I.J. Wireless and Microwave Technologies **2012, 4, 21-27**
Published Online August 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2012. 04.04

Available online at http://www.mecs-press.net/ ijwmt

A New Secure Strategy for Small-Scale IEEE 802.11 Wireless Local Area Networ

Huiting Liu [a, b], Hua Zhang [a], Weilin Xu [a, b], Yigang Yang [a, b]

[a] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications*
[b] *School of Computer, Beijing University of Posts and Telecommunications Beijing, 100876, China*

Abstract

As the main secret-key encryption techniques of the wireless local area network (WLAN) have been proven to be unsafe, wireless network security is faced with serious challenges. It is unpractical for home users and small companies to buy expansive network equipments to improve the network security. Therefore, the secure strategy of wireless network needs to be changed. In this paper, we first introduce secure issues of the main secret-key encryption techniques currently adopted by the most popular commercial wireless routers. Then we propose a new strategy for small-scale IEEE 802.11 wireless local area network which can strengthen the network security. The new secure strategy is based on web authentication with unshared key and virtual local area network (VLAN) in wireless network. It can provide protection against practical attacks which are popular nowadays. Moreover, it is simple, wieldy and low-cost.

Index Terms: WLAN; secure strategy; web authentication; identify theft; VLAN

1. Introduction

Wireless network brings great user experience to people for its flexibility, portability and low-cost. Commercial Wireless Local Area Network (WLAN) products are widely available on the market and most of them setup easily and operate simply. WLAN is rapidly deployed around the world. More and more public places, offices and even homes set up their own WLANs. Thus, the demand for wireless network security rises sharply. Encryption techniques such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access-Enterprise (WPA-Enterprise) and WPA-Pre-Shared Key (WPA-PSK) are the main means to protect the security of WLAN at present. WPA-Enterprise requires a Remote Authentication Dial-In User Service (RADIUS) server which is expensive and difficult for common user to setup. Because most small-scale wireless network will not select this strategy, we focus on WEP and WPA-PSK.

Corresponding author:
E-mail address: liuwaiting@gmail.com

WEP is the most widely used security algorithm for IEEE 802.11 wireless network. Several serious weaknesses in the protocol have been shown by cryptanalysts. In 2007, a research proposed a new attack which could recover a 104-bit WEP key with probability 50% less than one minute using only 40,000 captured packets [1].

WPA is defined in response to several serious weaknesses in WEP. WPA-PSK is designed for home and small office networks. Because the four-way handshake during the authentication is not protected in the WPA-PSK network, it is vulnerable to the password cracking attacks if users rely on a weak passphrase. In reality, most people use a simple password as a pre-shared passphrase. In November 2008 Erik Tews and Martin Beck—researchers of two German technical universities (HTU DresdenH and HTU DarmstadtH)—uncovered a WPA weakness which stems from a previously known flaw in WEP [2]. The flaw can decrypt short packets with mostly known contents, such as address resolution protocol (ARP) messages. In February 2010, a new attack was found by Martin Beck that allowed an attacker to decrypt all traffic towards the client [3].

Not only cryptanalysts and professional hackers can crack passwords of wireless network, but also ordinary computer users can do this by some decryption software such as Spoonwep and Spoonwpa in the famous hacker platform—Back Track 4. Tutorials of these decryption software can be found easily from the Internet. As a matter of fact, because of the existence of the WLAN decryption software, there are a lot of people stealing other people's network resources without paying.

In order to provide secure WLAN and resist existing attacks, a new secure strategy is needed. However, the new strategy must be able to be adopted by the existing wireless routers because millions of wireless routers have been released to market and are in use. Moreover, the new secure strategy should resist existing attacks and not introduce any new vulnerability. Finally, the new secure strategy should not increase users' financial burden.

Here, we propose a new strategy based on web authentication with unshared key and virtual local area network (VLAN) in wireless network.

We choose Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) and Message-Digest algorithm 5 (MD5) to provide protection for the user passwords in the web authentication. A random string is set to ensure that the login information is unique every time. Therefore, Wi-Fi-password decryption software will fail in the web authentication.

In order to solve identify theft on the existing wireless routers. We divide the WLAN into two VLANs. Client devices which have not passed the authentication and those have passed the authentication are administered separately in the two VLANs. Thus the hacker can't send packets to get IP address and media access control (MAC) address from valid users.

