can find SSID and its channel by using 3rd party software. DoS (Denial Of Service) attacks can be done to the wireless access points whose SSID is open. So hiding SSID will be useful. Hiding operation is done by the device software. After the hiding operation, users can no more see the SSID in Windows platform unless they use a 3rd party software. Authorized users can connect to the network automatically if they have known the SSID and its password.

b) Changing Default Password Of Wireless Access Points

When you buy a wireless access point, eah company has its own web interface to connect to the device to manage it. Authorized users or users the places which have a wireless network without a password can easily access to the interface by using gateway adress. One way to prevent this is changing the password used for connecting the access point. For example, most known user – pasword combination is admin – admin. When we buy an access point device we need to change this combination. If we don't, unauthorized users can change device settings.

c) MAC Filtering

The word MAC is composed of the first letters of Media Access Control. It is also known as physical adress. MAC adress is installed by the productor company. It can not be changed in normal ways and the most important is every network card has a different MAC adress. MAC adresses are written in 48 bit chiper and each machine has its own adress, it means that, your PC or notebook has its own MAC adress. So a network card uses this MAC adress to send data to another network card. It seems as two or more cards can have same number. But in fact the number produced under 48 bit can have 281.474.976.710.656 possible MAC addresses. So it is not possible to have same number. Access points filter the clients requesting the connection to the network by this number to decide if the client will connect or not connect. To do this in security section, MAC filtering should be activated and allowed MAC addresses should be entered. So access point gives permission to these computers. If the one who entered the password of the access point correctly is not in the list, he can not connect to the network. A MAC address can be shown as 01-23-45-67-89-ab.

d) WEP Chiper and Its Usage

WEP is a wireless network standard. In wired networks its corresponding protocol is named as

802.1 by its developers. It is exactly named as Wired Equivalent Privacy. The function of WEP is to encrypt the data on radio waves. WEP designed to compete with the traditional network secrecy is accepted as a part of 802.11 standard in 1999. WEP uses RC4 cryptographic algorithm designed by Ron Rivest for secrecy and CRC-32 checksum for completeness. The key width used in WEP is 40 or 104 bits. There are two verification methods in WEP.

1. **Open Key Authentication:** Any client can connect to the network by self authentication and ignoring WEP keys.

2. **Common Key Authentication:** WEP is used for authentication in Shared Key Authentication. In this communication there are 4 ways to request and answer.

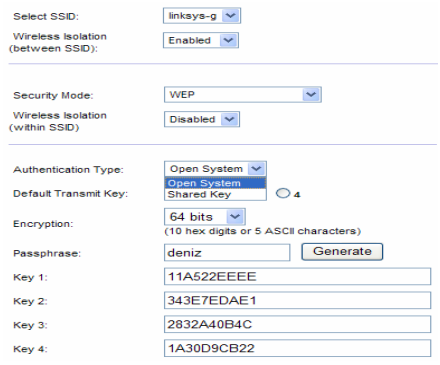

Figure 3. *WEP Authencation*

In WEP, RC4 cryptographic algorithm is used with the common key on clients and access point. But recently, on Linux or Windows platform, common key can be taken with some software. The weakness of RC4 algorithm and no key management mechanism for common keys cause this. Encryption does not provide enough secrecy because of usage of 24-bit Initialization Vector (IV) causing repeating encryption arrays. Common key can be got by recording enough data traffic.

e) WPA Chiper and Its Usage

Wi-Fi Alliance has made WPA standard to overcome the weakness of RC4 algorithm on WEP standard. WPA supports TKIP and TKIP (Temporal Key Integrity Protocol) has taken the place of WEP as a strong cryptographic system. TKIP uses a new cryptographic algorithm using computing facilities of wireless devices to carry out ecriyption process. Also TKIP provides some properties like correction of security configuration after ecryption keys are determined, changing one point broadcast ecryption key for every window simultanously, detection of uniquely start of common key authentication. WPA uses 128 bits for key length. In WPA, key is changed for every session and every package so much more security is provided. 802.1x is used for key management in WPA. WPA uses a strong method with 802.1x EAP for authentication. In WEP data integrity is provided by ICV, beside of this WPA uses a stronger mechanism called MIC(Message Integrity Code). WPA gives 2 alternatives for authentication/authorization.

1. WPA-PSK Structure

It has been designed for home users and small companies. A password in length 8-63 characters is determined. This is needed to be entered both in client side and in access point side. This is called pre-shared key. We choose WPA-PSK from the authentication method in network connection properties. It is not suitable in corporation wireless networks.

