Secure and Lightweight Remote Medical System

Yining Liu[1,2], Yuanjian Zhou[1], Youliang Tian[2], Mingzhe Liu[3], Yanbin Zheng[1,4]

[1] Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, China
[2] Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University, China
[3] School of Network Security, Chengdu University of Technology, China
[4] School of Computer Science and Network Security, Dongguan University of Technology, China
ynliu@guet.edu.cn, zhouyuanjian2017@gmail.com, youliangtian@163.com, liumz@cdut.edu.cn, zhengyanbin@guet.edu.cn

Abstract

The remote medical system helping the doctor in one city to diagnose the patient in another city improves the health-care quality greatly, and reduces the medical cost significantly. However, the security issue must be paid enough attention, for example, the unregistered devices may be illegally connected to the system, and the unauthorized doctor may access the system, therefore, the authentication is necessary to address these security problems. In this paper, a practical remote medical system is presented using multi-factor authentication and group key distribution technique. Compared with the previous literatures, the system burden is greatly reduced. Specifically, when a doctor needs to invoke the remote medical devices, he firstly calls the server. After the doctor is authenticated by the server, the server constructs a communication group including itself, the doctor, and the invoked devices using Shamir's secret sharing, which is proved to be more secure and efficient for the practical environment. Moreover, the proposed scheme can resist the impersonation attacks, the password guessing attacks, the eavesdropping attacks, etc.

Keywords: Remote medical system, Multi-factor authentication, Secret sharing, Group communication

1 Introduction

With the popularization of Internet, the remote medical system (RMS) is significantly developed nowadays, which has realized many functions such as remote monitoring, remote diagnosis, remote surgery, et al. For example, when a patient in city A wants the doctor in city B to diagnose, the doctor invokes the medical device near the patient to obtain the patient's current status, and gives more real-time and accurately medical advice. Moreover, the remote medical system collects the patient's health data with the help of Internet of things (IoT), which is very useful for the chronic disease.

The data collected and transmitted in RMS contains the privacy information. The security issue must be addressed since the information leakage may deduce the serious result. Therefore, many schemes [1-7] have been presented using the cryptography techniques such as hash function, AES, RSA, chaotic maps, elliptic curve cryptography, etc.

Khan et al. [8] proposed an authentication protocol to achieve the privacy using an anonymous identity. Moreover, Khan's scheme bounded the session key with the timestamp to resist against the replay attack, which is analyzed respectively by Chen et al. [9] and Jiang et al. [10]. Thus, Khan's scheme is improved to resist the insider attack. Specifically, Chen et al.'s scheme hid the doctor's real identity using a random number, and Jiang et al. [10] proposed an authentication scheme to allow the doctor to update his temporary identification. However, Kumari et al. [11] analyzed Jiang et al.'s scheme and achieved the anonymity and the untraceability. But the scheme in [11] failed to resist against the impersonation attack, the guessing attack and the DoS attack.

In recent years, more and more sensors are used in RMS. Due to its limited resource such as the battery capacity and the computing power, the traditional authentication is not suitable for Internet of Things (IoT). A variety of lightweight authentication protocols are proposed to satisfy the environment of RMS. Zhao et al. [12] presented an authentication scheme for IoT using secure hash algorithm and ECC to achieve the mutual authentication, low computation and communication cost. Sun et al. [13] proposed an authenticated group key agreement for mobile environment among participants who want to construct a group key using certificate-less public key cryptography, which is similar to ID-based cryptosystem. Mahalle et al. [14] proposed a group authentication in IoT for all devices taking part in the communication. Porambage et al. [15] proposed an authentication scheme in the distributed IoT applications environments. Hou and Yeh [16] proposed an authentication scheme for IoT based health-care

*Corresponding Author: Yanbin Zheng; E-mail: zhengyanbin@guet.edu.cn
DOI: 10.3966/160792642019012001016

systems and proved it using the formal proof.

There are still some problems in the above authentication protocols. Very recently, Park and Park [17] proposed a selective group authentication scheme using the threshold technique, in which there are two registries, Total Authority (TA), Region Authority (RA). However, YoHan et al.'s protocol has the following weakness: it cannot resist against the impersonation devices attacks and the password guessing attacks, moreover, the RA may increase the communication cost and the trust bottleneck.

The rest of the paper is organized as follows. In Section 2, the necessary knowledge is described. In Section 3, the communication model, and the threat model, and design goals are presented. YoHan et al.'s scheme is reviewed and analyzed in Section4. Our scheme is presented in Section 5, and is analyzed in Section 6. Finally, this paper is concluded in Section 7. The formal proof of the scheme is presented in section "Appendix".

