INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 5 (2018) PAGES 4026 - 4030
RECEIVED : 21.09.2018 PUBLISHED : 22.10.2018
Oct 22, 2018

SECURE AUTHENTICATION SCHEME USING DUAL CHANNEL IN ROUGE ACCESS POINT ENVIRONMENTS

P.Suba[1], M.Mailsamy[2]

[1]Research Scholar, Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tiruchengode, India.

[2]Assistant Professor, Computer Science and Engineering, Vivekananda College of Engineering for Women, Tiruchengode, India.

Abstract:

Authentication plays a critical role in securing any online banking system, and many banks and various services have long relied on username/password combos to verify users. Memorizing usernames and passwords for a lot of accounts becomes a cumbersome and inefficient task. Furthermore, legacy authentication methods have failed over and over, and they are not immune against a wide variety of attacks that can be launched against users, networks, or authentication servers. Over the years, data breach reports emphasize that attackers have created numerous high-tech techniques to steal users' credentials, which can pose a serious threat.

Keywords: Critical, Banking system, Batch reports.

1. INTRODUCTION

Traditional authentication schemes such as the username/password combo pose a serious threat to the online banking services, financial systems, and their users. Most current authentication systems assign or allow a user to choose a static and unique user id that acts as a label. This static label is typically attached to the user for a long time. Unfortunately, users tend to use the same user id in many different websites and systems. Furthermore, many users continue to employ the same password across online accounts and systems. According to a recent study, 51% of the surveyed users reuse the same password across different websites, and more than 77% of the participants either slightly change or reuse existing passwords with simple tricks. The technique benefits from the widespread usage of ubiquitous computing and various intelligent portable and wearable devices that can enable users to execute a secure authentication protocol. Our proposed scheme does not require an authentication server to maintain static username and password tables for identifying and verifying the legitimacy of the login users. It not only is secure against password related attacks, but also can resist replay attacks, shoulder surfing attacks, phishing attacks, and data breach incidents. In 1981, Lamport [1] first proposed a remote authentication scheme which provides authentication procedures between the remote user and server over an insecure channel. However, Lamport's scheme needs to store password table, the password table makes Lamport's scheme vulnerable to a stolen-verifier attack. In 1998, Jan and Chen [2] proposed a password based authentication scheme without password table stored in the system. Later, in 2000, Hwang and Li [3] proposed a novel remote user authentication scheme using smart card based ElGamal's [4] public key cryptosystem. By using smart cards, there are several advantages and properties due to its temper-resistance merit, i.e., such a smart card

based scheme helps a legal user with his unique identity or password to login to the remote server by using the smart card, since illegal users cannot get legal one's information via even insecure channel; the remote server in smart card based system does not have to keep a password table in its database. Thus, the well-known stolen verifier attack can be resisted. As far as we concerned, there are two categories of the traditional remote user authentication scheme [5-9], including the password based scheme and the cryptographic.

2. RELATED WORK

The password dictionary attack, and cryptographic keys based scheme must provide specific memorize to store the corresponding keys so that it is too expensive to maintain the keys in the system. Moreover, the two categories cannot provide non-repudiation since both passwords and cryptographic keys are easily forgotten, lost and no way to identity who the actual user is. Currently, the new technology of biometrics is becoming a popular method for engineers to design a more secure cryptosystem. In terms of physiological and behavioral human characteristics, biometrics is used as a form of identity access management and access control, and it services to identify individuals in groups that are under surveillance. With the development of computer technology, people's biometrics information, such as fingerprints, faces, irises, hand geometry, and palmprints can be used to convince their identities. Furthermore, our purpose of system design is to make scheme can be applied for deferent network environments such as wireless system, Wi-Fi, WiMAX, Mobile networks, and vehicle system. Wi-Fi is an advanced technology that allows devices to exchange data wirelessly over a computer network, including high-speed Internet connections. Wi-Fi Alliance defines Wi-Fi as any wireless local area network (WLAN) products that are based on the IEEE 802.11 standards. WiMAX is another brand used to upon wireless MANs and is based on IEEE 802.16d/802.16e. The remainder of this paper is organized as follows. Section 2 shows the proposed scheme step by step. In Section 3, we provide the relevant security analysis to prove that our scheme is actually secure for applications. In this section, we present how secure of the proposed scheme with our professional security analysis. As aforementioned designed using strategy of quadratic residues, exclusive-or operation and one-way hash function, which can withstand the possible well-known attacks. We can provide the detailed proof as follows. An attacker, named Eve, intercepts the communication messages from the legal user, and attempts to cheat the server by sending the intercepted messages. Proof: In the proposed scheme, we use the nonce-based mechanism and hash value comparisons of M and N to protect against the reply attacks. More specifically, the random numbers t and s are independently selected, and each of them is different in every session. Therefore, Eve cannot pass the authentication procedures, even if he intercepts the communication messages. It is clear that the proposed scheme can resist the reply attack.

