I.J. Computer Network and Information Security, 2011, 2, 19-25
Published Online March 2011 in MECS (http://www.mecs-press.org/)

A New Secure Strategy in Small-Scale IEEE 802.11 Wireless Local Area Networks with Web Authentication and Virtual Local Area Network

Huiting Liu[1,2]
1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications
2. School of Computer, Beijing University of Posts and Telecommunications
Beijing, China
Email: liuwaiting@gmail.com

Hua Zhang[1], Weilin Xu[1,2], Yigang Yang[1,2],Mengyuan Xu[2]
1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications
2. School of Computer, Beijing University of Posts and Telecommunications
Beijing, China
Email: zhanghua_288@bupt.edu.cn

***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 purchase expensive network equipments to improve the network security. Therefore, the secure strategy for 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 describe our initial designs and 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, easy to use and price moderate. At last, we evaluate the performance of the new secure strategy and give our conclusions.**

***Index Terms*—wireless local area network (WLAN); secure strategy; web authentication; identify theft; virtual local area network (VLAN)**

I. INTRODUCTION

Wireless network brings great user experience owing to its flexibility, portability and low-cost. Commercial Wireless Local Area Network (WLAN) products are widely available on the market, most of which are easily setup and simply operated. WLAN is rapidly deployed around the world. An increasing number of public places, offices and even household families are setting up their own WLANs. As air is the media for wireless networks, they are inherently less secure than traditional wired networks. When sensitive information is transmitted over a wireless network, the privacy and integrity of it must be concerned. 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 adopted 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. Since most small-scale wireless network would not opt for this strategy, we focus on WEP and WPA-PSK.

WEP is the most widely used security algorithm for IEEE 802.11 wireless network. WEP uses the stream cipher Rivest Cipher 4 (RC4) for confidentiality, and the Cyclic Redundancy Check (CRC-32) checksum for integrity. In standard 64-bit WEP, each 802.11 packet is respectively encrypted by a 64-bit RC4 key which is composed of a 24-bit Initialization Vector and a 40-bit WEP key. WEP is intended to provide wireless network with a security scheme that is equivalent to a wired network. However, 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]. Therefore, WEP is deprecated as a security algorithm for IEEE 802.11 wireless networks.

WPA is proposed in response to several serious weaknesses in WEP. WPA-PSK is designed for home and small office networks. The Temporal Key Integrity Protocol (TKIP) is brought into WPA. WEP’s small 40-bit encryption key is replaced by TKIP encryption. TKIP is a 128-bit per-packet key which prevents collisions by generating a new key for each packet dynamically. Meanwhile, WPA also includes a Message Integrity Check, designed to prevent attackers from capturing, tampering with and/or resending data packets and it replaces the CRC which was used and implemented by the WEP standard. However, as the four-way handshake during the authentication is not protected in the WPA-PSK network, when users only rely on a weak passphrase, it would be vulnerable to password cracking attacks. As a matter of fact, a simple password is used as a pre-shared passphrase by the majority of people. In November 2008 Erik Tews and Martin Beck—researchers of two German technical universities (TU Dresden and TU Darmstadt)—uncovered a WPA weakness derived 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]. Thus, WPA is facing with a predicament at present.

Not only cryptanalysts and professional hackers can crack passwords of wireless network, but common computer users can also do it by certain decryption software such as Spoonwep and Spoonwpa in the famous hacker platform—Back Track 4 (Fig. 1) . The tutorials of decryption software are available and easily accessible on the Internet. As a matter of fact, a lot of people stole other people's network resources without paying owing to the existence of the WLAN decryption software.

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

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.

Figure 1. Back Track 4

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

Our new secure strategy enjoys 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. According to their own demands, users can replace the old strategies with our new secure strategy or add it as a part in the network security framework.

The rest of this paper is organized as follows. Section 2 introduces some relevant knowledge occurred in this paper. Section 3 briefly represents our initial designs. Section 4 illustrates our new secure strategy. Section 5 evaluates the security of the new secure strategy. Finally, Section 6 draws our conclusions.