2 Preliminaries

The following cryptographic concept is necessary in this paper.

2.1 Multi-factor Authentication

Identity authentication [18] is an important way to guarantee the information system security in a distributed network environment. In the earlier stage, it is mostly based on a single factor knowledge such as the password. However, the password-based single factor authentication scheme has been proved to be easily cracked, therefore, in order to improve the security and the practicality, the password and biometric technology are combined, which is named as multi-factor authentication [19].

In addition, the biometric feature is unique, easily extracting, and anti-theft [20]. Traditional biometric authentication is simple by matching the hash value of the input biometrics and the stored value of templates. In fact, the input of the biometric template participates is usually with the noise, which affects the matching effect. Therefore, the newly advanced template protection techniques may provide the possible solution. Next, a fuzzy extractor using the template protection techniques is introduced.

The fuzzy extractor consists of the following two algorithms [21].

$Gen(B)$: Probabilistic algorithm that takes biometric B as input and returns an extracted random string σ and an auxiliary string θ.

$\mathrm{Re}p(B^*, \theta)$: Deterministic reproduction algorithm that takes a fresh element B^* and a bit string θ as input, if B^* is close to B (e.g. $dis(B, B^*) \leq d$, where d is the predefined acceptable distance), then returns σ. For simplicity, the biometric parameters in the article are denoted by the symbol B.

2.2 Shamir's Secret Sharing

Shamir's secret sharing is based on a Lagrange interpolation polynomial over a finite field F_p, where p is a prime number [22]. Suppose there are n shareholders $U_1, ..., U_n$, and a trusted dealer D, in which D divides the secret data s into n shares $y_i (1 \leq i \leq n)$ that is sent to $U_i (1 \leq i \leq n)$ securely. When at least l shares collaborate, the secret data s can be recovered, otherwise, nothing about s is obtained. The protocol consists of two algorithms:

(1) Share generation algorithm:

D chooses $(l\text{-}1)$ numbers randomly, and generates a polynomial $f(x) = a_0 + a_1 x + ... + a_{l-1} x^{l-1}$, in which the secret $s = a_0 = f(0)$.

D computes $y_i = f(x_i),\ (1 \leq i \leq n)$, and distributes y_i to U_i privately, $(i = 1, ...,\ n)$.

(2) Secret reconstruction algorithm:

When there are l shares from n shareholders, $f(x) = \sum_{i=1}^{l} g_i(x) y_i$ can be recovered, where $g_i(x) = \prod_{\substack{j=1 \\ j \neq 1}}^{l} \frac{x\text{-}x_j}{x_i\text{-}x_j}$, and $s = a_0 = f(0)$.

3 Models and Design Goals

The system model and the goals are described in this section.

3.1 Communication Model

The RMS architecture is illustrated in Figure 1, which consists of a trusted server, the doctor, and the remote medical devices. In the beginning phase, the doctor and the medical devices register to the trusted server with a secure manner such as face to face. Except the beginning phase, all communications are over the open channel.

When the doctor sends a request information to the server, the server verifies the identity of the doctor, and checks if the request is legal. If the request is authenticated, the server invokes the corresponding devices. Then, a communication group is formed by the server including itself, the doctor and the invoked devices, a session key is shared among them to guarantee the secure communication over the open channel.

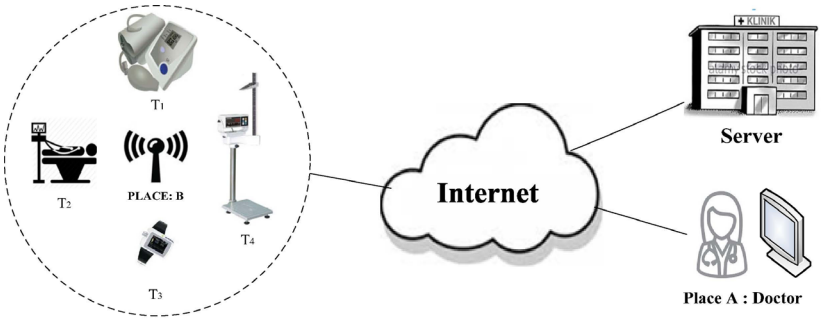

Figure 1. Remote medical system

3.2 Threat Model and Design Goals

3.2.1 Threat Model

Two kinds of adversary are assumed:

1. The external adversary. The external adversary can eavesdrop or modify the transmitted messages over the open channel, and can perform eavesdropping attack, replay attack, and so on.

2. The internal adversary. The internal adversary not only owns the capabilities of the external adversary, but also can easily get access to the medical server data-base and can perform the insider attack.

3.2.2 Design Goals

The design goals include the following items.