3. PROPOSED SYSTEM

An attacker Eve gets the master key of the mechanism for some reasons, he attempts to compromise the previous session keys. Proof: We assume that Eve gets the master key x in our scheme, and he wants to compromise the previously generated session keys. However, he will fail. The reason is Eve cannot compute any past versions of session keys without knowing the randomly changed numbers r , s, andt
Therefore, the proposed scheme can protect the forward secrecy. In this section, we provide the performance analysis to show how efficiency of our proposed scheme. More specifically, we compare our security mechanism with the previous published schemes [10-12] based on the computational cost

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 5 (2018) PAGES 4026 - 4030
RECEIVED : 21.09.2018 PUBLISHED : 22.10.2018
Oct 22, 2018

associated with one-way hash function (hash) and modular squaring (squ). From the view of efficiency aspect [13],[14], an example of the cheap modular squaring 2 () f x x an □□ where a is a coefficient [13] can replace the original equation 2 ( ) mod f x x n □ .

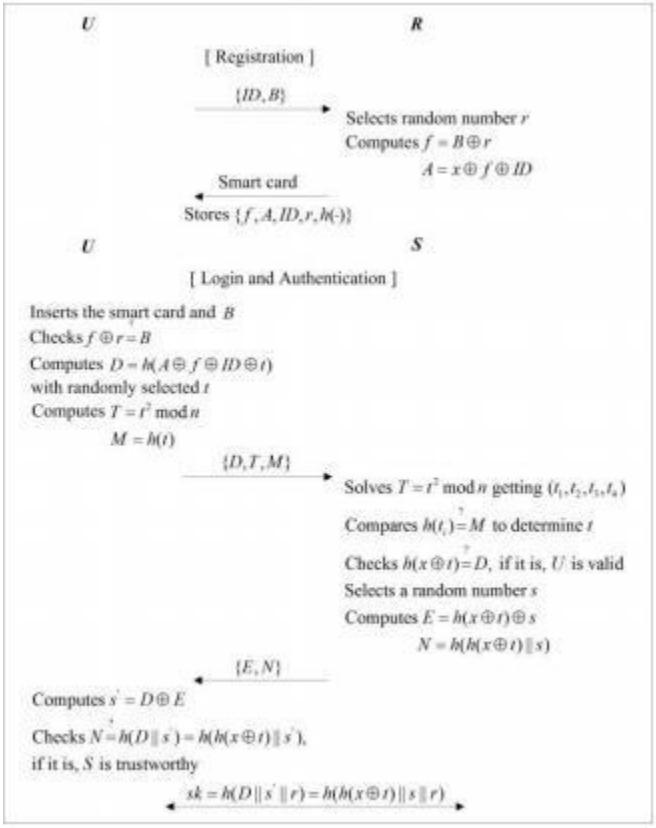

Fig.1.Proposed system

Therefore, the modular squaring is cheaper than the hash function such as MD5 (16 K gates) and SHA- 1 (20 K gates), since it costs only a few hundred gates. The detailed comparison is shown in Table 1. It is obvious that Khan et al.'s scheme [10] utilizes nine one-way hash functions is cheaper than Li and Hwang' scheme [11] and Li et al.'s scheme [12], cost ten one-way hash functions and fifteen one-way hash functions, respectively. In our system, we just need six one-way hash functions and two modular squaring. Hence, our proposed scheme is more practical with the biometric technologies, and our design is proved to be more efficient than others.