II. Relevant Knowledge

A. Back Track

Back Track is a world leading penetration testing and hacker attacking platform. It is a portable and free-of-installation system based on Linux. It can be stored in a USB flash disk or CD. A large number of network security detecting tools and hacker cracking software have been installed inside the system. In its fourth generation, Back Track 4 (BT4), the Linux kernel has been updated to 2.6.29.4. The new kernel has cause great changes in the structure of Back Track. Of course, it becomes more powerful as well.

B. SpoonWEP/WPA

SpoonWEP/WPA is a powerful graphical user interface (GUI) software which can crack WEP and WPA keys. The tool has been included inside the Back Track 4 system which is often sold with the so-called "network-scrounging cards". "Network-scrounging cards" are special USB Wi-Fi adapters existing in Chinese market in recent years. They promise accessing Internet "for free" forever.

C. 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. HTTPS can create a secure channel over an insecure network, so HTTPS connections are often used to transact important information on the Internet. The trust inherent in HTTPS is based on certificate authorities. When a user visits a website through an HTTPS connection, the browser software would ask whether he or she trust the certificate provided by the website in the first place.

D. Message-Digest Algorithm 5

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]. A collision attack has been found which can find collisions within seconds on a computer with a 2.6GHz Pentium4 processor [7]. Furthermore, there is also a chosen-prefix collision attack that can produce a collision for two chosen arbitrarily different inputs within hours, using off-the-shelf computing hardware [8]. Thus MD5 is no longer suitable for applications such as digital signatures which rely on collision resistant. However, recovering the source value remains impossible, so in our application, we still chose MD5 to ensure the security of messages throughout a web authentication process. In order to strengthen the security, we use some methods to remedy the defects of MD5.

E. Identity Theft

In this paper, identity theft is narrowly defined as that happened in local area network. Network access system usually identifies client devices according to their IP addresses and MAC addresses. By thieving both IP and MAC address, the hacker can pretend to be a valid user to access the network and do whatever he or she wants to. As it is easy to get other computers' IP addresses and MAC addresses and most operation system allows users to modify their IP addresses and MAC addresses, identity theft pervades all local area network. It has caused great damage to global network and even economy.

F. 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. The transmission of messages in different VLANs is separate, namely, users in a VLAN cannot communicate with those in other VLAN directly. If users in different VLAN want to build up a communication, they need a router. In recent year, VLAN has been applied in wireless network. Wireless routers with VLAN are widely available on the market.

G. 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. Then, it 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 would not turn up in the network selecting list on client devices.

H. 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, as a matter of fact, the entire conversation is controlled by the attacker. The attacker can obtain secrets and privacies that he or she is interested in by analyzing the messages going between the two victims. The man-in-the-middle attack has been an important network attack for a long time. Moreover, there is still has a large space for its expansion nowadays. Tempted by economic interests, the man-in-the-middle attack has become the most dangerous and destructive attacks towards internet bank, online game and electronic commerce.

III. Initial Designs

In reality, most wireless networks in homes or small offices are protected by Wi-Fi-password and almost all WLAN decryption software available on the Internet aims at cracking the Wi-Fi-password. Based on the facts mentioned above, the main idea of our design is similar to WPA-Enterprise. We choose unshared keys to substitute shared keys, that is, every valid user has their own identity and password. But we do not want to add extra devices such as RADIUS server, so we set a mini server program inside the router and use an encrypt file to record users' data. Besides, every valid user's computer is required to install a client program. When a user wants to access in the network, he must correctly input his identity and password in the client program. These messages will be encrypted and sent to the server program. Then the server program will compare the encrypted message with the data in the user record. When the identity and password match, the user is allowed to access the network.

In order to prevent identity theft, the client program is required to keep running in the background when the user is using the network. The client program will exchange information with the server program at regular intervals to make sure that the computer accessing the network belongs to a valid user. If hacker changes his IP address and MAC address to pretend a valid user, he would be found when the server program send a message to his computer and cannot get any reply.

There are several shortcomings in the initial design. Firstly, every computer must install a client program before they can access the network. The operation is a little bit fussy. Secondly, software is not compatible with heterogeneous personal computer operation systems generally (e.g. the three most popular operation systems, Windows, Linux and Macintosh Operating System). Thirdly, the fact that the client program must keep running during the whole process brings bad experience to users. What's worse, because all client programs keep communicating with the server program, the router will be busy in dealing with the client information. The router's ability is limited. As a result, the network speed and the amount of users will be affected.