Our new secure strategy has the advantages of simplicity and compatibility with the existing wireless routers. It strengthens the security of wireless network and does not introduce new secure issues. Users can replace the old strategies with our new secure strategy or add it as a part in the network security framework according to the demands.

The rest of this paper is organized as follows. Section 2 introduces some relevant knowledge occurred in this paper. Section 3 illustrates our new secure strategy. Section 4 evaluates the security of the new secure strategy. Finally, Section 5 gives our conclusions.

2. RELEVANT KNOWLEDGE

2.1. Hypertext Transfer Protocol over Secure Socket Layer

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a combination of the Hypertext Transfer Protocol with the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol to provide the encrypted communication and the secure identification of a network web server. HTTPS can provide sufficient protection against the eavesdropper attack and the man-in-the-middle attack.

2.2. Message-Digest Algorithm 5

This work is supported by the Research Innovation Fund for College Students of Beijing University of Posts and Telecommunications (Grant No. 101104537).

Message-Digest algorithm 5 (MD5) is a widely used cryptographic hash function which can produce a 128-bit hash value. It has been shown that MD5 is not collision resistant [4] [5] [6], but recovering the source value is still impossible. Therefore, MD5 is still employed in a wide variety of security applications.

2.3. Identity Theft

In this paper, identity theft is narrowly defined as identity theft happened in Local Area Network. Network access system usually identifies client devices according to their IP addresses and MAC addresses. By thieving IP address and MAC address, the hacker can pretend to be a valid user to access the network and do whatever he wants.

2.4. Virtual Local Area Network

Virtual Local Area Network, commonly known as VLAN is a data exchange technology which can divide local area network into separate segments thereby creating virtual workgroups. VLAN provides the flexibility to adapt to changes in network requirements and allow for simplified administration. By using VLAN, administrators can also control traffic between different segments to strengthen the network security. In recent year, VLAN has been applied in wireless network. Wireless routers with VLAN are widely available on the market.

2.5. Service Set Identifier

Service Set Identifier (SSID) is used to identify a particular 802.11 WLAN. A client device receives broadcast messages from all access points within range advertising their SSIDs. The client device can then either manually or automatically—based on configuration—select the network with which to associate. SSID broadcast can be forbidden, in this way, wireless network will not occur in the network selecting list on client devices.

2.6. The Man-In-The-Middle Attack

The man-in-the-middle attack is a form of indirect intrusion. The attacker makes independent connections with the victims at both ends of a conversation and relays messages between them. The victims believe that they are talking directly to each other over a private connection while the entire conversation is controlled by the attacker. The attacker can obtain secrets and privacies which he is interested in by analyzing the messages going between the two victims.

3. A NEW SECURE STRATEGY BASED ON WEB AUTHENTICATION WITH UNSHARED KEY AND VLAN IN WIRELESS NETWORK

3. 1 Web Authentication with Unshared Key

In reality, most wireless networks in homes or small offices are protected by Wi-Fi-password and almost all WLAN decryption software available in Internet aims at cracking the Wi-Fi-password. According to the actuality, in our new secure strategy, we set a mini web server in the wireless router. The mini web server provides a Web Authentication with unshared key, that is, every user has his own name and password. The user information is stored in a special file which can only be read and written by the root user. Before accessing network, all users must correctly input their names and passwords on an authentication web page. The Web Authentication is similar to WPA-Enterprise. However, it does not need additional equipments and based on different encryption. According to the actual security demand, users can replace the Wi-Fi-password Authentication with the Web Authentication or add the Web Authentication as a part in the network access authentication process.

We choose HTTPS and MD5 to ensure the security of the authentication process.

The Web Authentication is based on Client/Server model and it is similar to the 802.1x authentication, but simpler. The authentication process is shown in the Fig.1.

Step1: The Client sends a Login-Request to the Server to apply for the authentication.

Step2: The Server sends a MD5-Challenge to the Client which contains a random 16-byte string.

Step3: After receiving the MD5-Challenge, the Client adds the random string to the end of password and calls the MD5 function to deal with them. The MD5 function returns a 128-bit string and then the Client sends it with the username as a MD5-Response to the Server.