Eavesdropping attack resistance. The adversary can obtain nothing with the eavesdropped messages.

Replay attack resistance. When an outdated messaged is repeatedly transmitted, it can be detected.

Insider attack resistance. The authenticated doctor can only obtain the authorized medical information without knowing other information.

4 Review of YoHan et al.'s Protocol

4.1 YoHan et al.'s Scheme

YoHan et al.'s protocol consists of two stages: user registration and user authentication.

4.1.1 User Registration

A doctor with the identity Uid selects his password PW and a random number r_i , and calculates $MP, MP = h(PW, r_i)$, where $h(\cdot)$ is a secure hash function. Then doctor sends (Uid, MP) to the server via secure channel.

4.1.2 User Authentication

The doctor sends the requests $(Uid, TID_j, p_1, p_2, ..., p_t)$ to the RA, and the RA forwards the request to the server, where p_j , $(j = 1, ..., t)$ is the public point of each device. Then, the server selects a random number $R_i \in Z_q^*$ and computes a polynomial $f_u(x)$ using the public points $(p_1, p_2, ..., p_t, (MP, R_i))$. The server sends R_i to the doctor, and sends p_r that is a point on the polynomial $f_u(x)$ to the RA. After receiving R_i , the doctor can rebuild the polynomial $f_u(x)$, and sends $AM = h(s_1, Uid, f_u(0))$ to the RA. The RA verifies AM is authenticated. If yes, the RA accepts the doctor. If not, the RA rejects the doctor.

After successful authentication, the doctor and the RA can establish a secure channel using a session $K = h(f_u(0))$.

4.2 Security Analysis of YoHan et al.'s Protocol

YoHan et al. claimed their protocol to withstand various attacks, however, it is really vulnerable against the off-line password guessing attack and the devise impersonation attack.

In the authentication phase of YoHan et al's protocol, all messages are sent through the open channel. We can assume that an adversary can eavesdrop the communication channel, i.e., the adversary can intercept, insert, or delete the transmitted messages.

4.2.1 Off-line Password Guessing Attack

In real applications, people usually selects the easy-to-remember string as password, for example, birthday date, name, and telephone number. Both identity and password come from a very small dictionary. Therefore, the adversary can crack the correct identity and password through the brute-force attack. In YoHan et al's scheme, the doctor's identity is public information, the adversary just needs to guess the password. Therefore, the attack is easily launched and YoHan et al.'s protocol cannot resist the off-line password guessing attack.

4.2.2 Device Impersonation Attack

In the real environment, the public point of each device is not changed; the authentication process is executed between the doctor and the RA. At the same

time, RA is only an agency and does not have the capability to verify the legality of device. In other words, after the device is confronted by the adversary and there is no means to identify the attacker. Therefore, YoHan et al.'s protocol cannot withstand the device impersonation attack.

5 Our Scheme

To overcome the weaknesses in YoHan et al's protocol, a secure and lightweight remote medical system is presented, which consists of two phases: registration phase and remote invoking establishment phase.

5.1 Registration Phase

5.1.1 User Registration

A doctor with Uid sends a registration request to the server.

Step 1: The doctor chooses his password PW and imprints his biometric **impression** B.

Step 2: The doctor calculates $MP = h(PW, B)$, and sends (Uid, MP) to the server via secure channel.

Step 3: Server receives and stores Uid, MP.

5.1.2 Device Registration

In this phase, a long-term secret is shared between the server and the medical device.

Before a device is equipped in the system, the server generates a random number m_j $(j = 1, 2, ..., n)$, and injects m_j to $T_j, (j = 1, 2, ..., n)$ in a secure manner. m_j $(j = 1, 2, ..., n)$ can be updated when necessary.

5.2 Remote Invoking Establishment

Assume a doctor chooses to invoke t medical devices whose identities are $TID_1, TID_2, ..., TID_t$. This section includes the following three phases.

5.2.1 Authentication between Doctor and Server

Step 1: The doctor wants to invoke the remote medical devices $TID_1, ..., TID_t$, he sends the request and $(Uid, TID_1, ..., TID_t)$ to the server.

Step 2: Upon receiving the request, the server chooses a random number r_s, and sends it to the doctor. Then, the doctor computes $A_1 = h(MP, r_s)$, and sends A_1 and a random number r_u to the server.

Step 3: The server authenticates the doctor by checking $A_1 = h(MP, r_s)$ with the stored MP. If yes, the server computes $A_2 = h(MP, r_s, r_u)$, and sends A_2 to the doctor.

Step 4: The doctor verifies if the equation $A_2 = h(MP, r_s, r_u)$ holds. If yes, the mutual authentication is achieved.

