An Authentication Scheme with Anonymity for Wireless Environments

Sherif Abu Al-Khair[1]

ABSTRACT

Transferring data is the most important goal in our life. Because our life is built on sharing data, sending and receiving information between people. Most of these data are confidential, so we should safe it from any body that doesn't have permission to get it. When talking about saving data, we mean the security methods. We find that the security methods contain many encryption and decryption algorithms. So, this documentation focused on how to increase the complexity of the encryption method. In a paper recently published in the IEEE Transactions on Consumer Electronics, Zhu and Ma proposed a new authentication scheme with anonymity for wireless environments. However, this paper shows the improvements of Zhu-Ma scheme in security field. By using different keys in complex hash (i.e. MD4, MD5, and SHA1) function and the keys periodically are changed depending on the time. We note that it is difficult to obtain both the keys and original data.

I. INTRODUCTION

Wireless communications offer organizations and users many benefits such as portability, flexibility, increased productivity and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access.

Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders [1]. We should know the difference between Authentication, Authorization and Least Privilege concepts. Authentication is the process of something or someone. Authentication usually involves a user name and a password, but can include any method of demonstrating identity, such as a smart card, a retinal scan, voice recognition, or a fingerprint. Authorization is the process of determining whether an identified user or process is permitted access to a resource and what the appropriate level of access is for that user. Least privilege is the process of least privilege states that you should provide users with the necessary level of privilege to perform their jobs and no more [2]. In this paper we will deal with authentication process, because it is too famous and can cause many dangerous problems in wireless

[1]Ayman EL-SAYED (IEEE Member), Hamdy kelash and magdy kotb, Computer Eng. and science Department Faculty of Electronic Eng., Menofiya University

environments. Also we will focus on how we can improve the security of data transfer between any two points or between the client and server. Finally we will discuss our experimental work and show the advantages and disadvantages of our scheme [3, 4].

II. Zhu-Ma Scheme

Zhu-Ma scheme is one of the most important schemes which dealing with security in wireless environment. In wireless mobile communication system, user anonymity and user authentication have been addressed. The advantage of Zhu-Ma scheme authenticating mobile user's protocol is simple and efficient [5]. The security of the proposed scheme relies on the two assumptions: tamper-proof devices and the security of the one-way scheme. Zhu-Ma scheme is based on the public key cryptosystems, but mobile users only do symmetric encryption and decryption [6]. In Zhu-Ma protocol, it takes only one round of message exchange between the mobile user and the visited network, and one round of message exchange between the visited network and the corresponding home network. The most significant feature is one-time use of key between mobile user and visited network [7, 8].

Zhu-Ma scheme Model: In wireless environments, MN indicates (mobile user), HA indicated (home agent) of a mobile user MN, and FA indicates (foreign agent) of the network that a mobile MN wants to visit. A simplified model is shown in Figure (1), in which f indicates a (fixed node), HA and FA indicate a mobile agent, respectively, R indicates a (router). In our protocol, MN wants to directly communicate with FA. FA is responsible for authenticating MN by HA [9].

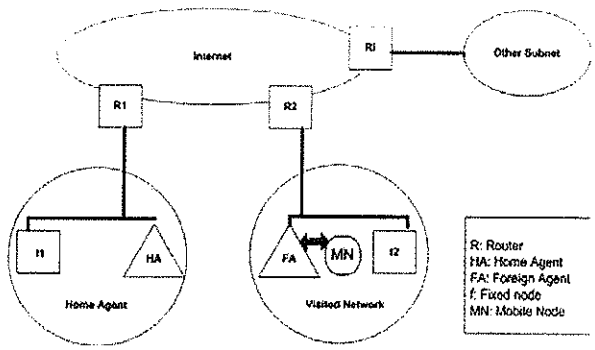

Figure (1). The model of wireless environments

Consider the security goals that may be achieved after the successful run of the wireless authentication protocol. They include the following:

- Mutual authentication of mobile user and visited network
- Mutual agreement of shared secret key
- Mutual implicit key authentication
- Assurance of session key freshness
- Non-repudiation of origin for relevant user data
- Confidentiality of relevant data
- User anonymity as a data and destination

As well as these requirements, another factor in design of authentication protocol for the wireless environment is the limited resource of the mobile devices [10].

The security features for mobile communication system include: confidentiality on the air interface, anonymity of the user and, most importantly, authentication of the user to the network in order to prevent fraudulent use of the system.