Our objective is that all users could enjoy a more safety network environment without any changes in their computer. Thus, all the changes should be done inside the router. We modify the design scheme. A web authentication is design to take place of the client program authentication. After a careful and thorough consideration, we get our current secure strategy based on web authentication and VLAN.

IV. A New Secure Strategy Based On Web Authentication With Unshared Key And Vlan In Wireless Network

A. Web Authentication with Unshared Key

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's 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 needs no additional equipments and is 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. 2.

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 would be recorded. Then a Success page would be sent to the Client and the Client is allowed to access the network. If the Client submits incorrect information, it would receive a Failure page.

Two steps are needed in the logoff process:

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 does not receive the MD5-Response from the Client in the life time, the random string becomes invalid. If the Client wants to continue the authentication process, it must send a new request to get a new random string.

In order to prevent the brute force attack, we set a password retry count to forbidden hackers from keeping trying different passwords. The password retry count can be modified by the administrator according to the security requirement. If the times that the Client submits incorrect information exceeds the password retry count, the client will be refused to login in an hour. If valid users forget their passwords, they can ask the administrator for help.

B. 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 easily get IP addresses and MAC addresses of valid users. 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—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.

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

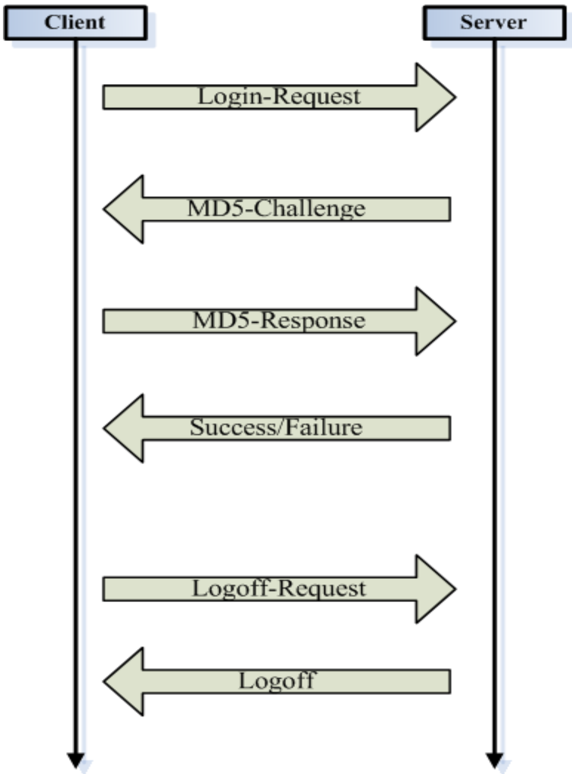

Figure 2. Web authentication

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. 3). 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 the correct username and password, it would 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 cannot send packets to valid users to get their IP addresses and MAC addresses, and he even cannot get the fact that there is another VLAN in the network. In this way, we ensure the security of user identity.

V. Performance Evaluation

Now we evaluate the security of the new secure strategy. Let's see whether the most popular attacks including Wi-Fi-password decryption software, identity theft, the brute force attack, the eavesdropper attack and the man-in-the-middle attack will work on the new security framework or not.

A. *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.

B. *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. He even cannot get the fact that there is another VLAN in the network. So identity theft is useless.

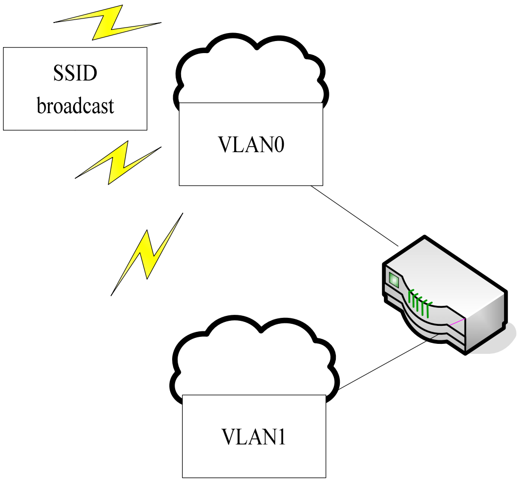

Figure 3. Wireless network with two VLANs

C. *The Brute Force Attack*

If the hacker gets a valid username and keeps on trying different passwords, he will not succeed. We have set a password retry count to prevent the brute force attack. For example, suppose the password contains five digits(0~9) and the password retry count is five, that is, if someone falsely enter five times continuously, he could not login in an hour.