5.2.2 Authentication between Server and Devices

Step 1: The server forwards the invoking request to t devices by broadcasting $(Uid, TID_1, ..., TID_t)$.

Step 2: The medical device with the identity T_j sends a random number r_j^D to the server, $(j = 1, ..., t)$. The server computes $AH_j = h(m_j, r_j^D)$, $(j = 1, ..., t)$, and sends AH_j and a random number r_j^S to T_j, $(j = 1, ..., t)$.

Step 3: T_j authenticates the server by checking $AH_j = h(m_j, r_j^D)$. If yes, T_j calculates $ATH_j = h(m_j, r_j^S, r_j^D)$, and sends ATH_j to the server.

Step 4: The server authenticates the T_j by checking $ATH_j = h(m_j, r_j^S, r_j^D)$, $(j = 1, ..., t)$. If true, the server believe that T_j is legal.

5.2.3 Session Key Establishment

Step 1: The server randomly selects a session key SK, and generates $f(x)$ passing through $(0, SK)$, $(Uid, h(MP, r_u))$, $(TID_j, h(m_j, r_j^D)), (j = 1, \cdots, t)$. Then, the server computes additional $(t+1)$ points $Q_1 = (1, f(1)), ..., Q_{t+1} = (t+1, f(t+1))$, and broadcasts $\{Q_1, ..., Q_{t+1}\}$.

Step 2: The doctor recovers $f(x)$ with the broadcasted messages $\{Q_1, ..., Q_{t+1}\}$ and his secret $(Uid, h(MP, r_u))$, and T_j recovers $f(x)$ with $\{Q_1, ..., Q_{t+1}\}$ and its $(TID_j, h(m_j, r_j^D))$, $(j = 1, 2, ..., t)$. Therefore, the session key $SK = f(0)$ is shared among them, which guarantees the secure communication.

5.3 Multi-factor Update Phase

When the doctor wants to update his password or the biometric, he sends an update request to the server. After the mutual authentication process between the doctor and the server, the doctor submits his new password PW^{new} or the new biometric B^{new}, and generates the new $MP^{new} = h(PW^{new}, B^{new})$. MP^{new} is sent to the server, and stored in the server.

6 Analysis

6.1 Security Analysis

The security is analyzed to satisfy the design goals.

6.1.1 Eavesdropping Attack Resistance

An adversary (either external or internal) eavesdrops to the transmitted message over the open channel, and the message $Uid, TID_j, A_1, A_2, r_u, r_s, AH_j, ATH_j, r_j^D, r_j^S$ are known by all. Therefore, due to the one-way property of hash function, the adversary cannot obtain MP and m_j. It is computational infeasible for an adversary to obtain any useful knowledge with the eavesdropped information. Therefore, the proposed scheme can resist the eavesdropping attack.

6.1.2 Impersonation Attack Resistance

If an adversary tries to impersonate the legal doctor, he needs pass mutual authentication between the doctor and the server, in which the secret information MP is only known by the doctor and the server, the adversary can not obtain MP. Moreover, it is computational infeasible to deduce MP from the messages over the open channel.

Similarly, it is impossible for the adversary to impersonate the legal device with the information transmitted over the channel.

6.1.3 Replay Attack

If an adversary tries to use the outdate message to launch the replay attack, it is still computational infeasible since the fresh random number is used to resist this attack. In order to achieve this goal, random number r_u, r_s, r_j^D, r_j^S is necessary. In addition, the date information can be also used to enhance this process when necessary.

6.1.4 Password Peeking Attack

Since the secret information shared between the doctor and the server is generated by involving the doctor's easily rememberable password and the biometric, it is more suitable for the practical environment. Even if the password is stolen, it is still secure since the biometric cannot be easily obtained by others. Moreover, the biometric includes several features, such as the fingerprints, the voiceprint, iris recognition, and other new techniques, which guarantees the scheme is scalable for the future.

6.2 Performance Analysis

In this section, the performance simulation is presented and compared with the related works, which is shown in Table 1, and Table 2.

Table 1. Comparison of computational cost

	User	User Efficiency	Server	Server Efficiency
Kumari et al. [11]	$5T_h + T_s$	Medium	$3T_h + T_s$	High
Jiang et al. [10]	$2T_h + 1T_s + 3T_{ch}$	Medium	$1T_h + 2T_s + 3T_{ch}$	Medium
YoHan et al. [17]	$1T_h + T_f$	High	$1T_s + 1T_f$	High
Our scheme	$4T_h + T_f$	High	$4T_h + T_f$	High

Table 2. Comparison of security features

	Jiang et al. [10]	Kumari et al. [11]	YoHan et al. [17]	The proposed scheme
E1	Yes	Yes	Yes	Yes
E2	-	Yes	No	Yes
E3	No	Yes	No	Yes
E4	Yes	Yes	No	Yes
E5	Yes	Yes	Yes	Yes
E6	Yes	Yes	Yes	Yes
E7	-	-	No	Yes

E1 Mutual authentication,
E2 Resist insider attack,
E3 User friendliness,
E4 Resist password guessing attack,
E5 Resist user impersonation attack,
E6 Resist replay attack,
E7 Resist device impersonation attack.