For the lack of a physical association between the mobile nodes (MNs) and the wired network and easy access to the radio, proper authentication is necessary to protect the communication against illegal usage and to ensure that users are connected to the network that he trusts. To

provide universal wireless access to services, such authentication must deal with users' roaming among areas administered by different network operators (NOs), and be implemented by users' devices with limited computing resources. During the authentication process, some secret information must be mutually agreed upon so the following communication can proceed efficiently in protected mode to achieve desired confidentiality [11, 12].

Zhu and Ma's scheme has some security weaknesses. Therefore, they made a slight modification to their scheme to improve their shortcomings.

These weaknesses are :

1) It cannot achieve perfect backward secrecy.

2) It cannot achieve mutual authentication.

3) It cannot protect against a forgery attack.

After the modification which they made, the scheme was been more powerful. But we found that we can use the basic principal of the Zhu-Ma scheme and adding some modifications to increase its security and powerful [13, 14].

Now we will discuss our new scheme and our modifications to show how we can improve Zhu-Ma scheme.

Our protocol is similar as Zhu-Ma scheme protocol. But we improve it to be more secure than Zhu-Ma scheme. Also it can be used with LAN and WAN connection.

In our protocol we improve the security by two ways: First, we encrypt the data by using three types of hashing function algorithms. These types are MD4, MD5 and SHA1. So if we want to encrypt any data like password, the password will encrypt by MD4 algorithm. The result of MD4 will be encrypted by MD5 algorithm. The result of MD5 will be encrypted by SHA1 [15].

III. Our improvements of Zhu-Ma Scheme

Our protocol is similar as Zhu-Ma scheme protocol. But we improve it to be more secure than Zhu-Ma scheme. Also it can be used with LAN and WAN connection.

In our protocol we improve the security by two ways: First, we encrypt the data by using three types of hashing function algorithms. These types are MD4, MD5 and SHA1. So if we want to encrypt any data like password, the password will encrypt by MD4 algorithm. The result of MD4 will be encrypted by MD5 algorithm. The result of MD5 will be encrypted by SHA1 [16, 17].

The result of SHA1 will be our result. We make this sequence to prevent any hacker to obtain the original data.

If there is any hacker (man in the middle) that success to obtain the hashed data and the key of SHA1. So the result which he will get, will not be the original data, because the hacker should have the original keys of MD4, MD5 and SHA1. And it will be very difficult process. Also he should decrypt the data in the same sequence of encryption.

Second, we want to increase the encryption and the difficulty of decryption. So we improve our protocol to change the keys each hour. So it will be found that each hour the key which we use to encrypt the data will be changed. This change depends on the time of servers. But not depends on client time. Because we know that the time is different between each country. So we can't fix the key. To solve this problem we make our protocol to change its keys depending on GRENETCH time, because GRENETCH time is fixing in all PC's on all over the world. So any user in any location can contact with his servers by using our protocol without any problems and get all its benefits.

By using the previous method we will find that we have 24 database tables which we save the encrypted data by each key to obtain 24 encrypted data for the same original data. So, if a user encrypt his password at 2 clock and submit it to the server which using our algorithm, the server will search in the database of current time. Because we suppose that the user should encrypt and send the data and the server decrypts the data in the same hour.

But when we apply this system, we found that there are a delay time which begins from starting to encrypt the data and finishing when the server receives the data. So, assume there is a user who start to encrypt his password at 2:59:59:90 Pm as shown in Figure (2) so, in this case the server should decrypt this data by using the key of 2 clock. But we find that the server receive the data at 3:00:00:60 Pm so, the server will decrypt that data by using the key of 3 clock. In this case the sever will not find the original data and reply that this user is not authorized. On the other hand when the same user encrypt the same data again at 3:01:00:00 Pm and submit it to the server, the server will decrypt it and find the original data in the table of encryption by the key of 3 clock.

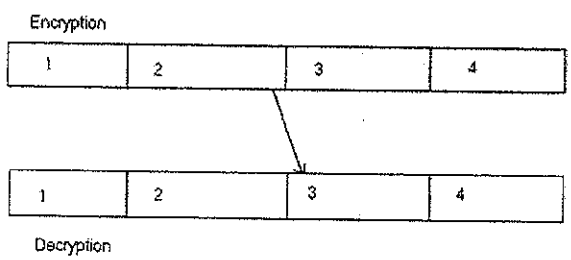

Figure (2): Different keys on both sides problem

To solve the previous problem, we put a time stamp with the encrypted packet to mark the time of encryption process. Also the server will have two database tables opened in the same time which include the database of this time key and the previous time key. So, when the server receives the data, it will search about the time stamp to know which database it will use to decrypt this data. By using this solution we will overcome the previous problem.