2. 802.1X Structure

IEEE 802.1x is a port based network access control mechanism and is used in wired networks as authentication/authorization method of units/applications like remote access, VPN, key production device etc. The components of 802.1x access control are client (laptop, PDA, cell phone, PC etc.), access point and RADIUS/TACACS access control server. Clients notify the access point about connection request, access point leads this request towards the RADIUS/TACACS server, RADIUS/TACACS server makes the authentication/authorization process and tells the result to the client and server. According to this result, access point opens a virtual port to the client for connection. In addition to this after these processes the encryption key is produced for encrypted communication between client and access point.

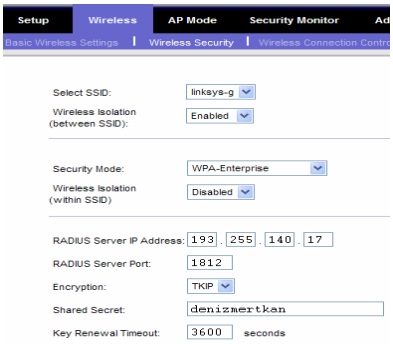

Figure 4. *WPA-Enterprise (RADIUS Server)*

f) WPA-2 Encyption (IEEE 802.11i)

It is a security standard produced by IEEE 802.11i work group to overcome the all weakness of WEP. It is also known as WPA2 or Robust Security Network (RSN). It is recommended to be used for authentication/authorization of 802.1x and for data integrity and encryption in Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) mode of Advanced Encryption Standard (AES)

cryptographic algorithm. It uses the same structure in WPA which is 802.1x. Advanced Encryption Standard (AES) cryptographic algorithm is used in Counter Mode. A structure that prevents repeating encryption key without the help of per-packet keying mechanism in TKIP and IV used in WEP and TKIP is produced by this method. AES is stronger than RC4 and it has no known weakness. TKIP structure using RC4 cryptographic algorithm for compatibility of hardware not supporting AES is found in IEEE 802.11i standard.

RESULTS

Security standards and policies in wireless networks can be change in every situation. The method used by home user and the method in a company that need a high security is different. SSID hiding is not exact security prevention but it can be useful for some attackers. If WEP and MAC filtering are used together, networks become more secure. But although it loads weight to the system, generally WPA2 is the strongest structure because it uses AES and AES has no security holes until now. Weaknesses based on RC4 in WEP and TKIP supported by WPA based on RC4 make the key easily taken. RADIUS server usage in 802.1x authentication method increases the security. As a result WPA2 and 802.1x are the advised security standards.

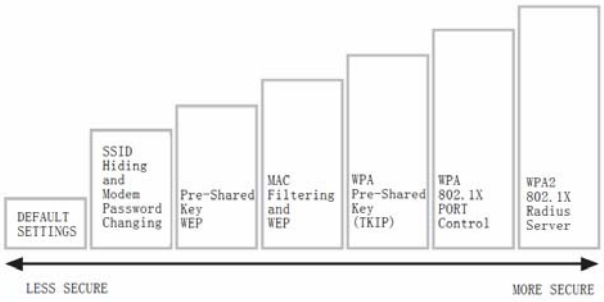

Figure 5. *Wireless Network Security Level*

REFERENCES

1. Matthew Gast , “802.11 Wireless Networks The Definitve Guide” ,O’Reilly,April 2005 , 0-596-10052-3
2. David Johansson , Alexander Sandström Krantz , “Practical WLAN Security”, TDDC03 Projects, Spring 2007
3. Deniz M. Gezgin, E. Buluş, “Kablosuz Erişim Noktalarına Yapılan DOS Saldırıları”,
4. Akademik Bilişim 2008, Çanakkale 30 Ocak-1 Şubat 2007
5. Deniz M. Gezgin, E. Buluş , H. N. Buluş, “The Technical Analysis of the Comparison of 802.11n Wireless Network Standard”, International Scientific Conference ,21 – 22
6. November 2008, Gabrovo
7. Borsc, M., Shinde, H., “Personal Wireless Communications, 2005. ICPWC 2005. 2005
8. IEEE International Conference on”, 0-7803-8964-6, 23-25 Jan. 2005
9. Battal Özdemir (2008), “Kablosuz Yerel Alan Ağı Güvenliği Klavuzu” ,BGT-6001
10. IEEE Std 802.11i™-2004, “Wireless LAN Medium Access Control (MAC) and
11. Physical Layer (PHY) specifications, Medium Access Control (MAC) Security
12. Enhancements”
13. WPA and WPA2 Implementation White Paper “Deploying Wi-Fi Protected Access
14. (WPA™) and WPA2™ in the Enterprise”, March 2005
15. G.Zeynep Gürkaş, Şafak Durukan, A.Halim Zaim, Azer Demir, M.Ali Aydın, “
16. 802.11b Kablosuz Ağlarda Güvenliğin Ağ Trafiği Üzerindeki Etkilerinin Analizi”, II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi , MBGAK 2005 ,İstanbul ,Kasım 2005