In order to test the performance, we define some notations as follows:

T_h = Time to compute a one way hash operation.

T_s = Time to compute a symmetric encryption operation.

T_f = Time to compute a polynomial operation.

T_{ch} = Time to compute a Chebyshev hash operation.

Efficiency = Total number of operations performed by the doctor and the server.

High efficiency = Total number of operations ≤ 05

Medium efficiency = 08 ≥ Total number of operations ≥ 06.

Low efficiency = Total number of operations ≥ 08.

7 Conclusion

In this paper, the weakness of YoHan's scheme is firstly analyzed, then a lightweight and secure remote medical authentication scheme is presented with the multi-factor authentication and the group communication, which aims to make it more suitable for the practical environment. Moreover, the security is enhanced due to the server-device mutual authentication and the server-doctor mutual authentication.

Acknowledgements

This work was partly supported by National Natural Science Foundation of China under grant Nos. 61363069, 61662016, 61602125, and 61772224, Foundation of Guizhou Provincial Key Laboratory of Public Big Data, Innovation Project of GUET Graduate, No. 2017YJCX49, and Innovation Project of Guangxi Graduate, No. YCSW2017139.

References

[1] I.-C. Lin, M.-S. Hwang, L.-H Li., A New Remote User Authentication Scheme for Multi-server Architecture, *Future Generation Computer Systems*, Vol. 19, No. 1, pp. 13-22, January, 2003.

[2] A. Irshad, M. Sher, M. S. Faisal, M. S, Faisal, A. Ghani, M. UI Hassan, S. Ashraf Ch, A Secure Authentication Scheme for Session Initiation Protocol by Using ECC on the Basis of the Tang and Liu Scheme, *Security and Communication Networks*, Vol. 7, No. 8, pp. 1210-1218, August, 2014.

[3] A. Irshad, M. Sher M, S. A. Chaudhary, H. Naqvi, M. S. Farash, An Efficient and Anonymous Multi-server Authenticated Key Agreement Based on Chaotic Map without Engaging Registration Centre, *The Journal of Supercomputing*, Vol. 72, No. 4, pp. 1623-1644, April, 2016.

[4] C.-L. Hsu, Y.-H. Chuang, C-l. Kuo, A Novel Remote User Authentication Scheme from Bilinear Pairings via Internet, *Wireless Personal Communications*, Vol. 83, No. 1, pp. 163-174, July, 2015.

[5] D. Giri, T Maitra, R. Amin, P. D. Srivastava, An Efficient and Robust Rsa-based Remote User Authentication for Telecare Medical Information Systems, *Journal of Medical Systems*, Vol. 39, No. 1, pp. 145, January, 2015.

[6] C.-C. Chang, T.-F. Cheng, W.-Y. Hsueh, A Robust and Efficient Dynamic Identity-based Multi-server Authentication Scheme Using Smart Cards, *International Journal of Communication Systems*, Vol. 29, No. 2, pp. 290-306, January, 2016.

[7] Y. Liu, C. Cheng, T. Gu, T Jiang, X. Li, A Lightweight Authenticated Communication Scheme for Smart Grid, *IEEE Sensors Journal*, Vol. 16, No. 3, pp. 836-842, February, 2016.

[8] M. K. Khan, S. K. Kim, K. Alghathbar, Cryptanalysis and Security Enhancement of a "More Efficient & Secure Dynamic ID-based Remote User Authentication Scheme , *Computer Communications*, Vol. 34, No. 3, pp. 305-309, March, 2011.

[9] H.-M. Chen, J.-W. Lo, C.-K. Yeh, An Efficient and Secure Dynamic Id-based Authentication Scheme for Telecare Medical Information Systems, *Journal of Medical Systems*, Vol. 36, No. 6, pp. 3907-3915, December, 2012.

[10] Q. Jiang, J. Ma, Z. Ma, G. Li, A Privacy Eenhanced Authentication Scheme for Telecare Medical Information Systems, *Journal of Medical Systems*, Vol. 37, No. 1, February, 2013.

[11] S. Kumari, M. K. Khan, R. Kumar, Cryptanalysis and Improvement of "A Privacy Enhanced Scheme for Telecare Medical Information Systems , *Journal of Medical Systems*, Vol. 37, No. 4, August, 2013.