Some body can ask why we don't let all databases be opened and let the server to search in all that databases. The answer will be that if we open all databases and any hacker catch any encrypted or decrypted data he can use it in any time. But in case which we close unused databases, this hacker can't use this data only in the same time which is encrypted in it. And by the way it is difficult to know the time which this data is encrypted in it. Also if we open all databases this will be an overload on the server to search in all these databases.

IV. Comparison between Zhu-Ma scheme and our scheme

Now we will compare between Zhu-Ma scheme as shown in Figure (3) and our scheme as shown in Figure (4) by using the block diagram [18, 19]:

A) Zhu-Ma scheme :

As shown in Figure (3) the features of Zhu-Ma scheme are:

1- Zhu-Ma scheme uses one fixed key only in each session, so if the session was opened for 10 hours, the scheme will encrypt any data by the same key.

2- Zhu-Ma scheme uses only one encryption method like MD4, MD5 or SHA1 to encrypt the data.

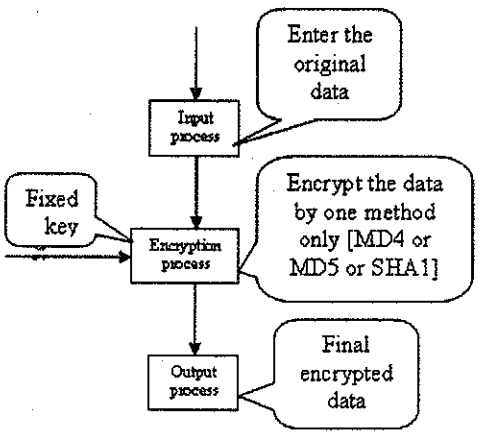

Figure (3): Zhu-Ma scheme.

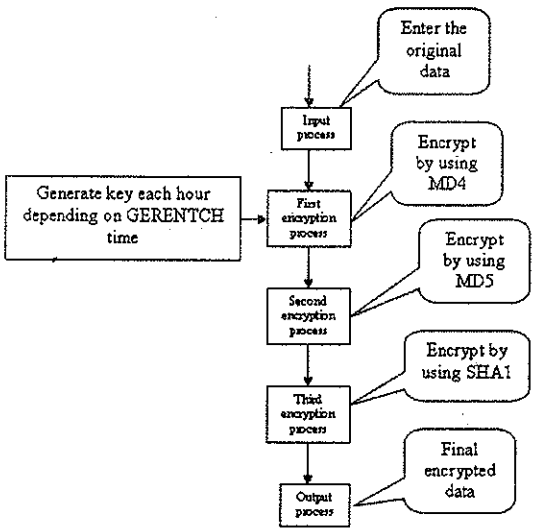

Figure 4: Our proposed scheme

between our scheme and Zhu-Ma scheme. These features are:

1- Our scheme change the key each hour, so our scheme can use 24 encryption key for the same data and the original data will have 24 different encrypted result.

2- Our scheme uses three encryption methods to encrypt the data. As we can see the original data should be encrypted by using MD4 method in the first process, then it is encrypted by using MD5 method, finally it is encrypted by using SHA1 method. After all the previous methods we can get the encrypted data.

V. Performance Evaluation of our proposed scheme

Now we will discus the performance of our proposed scheme to show the efficient of our improvements.

Table 1: Performance evaluation of our proposed scheme

	Zhu-Ma scheme	Our proposed scheme
No. of hash algorithm	1	3
Using with LAN and WAN	WAN only	LAN and WAN
Changing key	Each session	Each an hour
Using symmetric encryption	Yes	Yes
No.of round of message exchange	One	One
Loading on hardware	Medium	High
Security	Medium	High

From table (1) we can make a comparison between Zhu-Ma scheme and our proposed scheme, and find that Zhu-Ma scheme change the key in each session, so if the session opened three hours, we find that it uses the same key. But in our scheme the key will change each hour. Each Zhu-Ma scheme and our scheme are using symmetric encryption. Because each of them using hash function to encrypt the data at the client and using data bases at the servers to decrypt that data. Each scheme is using one round of message exchange to make the authentication. Zhu-Ma is less than our proposed scheme in hardware loading. But on the other hand we can find that our proposed scheme is more secure than Zhu-Ma scheme. Because we use three types of algorithms in hash function, also the key is changing each hour.