Now we calculate the average time cost in cracking the password. Suppose we have N cases, the probability of enter i times to hit is P_i, the mathematical expectation of the enter count is E, the mathematical expectation of total need time is T and the password retry count is R.

For

$$P_1 = \frac{1}{N}, P_2 = (1-\frac{1}{N})*\frac{1}{N-1} = \frac{1}{N} ..., P_N = \frac{1}{N},$$

We have

$$P_i = \frac{1}{N}, i = 1,2,3\cdots N, \quad (1)$$

$$E = \sum_{i=1}^{N} i * P_i = \frac{1}{N}\sum_{i=1}^{N} i = \frac{N+1}{2}. \quad (2)$$

For

$$N = 10^5, P_i = \frac{1}{N}, i = 1,2,3\cdots N, R = 5,$$

According to (2), we have

$$\begin{aligned} E &= \frac{1}{10^5}(1+2+\cdots+10^5) \\ &= \frac{10^5+1}{2} \\ &= 50000.5 \end{aligned},$$

$$T = \frac{E}{R} = \frac{E}{5} = 10000.1 hours.$$

10000 hours is needed to crack the password of length five, as the length of secret increasing and the retry count decreasing, the cracking time would increase. The corresponding equation is shown in (3).

$$T = \frac{E}{R} = \frac{N+1}{2} * \frac{1}{R} = \frac{N+1}{2R} \quad (3)$$

The relationship between the cracking time and the length of password is shown in Fig. 4 (the password retry count is set to be 5). The relationship between the cracking time and the password retry count is shown in Fig. 5 (the length of the password is set to be 5).

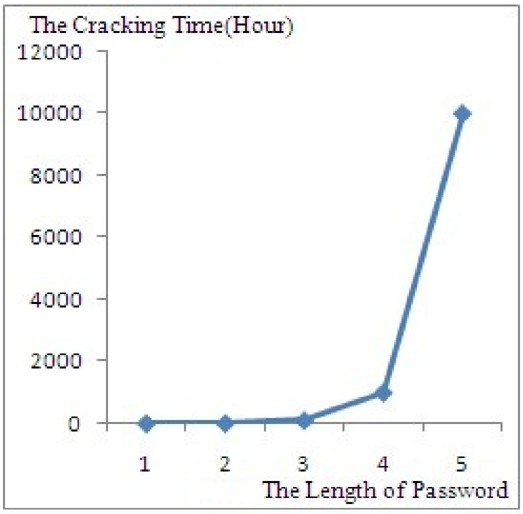

Figure 4. The relationship between the cracking time and the length of password

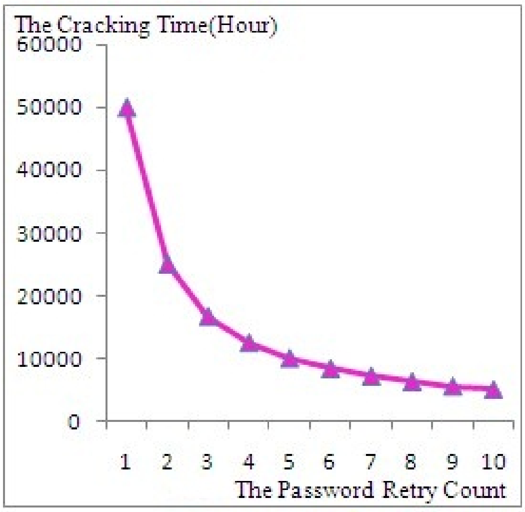

Figure 5. The relationship between the cracking time and the password retry count

If the passwords contain letters or symbols, the cracking difficulty will increase significantly. We suggest that users choose passwords equal or longer than five and the passwords should be made up of numbers, letters and symbols. Moreover, the password retry count is suggested to be set between 3 and 10. According to the suggestions, the brute force attack will take a long time to crack the web authentication. We think it is safe enough for a small-scale wireless network.