[12] G. Zhao., X. Si., J. Wang., X. Long, T. Hu, A Novel Mutual Authentication Scheme for Internet of Things, *Proceedings of 2011 International Conference on Modelling, Identification and Control (ICMIC),* Shanghai, China, 2011, pp. 563-566.

[13] H.-M. Sun, B.-Z. He, C.-M. Chen, T.-Y. Wu, C.-H. Lin, H. Wang, A Provable Authenticated Group Key Agreement Protocol for Mobile Environment, *Information Sciences*, Vol. 321, pp. 224-237, November, 2015.

[14] P. N. Mahalle, N. R. Prasad, R. Prasad, Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT), *2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE),* Aalborg, Denmark, 2014, pp. 1-5, DOI: 10.1109/VITAE.2014.6934425.

[15] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, M. Ylianttila, PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications, *International Journal of Distributed Sensor Networks*, Vol. 10, No. 7, July, 2014.

[16] J.-L Hou, K.-H. Yeh, Novel Authentication Schemes for IoT Based Healthcare Systems, *International Journal of Distributed Sensor Networks*, Vol. 11, No. 11, pp. 1-9, August, 2015.

[17] Y. H. Park, Y. H. Park, A Selective Group Authentication Scheme for IoT-Based Medical Information System, *Journal of medical systems*, Vol. 41, No. 4, pp. 41-48, April, 2017.

[18] Shen J., Tan H., An Efficient RFID Authentication Protocol Providing Strong Privacy and Security, *Journal of Internet Technology*, Vol. 17, No. 3, pp 443-455, May, 2016.

[19] D. Wang, C. Ma, C. Weng, C. Jia, Cryptanalysis and Improvement of a Remote User Authentication Scheme for Resource-limited Environment, *Journal of Electronics and Information Technology*, Vol. 34, No. 10, pp. 2520-2526, October, 2013.

[20] D. He, D. Wang, Robust Biometrics-based Authentication Scheme for Multiserver Environment, *IEEE Systems Journal*, Vol. 9, No. 3, pp. 816-823, September, 2015.

[21] Y. Liu, Q. Zhong, L. Chang, Z. Xia, D. He, C. Cheng, A Secure Data Backup Scheme Using Multi-factor Authentication, *IET Information Security*, Vol. 11, No. 5, pp. 250-255, November, 2016.

[22] A. Shamir, How to Share a Secret, *Communications of the ACM*, Vol. 22, No. 11, pp. 612-613, November, 1979.

Appendix

Authentication Proof Based on BAN Logic

In this section, the authentication protocol is proved by the BAN logic.

For convenience, some notations is used in the BAN logic analysis.

- $P \mid\equiv X$: The principal P believes a statement X,

or P is entitled to believe X.

- $\#(X)$: The formula X is fresh.
- $P \Rightarrow X$: The principal P has jurisdiction over the statement X.
- $P \lhd X$: The principal P sees the statement X.
- $P \mid\sim X$: The principal P once said the statement X.
- (X, Y): The formula X or Y is one part of the formula (X, Y).
- X_Y: The formula X combined with the formula Y.
- $\{X\}_Y$: The formula X is encrypted under the key K.
- $(X)_Y$: The formula X is hash with the key K.
- $P \overset{K}{\leftrightarrow} Q$: The principals P and Q use the shared key K to communicate. The key K will never be discovered by any principal except P and Q

Some rules or logical postulates of BAN logic is defined as follows:

Rule 1 Message-meaning rule:

$$\frac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q \ , \ P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}.$$

Rule 2 Nonce-verification rule:

$$\frac{P \mid\equiv \#(X) \ , \ P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}.$$

Rule 3 Jurisdiction rule:

$$\frac{P \mid\equiv Q \mid\Rightarrow X \ , \ P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}.$$

Rule 4 Freshness rule:

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}.$$

Rule 5 Belief rule:

$$\frac{P \mid\equiv (X) \ , \ P \mid\equiv (Y)}{P \mid\equiv (X \ , \ Y)}.$$

Rule 6 Session keys rule:

$$\frac{P \mid\equiv \#(X) \ , \ P \mid\equiv Q \mid\equiv X}{P \mid\equiv P \overset{K}{\leftrightarrow} Q}.$$

The proposed protocol needs to satisfy the following goals under BAN logic.