V. Conclusion

ZHU-MA scheme is not strong enough against some security weakness. So, this paper shows the improvements

of Zhu-Ma scheme in security field. We find that our proposed scheme is similar as Zhu-Ma scheme. And we built our proposed scheme on the main principles of Zhu-Ma scheme. So we use all Zhu-Ma scheme benefits. Also we made some improvements on Zhu-Ma scheme to make our proposed scheme more secure than Zhu-Ma scheme. Also to come over all Zhu-MA scheme security problems. By comparing between our proposed scheme and Zhu-Ma scheme, we find that Zhu-Ma scheme is easier and less overload in hardware than our proposed scheme. But our proposed scheme is more secure than Zhu-Ma scheme and can be used in LAN and WAN.

REFERENCES :

[1] Tom Karygiannis and Les Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices", Recommendations of the National Institute of Standards and Technology. (November 2002).

[2] Fu, X., Graham, B., Bettati, R., Zhao, W.: Active Traffic Analysis Attacks and Countermeasures. In: Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing. (2003)

[3] Fu, X., Graham, B., Bettati, R., Zhao, W.: Analytical and Empirical Analysis of Countermeasures to Traffic Analysis Attacks. In: Proceedings of the 2003 International Conference on Parallel Processing. (2003)

[4] Wright, M., Adler, M., Levine, B.N., Shields, C.: Defending Anonymous Communication Against Passive Logging Attacks. In: Proceedings of the IEEE Symposium on Security and Privacy (Oakland). (2003) 28–41

[5] IBM Redbooks (http://www.ibm.com/redbooks:IBM form: GG24-3376,ISBN: 013067101 TCP/IP tutorial and technical overview.

[6] Levine, B.N., Reiter, M., Wang, C., Wright, M.: Stopping Timing Attacks in Low-Latency Mix-Based Systems. In: Proceedings of Financial Cryptography (FC).(2004)

[7] Hintz, A.: Fingerprinting websites using traffic analysis. In: Proceedings of Privacy Enhancing Technologies workshop (PET 2002), Springer-Verlag, LNCS 2482 (2002)

[8] Jianming Zhu and Jianfeng Ma, Member, IEEE. "A New Authentication Scheme with Anonymity for Wireless Environments", IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, February 2004.

[9] Sun, Q., Simon, D.R., Wang, Y.M., Russell, W., Padmanabhan, V., Qiu, L.: Statistical identification of encrypted web browsing traffic. In: Proceedings of the IEEE Security and Privacy Conference. (2003)

[10] Raymond, J.F.: Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems. In: Proceedings of the International Workshop on Design Issues in Anonymity and Unobservability. Volume 2009. (2001) 10–29

[11] Cheng-Chi Lee, Min-Shiang Hwang, Member, IEEE, and I-En Liao, Member, IEEE "Security Enhancement on a New Authentication Scheme With Anonymity for Wireless Environments", IEEE Transactions on Industrial Electronics, Vol. 53, No. 5, October 2006.

[12] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: The insecurity of 802.11. In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking - Mobicom'01, pages 180-189, July 2001.

[13] D. B. Faria and D. R. Cheriton. DoS and Authentication in Wireless Public Access Networks. In Proceedings of the First ACM Workshop on Wireless Security (WiSe'02), pages 47-56, Sept. 2002.

[14] C.W. Chen, M.-C. Chuang, and C.-S. Tsai, "An efficient authentication scheme between MANET and WLAN based onmobile IPv6," *Int. J. Netw. Secur.*, vol. 1, no. 1, pp. 12–19, 2005.

[15] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: The insecurity of 802.11. In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking - Mobicom'01, pages 180-189, July 2001.

[16] D. B. Faria and D. R. Cheriton. DoS and Authentication in Wireless Public Access Networks. In Proceedings of the First ACM Workshop on Wireless Security (WiSe'02), pages 47-56, Sept. 2002.

[17] C.-Y. Yang, C.-C. Lee, and S.-Y. Hsiao, "Man-in-the-middle attack on the authentication of the user from the remote autonomous object," *Int. J.Netw. Secur.*, vol. 1, no. 1, pp. 22–24, 2005.

[18] S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the key scheduling algorithm of RC4. In Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

[19] A. Stubblefield, J. Ioannidis, and A. D. Rubin. Using the Fluhrer, Mantin, and Shamir attack to break WEP. Technical Report TD-4ZCPZZ, AT&T Labs Research, Aug. 2001.