Step4: After receiving the MD5-Response, the Server checks the user data and gets the corresponding password. The server does the same thing as the Client does in step3 to get a hash string. If the string in the MD5-Response matches the string produced by the Server, the corresponding IP address and MAC address will be recorded. Then a Success page will be sent to the Client and the Client is allowed to access the network. If the Client submits incorrect information, it will receive a Failure page.

The logoff process needs two steps:

Step1: The Client submits a Logoff-Request to the Server.

Step2: The Server cancels the Client's network access qualification and sends a Logoff page to the Client.

In the view of the security, the random string can be used only once and a life time is set to indicate the valid time of a random string to a specific client. If the Server doesn't receive the MD5-Response from the Client in the life time, the random string becomes invalid. If the Client wants to continue the authentication, it must send a new request to get a new random string. In addition, if the Client submits incorrect information ten times continuously, it will be refused to login in an hour.

3. 2 A Solution to Identify Theft

In the new security framework, whether a packet is from a valid user is determined by its IP address and MAC address. After cracking the Wi-Fi-password, the hacker can get IP addresses and MAC addresses of valid users easily. Therefore, the new security framework is vulnerable to identity theft.

The most effective and widely used method to deal with the identity theft is IP-MAC-port-bind which means setting a binding of IP address, MAC address and port. The specific user's data stream can only get through the network from a corresponding port. The hackers cannot find out which port is the correct one, so identity theft is useless. However, IP-MAC-port- bind can only be done on advanced switches.

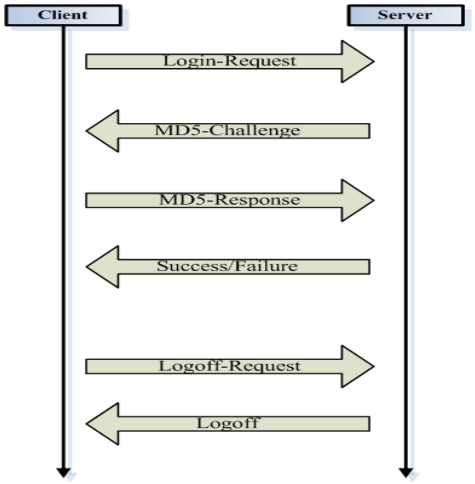

Figure 1. Web authentication

We propose our strategy based on VLAN in wireless network. We divide the WLAN into two VLANs marked as VLAN0 and VLAN1 separately. VLAN0 associates with client devices before authentication and its SSID broadcast is permitted. VLAN1 associates with client devices after authentication and its SSID broadcast is forbidden (Fig.2). In this way, client devices can only receive broadcast messages from VLAN0. When a computer connects to the router, the IP it got is from VLAN0. After submitting correct username and password, it will receive SSID information of VLAN1 from VLAN0. Then the user can associate the computer with VLAN1 and gets a new IP. A rule is written in route table to forbid communications between the two VLANs. Thus the hacker can't send packets to valid users to get their IP addresses and MAC addresses, he even cannot get the fact that there is another VLAN in the network. In this way, we ensure the security of user identity.

4. PERFORMANCE EVALUATION

Now we evaluate the security of the new secure strategy.

4. 1 Wi-Fi-Password Decryption Software

Not all the people can handle complex and advanced decryption technique, so Wi-Fi-password decryption software is the most common and widely used method. We design the new secure strategy in response to weaknesses of Wi-Fi-password protection. A Web Authentication with unshared key is added as a part in the network access authentication process. We adopt MD5 and HTTPS to protect the user passwords. It is different from the encryption techniques of Wi-Fi-password. Therefore, Wi-Fi-password decryption software will fail in the new security framework.

4. 2 Identity Theft

In the new security framework, the WLAN is divided into two VLANs. Communications between the two VLANs are forbidden. The hacker cannot get users' IP address and MAC address. So identity theft is useless.

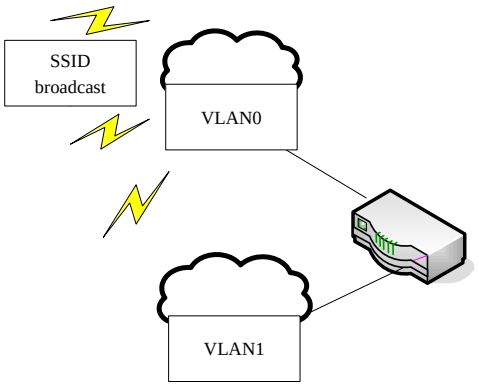

Figure 2. Wireless network with two VLANs

4. 3 The Eavesdropper Attack

After cracking Wi-Fi-password, the hacker listens in the authentication communication as an Eavesdropper (Fig.3). Based on the secure channel provided by HTTPS, most eavesdropping tools will be useless. However,

there are some infrequent attacks which are able to steal secure data from the connection. But what contain in the packet are a username and a 128-bit encrypted string. Besides, the string can be used only once, so the hacker will not succeed in accessing network by sending this message to the web server.