Goal 1: $U \mid\equiv U \overset{MP}{\leftrightarrow} S$

Goal 2: $U \mid\equiv S \mid\equiv U \overset{MP}{\leftrightarrow} S$

Goal 3: $S \mid\equiv U \overset{MP}{\leftrightarrow} S$

Goal 4: $S \mid\equiv U \mid\equiv U \overset{MP}{\leftrightarrow} S$

Goal 5: $S \mid\equiv S \overset{m_j}{\Leftrightarrow} T$

Goal 6: $S \mid\equiv T \mid\equiv S \overset{m_j}{\Leftrightarrow} T$

Goal 7: $T \mid\equiv S \overset{m_j}{\Leftrightarrow} T$

Goal 8: $T \mid\equiv S \mid\equiv S \overset{m_j}{\leftrightarrow} T$

Since everyone knows the doctor's identity Uid, it may be considered as the doctor's public key, then $MP = h(PW, B)$ is the corresponding private key, only between legitimate doctors and servers shared.

General form:

Message 1: (A_1, r_u)

$$U \rightarrow S: ((U \overset{MP}{\leftrightarrow} S \ , \ r_s)_{(MP)} \ , \ r_u)$$

Message 2: A_2

$$S \rightarrow U: (S \overset{MP}{\leftrightarrow} U \ , \ r_u \ , \ r_s)_{(MP)}$$

Message 3: (AH_j, r_j^S)

$$S \rightarrow T: ((S \overset{m_j}{\Leftrightarrow} T \ , \ r_j^D)_{(m_j)} \ , \ r_j^S)$$

Message 4: ATH_j

$$T \rightarrow S: (S \overset{m_j}{\Leftrightarrow} U \ , \ r_j^S \ , \ r_j^D)_{(m_j)}$$

Idealized form:

Message 1: (A_1, r_u)

$$U \rightarrow S: (U \overset{MP}{\leftrightarrow} S \ , \ r_s)_{(MP)}$$

Message 2: A_2

$$S \rightarrow U: (S \overset{MP}{\leftrightarrow} U \ , \ r_u \ , \ r_s)_{(MP)}$$

Message 3: (AH_j, r_j^S)

$$S \rightarrow T: (S \overset{m_j}{\Leftrightarrow} T \ , \ r_j^D)_{(m_j)}$$

Message 4: ATH_j

$$T \rightarrow S: (S \overset{m_j}{\Leftrightarrow} T \ , \ r_j^S \ , \ r_j^D)_{(m_j)}$$

According to the description of our protocol, the following assumptions about the initial state is established, which will be used in the analysis of our protocol.

$$a_1: \ U \mid\equiv U \overset{MP}{\leftrightarrow} S$$

$$a_2: \ S \mid\equiv U \overset{MP}{\leftrightarrow} S$$

$$a_3: \ S \mid\equiv \#(r_s)$$

$$a_4: \ S \ |\equiv \ U \ |\Rightarrow \ U \overset{MP}{\leftrightarrow} S$$
$$a_5: \ U \ |\equiv \ \# \ (r_u)$$
$$a_6: \ S \ |\equiv \ S \overset{m_j}{\Leftrightarrow} T$$
$$a_7: \ T \ |\equiv \ \# \ (r_j^D)$$
$$a_8: \ T \ |\equiv \ S \ |\Rightarrow \ S \overset{m_j}{\leftrightarrow} T$$
$$a_9: \ S \ |\equiv \ \# \ (r_j^S)$$

Based on the above assumptions, the idealized form of our protocol is analyzed as follows. The main steps of the proof are described as follows:

According to a_1,

$$P_1: \ U \ |\equiv \ U \overset{MP}{\leftrightarrow} S \text{; (Goal1)}$$

According to the message (A_1, r_u),

$$P_2: \ S \ \triangleleft \ (U \overset{MP}{\leftrightarrow} S \ , \ r_s)_{(MP)};$$

According to a_2, P_2, and the message-meaning rule,

$$P_3: \ S \ |\equiv \ U \ |\sim \ (U \overset{MP}{\leftrightarrow} S \ , \ r_s);$$

According to a_3, and the freshness rule,

$$P_4: \ S \ |\equiv \ \# \ (U \overset{MP}{\leftrightarrow} S \ , \ r_s);$$

According to P_3, P_4, and the nonce-verification rule,

$$P_5: \ S \ |\equiv \ U \ |\equiv \ (U \overset{MP}{\leftrightarrow} S \ , \ r_s);$$

According to P_5, and the belief rule,

$$P_6: \ S \ |\equiv \ U \ |\equiv \ U \overset{MP}{\leftrightarrow} S \text{; (Goal 4)}$$

According to a_4, P_6, and the jurisdiction rule,

$$P_7: \ S \ |\equiv \ U \overset{MP}{\leftrightarrow} S \text{; (Goal 3)}$$

According to the message A_2,

$$P_8: \ U \ \triangleleft \ (U \overset{MP}{\leftrightarrow} S \ , \ r_u \ , \ r_s)_{(MP)};$$