4. ANALYSIS

In the proposed scheme, we use the nonce-based mechanism and hash value comparisons of M and N to protect against the reply attacks. More specifically, the random numbers t and s are independently selected, and each of them is different in every session. Therefore, Eve cannot pass the authentication procedures, even if he intercepts the communication messages. It is clear that the proposed scheme can resist the reply attack. Assume a legal user U , who actually losses his or her smart card. Meanwhile, an attacker Eve who gets the smart card tries to pass the login phase in the proposed scheme. First, Eve inserts

the smart card and provides his The detailed comparison is shown in Table 1. It is obvious that Khan et al.'s scheme [10] utilizes nine one-way hash functions is cheaper than Li and Hwang' scheme [11] and Li et al.'s scheme [12], cost ten one-way hash functions and fifteen one-way hash functions, respectively. In our system, we just need six one-way hash functions and two modular squaring. Hence, our proposed scheme is more practical with the biometric technologies, and our design is proved to be more efficient than others. Furthermore, our purpose of system design is to make scheme can be applied for deferent network environments such as wireless system, Wi-Fi, WiMAX, Mobile networks, and vehicle system. Wi-Fi is an advanced technology that allows devices to exchange data wirelessly over a computer network, including high-speed Internet connections. Wi-Fi Alliance defines Wi-Fi as any wireless local area network (WLAN) products that are based on the IEEE 802.11 standards. WiMAX is another brand used to upon wireless MANs and is based on IEEE 802.16d/802.16e.

CONCLUSION

In this paper, we propose a novel biometric-based user authentication scheme, which does not need the traditional password anymore, it helps the user can prove his or her identity with the relevant biometrics. And, we design the proposed scheme by using the strategy of quadratic residues. This advantage is that the performance of our system is much cheaper than the hash based system since the implementation of such a modular squaring can be reduced to a few hundred gate-equivalents [14]. In addition, we present that our scheme can withstand to some possible attacks in Section 3. Therefore, the proposed scheme is actually secure, efficient and practical for real network applications such as wireless environment, Wi-Fi, WiMAX, mobile system, and vehicle network. In the future, we will design and adapt our scheme to implement on more network environments.

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1993.

[2] J. K. Jan and Y. Y. Chen, "Paramita wisdom password authentication scheme without verification tables," The Journal of Systems and Software, vol. 42, no. 1, pp. 45-57, 1998.

[3] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards,"IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp. 28-30, 2000.

[4] T. ElGamal, "A public-key cryptosystem and a signature schemebased on discrete logarithms", IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, 1985.

[5] A. K. Awasthi and S. Lal, "An enhanced remote user authentication scheme using smartcards," IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 583-586, 2004.

[6] N. Y. Lee and Y. C. Chiu, "Improved remote authentication scheme with smart card,"Computer Standards & Interfaces, vol. 27, no. 2, pp. 177-180, 2005.

[7] C. C. Chang and J. S. Lee, "An efficient and secure remote authentication scheme using smart cards,"Information & Security, vol. 18, pp. 122-133, 2006.

[8] J. Xu, W. T. Zhu, and D. G. Feng, "An improved smart card based password authentication scheme with provable security," Computer Standards & Interfaces,vol. 31, no. 4, pp. 723-728, 2009.

[9] R. Song, "Advanced smart card based password authentication protocol,"Computer Standards & Interfaces, vol. 32, no. 5-6, pp. 321-325, 2010.

[10] M. K. Khan, J. Zhang, and X. Wang, "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices," Chaos, Solitons and Fractals, vol. 35, no. 3, pp. 519-524, 2008.