D. The Eavesdropper Attack

After cracking Wi-Fi-password, the hacker listens in the authentication communication as an Eavesdropper (Fig.6). 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.

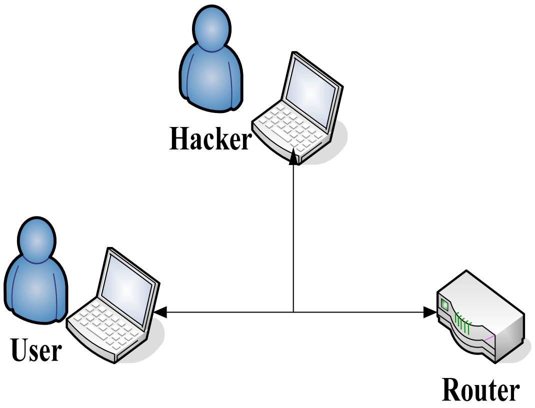

Figure 6. The eavesdropper attack

E. The Man-In-The-Middle Attack

There are two authentication processes in the man-in-the-middle attack in fact (Fig.7).

If the hacker chooses this attack, he needs to construct a wireless network with the same name and Wi-Fi-password to attract valid users. But it is still not enough. Users will receive a certificate provided by the web server when visiting the login page. 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[9]. 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 two authentication processes in the man-in-the-middle attack need 2T seconds at least. The attack would fail if the life time is set to be a value between T and 2T. In addition, it is not worthwhile to choose this high-cost attack for a small-scale wireless network.

VI. Conclusions

In this paper, we first introduce the secure issues of common secure strategies supported by most popular commercial wireless routers currently. Then we introduce some relevant knowledge. Then we describe our initial designs and 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 the already known knowledge and techniques, the new strategy can ensure the security of the small-scale wireless network. Moreover, it is simple, easy to use and price moderate.

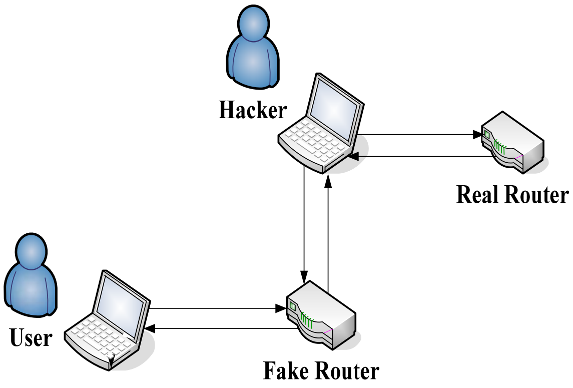

Figure 7. The man-in-the-middle attack

ACKNOWLEDGMENT

We wish to thank Lu Lu, Yi Sun, Yi Huang, Tianqi Tong, Wanqiong Pan. This work is supported by the Research Innovation Fund for College Students of Beijing University of Posts and Telecommunications (Grant No. 101104537). We would like to thank the anonymous reviewers for their perspicacious comments.

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. M. J. Stevens, “On collisions for MD5”, unpublished.
[8] M. Stevens, A. Lenstra, and B. Weger, “Chosen-prefix collisions for MD5 and Applications.”,unpublished.
[9] 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.

Huiting Liu is currently a B.S. student of School of Computer in Beijing University of Posts and telecommunications, Beijing, China.

His research interests include network security, Next Generation Internet and middlebox.

Hua Zhang received the M.S degree at Xidian University in 2005, and Ph.D degree in cryptography at Beijing University of Posts and Telecommunications in 2008.

Her research interests include cryptography, information security, Ad Hoc and Sensor Networks.

Weilin Xu is currently a B.S. student of School of Computer in Beijing University of Posts and telecommunications, Beijing, China.

His research interests include network security, Next Generation Internet, middlebox and content security.

Yigang Yang is currently a B.S. student of School of Computer in Beijing University of Posts and telecommunications, Beijing, China.

His research interests include Next Generation Internet and middlebox.

Mengyuan Xu is currently a B.S. student of School of Computer in Beijing University of Posts and telecommunications, Beijing, China.

Her research interests include data structure, computer algorithm and computer programming.