According to a_2, P_8, and the message-meaning rule,

$$P_9: \ U \ |\equiv \ S \ |\sim \ (U \overset{MP}{\leftrightarrow} S \ , \ r_u \ , \ r_s);$$

According to a_5, and the freshness rule,

$$P_{10}: \ U \ |\equiv \ \# \ (U \overset{MP}{\leftrightarrow} S \ , \ r_u \ , \ r_s);$$

According to P_9, P_{10}, and the nonce-verification rule,

$$P_{11}: \ U \ |\equiv \ S \ |\equiv \ U \overset{MP}{\leftrightarrow} S \text{; (Goal 2)}$$

According to a_6,

$$P_{12}: \ S \ |\equiv \ S \overset{m_j}{\Leftrightarrow} T \text{; (Goal 5)}$$

According to the message (AH_j, r_j^S),

$$P_{13}: \ T \ \triangleleft \ (S \overset{m_j}{\Leftrightarrow} T \ , \ r_j^S)_{(m_j)};$$

According to a_7, P_{13}, and the message-meaning rule,

$$P_{14}: \ T \ |\equiv \ S \ |\sim \ (S \overset{m_j}{\Leftrightarrow} T \ , \ r_j^S);$$

According to a_7, and the freshness rule,

$$P_{15}: \ T \ |\equiv \ \# \ (S \overset{m_j}{\Leftrightarrow} T \ , \ r_j^S);$$

According to P_{14}, P_{15}, and the nonce-verification rule,

$$P_{16}: \ T \ |\equiv \ S \ |\equiv \ (S \overset{m_j}{\Leftrightarrow} T \ , \ r_j^S);$$

According to P_{16}, and the belief rule,

$$P_{17}: \ T \ |\equiv \ S \ |\equiv \ S \overset{m_j}{\Leftrightarrow} T \text{; (Goal 8)}$$

According to P_{16}, P_{17}, and the jurisdiction rule,

$$P_{18}: \ T \ |\equiv \ S \overset{m_j}{\Leftrightarrow} T \text{; (Goal 7)}$$

According to the message ATH_j,

$$P_{19}: \ S \ \triangleleft \ (S \overset{m_j}{\Leftrightarrow} T \ , \ r_j^S \ , \ r_j^D)_{(m_j)};$$

According to a_6, P_{19}, and the message-meaning rule,

$$P_{20}: \ S \ |\equiv \ T \ |\sim \ (S \overset{m_j}{\Leftrightarrow} T \ , \ r_j^S \ , \ r_j^D);$$

According to a_9, and the freshness rule,

$$P_{21}: \ S \ |\equiv \ \# \ (S \overset{m_j}{\Leftrightarrow} T \ , \ r_j^S \ , \ r_j^D);$$

According to P_{20}, P_{21}, and the nonce-verification rule,

$$P_{22}: \ S \ |\equiv \ T \ |\equiv \ (S \overset{m_j}{\Leftrightarrow} T \ , \ r_j^S \ , \ r_j^D);$$

According to and the belief rule,

$$P_{23}: \ S \ |\equiv \ T \ |\equiv \ (S \overset{m_j}{\Leftrightarrow} T); \text{ (Goal 6)}$$

According to Goal 1~Goal 8, the scheme implements the interactive authentication between the doctor and the device, and can prevent replay attack.

Biographies

Yining Liu is currently a professor in School of Computer Science and Information Security, Guilin University of Electronic Technology, China. He received the Ph.D. degree in Mathematics from Hubei University, Wuhan, China, in 2007. His research interests include the analysis of information security protocol, the smart grid, and privacy-preserving data aggregation.

Yuanjian Zhou received the B. E. degree from Zhengzhou University of Light Industry, China, in 2016. He is pursuing his M.E. degree in School of Computer Science and Information Security, Guilin University of Electronic Technology. His research interests focuses on information security protocol.

Youliang Tian received the Ph.D. degree in cryptography from Xidian University, Xi'an, China in 2012. He is a professor and Ph.D. supervisor in College of Computer Science and Technology at Guizhou University, Guiyang, China. His current research interests include algorithm game theory, cryptography and Information security.

Mingzhe Liu is currently a professor in School of Network Security, Chengdu University of Technology, China. He received the Ph.D. degree in Computer Science from Massey University, Palmerston North, New Zealand, in 2010. His research interests include intelligent information processing, information security, and system control.

Yanbin Zheng received the Ph.D. degree from the Guangzhou University, in 2016. He is currently a postdoctoral researcher in the School of Computer Science and Network Security, Dongguan University of Technology. His research interests include finite fields and cryptography.