4. 4 The Man-In-The-Middle Attack

There are two authentication processes in the man-in-the-middle attack in fact (Fig.4).

If the hacker chooses this attack, he needs to construct a wireless network with the same name and the same Wi-Fi-password to attract valid users. But it is not enough, because users can verify whether the server certificate is trusted or not. The worst situation is that the hacker succeeds in faking a server certificate. It has been proven practical by Arjen Lenstra[7]. But because of the life time which has been set to indicate the valid time of a random string to a specific client, the hacker needs to accomplish the whole attack in quite limited time. We suppose that an authentication process needs T seconds. The attack will fail if the life time is set to be a value between T and 2T. In addition, it is not worth to choose this high-cost attack for a small-scale wireless network.

4. 5 The Brute Force Attack

If the hacker gets a valid username and keeps on trying different passwords, he will not succeed. Failing ten times continuously, he will be refused to login in an hour by the system.

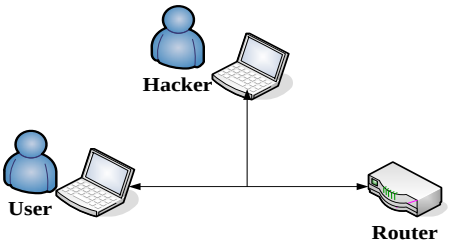

Figure 3. The eavesdropper attack

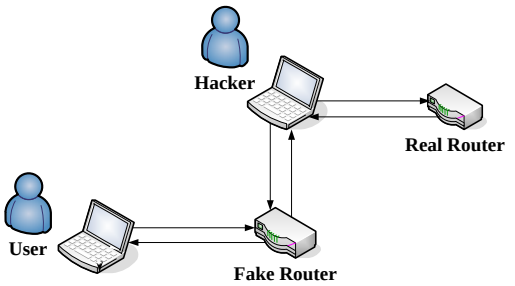

Figure 4. The man-in-the-middle attack

5. CONCLUSIONS

In this paper, we first introduce the secure issues of common secure strategies supported by most popular commercial wireless routers currently. Then we propose a new strategy for small-scale IEEE 802.11 wireless

local area network based on web authentication with unshared key and VLAN in the wireless network. Finally we evaluate the new strategy's security against practical attacks. Based on known knowledge and techniques, the new strategy can ensure the security of the small-scale wireless network. Moreover, it is simple, wieldy and low-cost.

References

[1] E. Tews, R.-P. Weinmann, and A. Pyshki, "Breaking 104—bit WEP in less than 60 seconds," WISA'07 Proceedings, Springer-Verlag Berlin, Heidelberg, pp. 188-202, 2007.
[2] E. Tews, M. Beck, "Practical attacks against WEP and WPA," WiSec '09 Proceedings, ACM New York, pp.79-86. 2009
[3] M. Beck, "Enhanced TKIP michael attacks", unpublished.
[4] Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu, "Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD," Crypto 2004, August, 2004, retrieved July 27, 2008, in press.
[5] Xiaoyun Wang and Hongbo Yu, "How to break MD5 and other hash functions," EUROCRYPT 2005 Proceedings, Springer-Verlag Berlin, Heidelberg, pp.19-35, 2005. Retrieved December 21, 2009.
[6] J. Black, M. Cochran, and T. Highland, "A study of the MD5 attacks: insights and improvements," FSE 2006 Proceedings, Springer-Verlag Berlin, Heidelberg, pp.262-277, March, 2006. Retrieved July 27, 2008.
[7] M. Stevens, A. Lenstra, and B. Weger, "Chosen-Prefix collisions for MD5 and colliding X.509 certificates for different identities", EUROCRYPT '07 Proceedings, Springer-Verlag Berlin, Heidelberg, pp.1-22, 2007.