SCHEME OF AUTHENTICATION OF HEALTH MONITORING SYSTEM BASED ON CREDIT CARD MECHANISM

Qiming Huang, Qilei Hao, Chao Guo and Shuang Li
School of Computer and Communication Engineering, University of Science and Technology Beijing
No.30 Xueyuan Road, Beijing, P.R. China

Keywords: Health monitoring system, Credit card mechanism, Authentication and Key Agreement (AKA), Identity-Based Cryptograph (IBC).

Abstract: Health monitoring systems are not just supported by local hospitals, but also supported by other province's hospitals. How to share the patient's health data by different hospitals? Similarly, a user first applies for a credit card with a bank whereby to buy goods at any merchant accepting credit cards. Merchants need not establish agreements with each other, but just need to have a trust relationship with one or a few banks that accept payments from credit-card users and pay merchants. After designing the logic hierarchical diagram of the health monitoring system, the credit card mechanism is applied to establish mutual authentication scheme with Identity-Based Cryptograph (IBC), which are used by clients in referral care between different hospitals of different provinces and between different hospitals of the same province. The authentication scheme ability has been analyzed to resist for Anti-counterfeit attacks, location privacy attacks and replay attacks.

1 INTRODUCTION

With the development of the aging problem in our country, research on the health monitoring system becomes one of the focuses. The confidentiality of patients' health information and the modes of authentication are the leading factors of protecting the safety and privacy of patients. Patients wear sensor nodes which measure health data such as heart rate and blood pressure. The sensor signals are transmitted to hospital through the mobile communication system (ETSI, 1993; Perkins, 2002) by the portable mobile communication networks access point sensor (such as mobile phone). Doctors read the patient's data, and emergency is disposed in time. Meanwhile the health care monitoring system can be also used to collect the physiological data of one person for a long time.

The security of medical data is a very important factor of the healthcare system. It is very significant to establish a safe cross-realm authentication mechanism of the medical data. The coordination opportunities between hospitals are increasingly more and more, and identities of clients need to be certificated when clients transmit between different hospitals. We propose a medical data certification schemes based on credit card mechanism for the problems of data authentication between different hospitals of different provinces and between different hospitals of the same province. This program applies encryption mechanisms to protect sensitive patient information, and the signature mechanism is use between partners completes cross-domain authentication.

Medical information security in IHE IT Infrastructure Technical Framework proposed audit trail and node authentication (ATNA), cross-enterprise user authentication (XUA) and digital signature guideline (DSG) and other technical specifications (Jianhu et al., 2008). ATNA, CUA and DSG can be shared in addressing security issues medical information. They are good references and technical guidelines to solve the sharing and security problem of medical information. This paper proposes an authentication mechanism based on credit card authentication system for the characteristics of the healthcare system in China, and puts audit trail and node authentication (ATNA), cross-enterprise user authentication (XUA) as references. We introduce the importance of security

Huang Q., Hao Q., Guo C. and Li S..
SCHEME OF AUTHENTICATION OF HEALTH MONITORING SYSTEM BASED ON CREDIT CARD MECHANISM.
DOI: 10.5220/0003605103500354
In *Proceedings of the 13th International Conference on Enterprise Information Systems* (ICEIS-2011), pages 350-354
ISBN: 978-989-8425-55-3

of medical data and propose a medical data certification schemes based on credit card mechanism in the first section. Then analyze the health monitoring system hierarchy in the second section. To carry out Authentication of Health monitoring system, three system models and their respective parameters are proposed. What's more, the method of an authentication and key agreement (AKA) are also included in the third section. At last we explicate the ability to resist for attacks in fourth section and reach a decision in the last section.

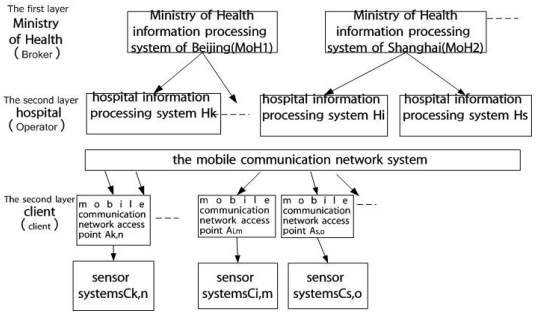

Figure 1: The logic diagram of the health monitoring system hierarchy.

2 BASICS OF AUTHENTICATION SYSTEM

2.1 The Definition of Bilinear

Let G_1 denote a cyclic additive group of some large prime order q and G_2 a cyclic multiplicative group of the same order. Assume that the discrete logarithm problem (DLP) is hard in both G_1 and G_2 (Mathis, 1956). For us, a pairing is a map $\hat{e}: G_1 \times G_2 \rightarrow G_2$ such that for all $P, Q \in G_1$ and all $a, b \in N$

$$\hat{e}(aP, bQ) = \hat{e}(aP, Q)^b = \hat{e}(P, bQ)^a = \hat{e}(P, Q)^{ab}$$

This paper meets the demand of confidentiality of data, using the discrete logarithm problem (DLP) in additive group (Mao, 2004). This means that choose two figure $P, Q \in G_1$ freely. It is difficult to find an integer $a \in Z_q^*$ which can fulfil $Q = aP$.

2.2 The Medical System Model

Medical health system can be divided into the following several levels, Ministry of Health, hospital and patient. The corresponding system of medical and health information is consist of three layers, which are provincial Ministry of Health information processing system (MoH), hospital information processing system (H), mobile communication network access point (A). And sensor systems of client connect with access point. Each provincial Ministry of Health and its affiliated form a domain. It is as shown below:

3 HEALTHCARE SYSTEM MODEL

3.1 Trust Model

This trust model for the health monitoring system bases on a credit card mechanism (TPM). The Broker, Operator and User in network correspond to the banks, merchants and users, in the credit card mechanism. And they correspond to the provincial Ministry of Health information processing system (MoH), hospital information processing system (H), mobile communication network access point (Ak) and sensor systems. To ensure the transmission of patient data in the Credit card mechanisms, users first to apply for permits from the bank. After passing authentication, the bank issued an electronic permit to the patient. Trust relationship is established between the user and the bank. Businesses only need to verify the user's permit.

We use MoH_1 and H_k on behalf of Broker1 and the Operator k respectively. We use $C_{K,n}$ to identification the unique client n enrolled in H_k . In addition, Ak,n refers to the mobile communication network access point n in H_k .. $PASSAk,n$ is a pass of $A_{k,n}$, signed by $MoH1$ .And $K_{Ak,n}$ is a pass-based key signed by MoH_1 . Similarly $PASSH_k$ and K_{Hk} are the pass and the pass-based key of H_k respectively. They are signed by MoH_1 . Furthermore, $(PASS_{Ak,n}^{MoH1}, K_{Ak,n}^{MoH1})$ refers to a temporary client (pass, pass-key) pair which MoH_1 issues to a served client.

3.2 Trust-domain Initialization

1) Generate the pairing parameters $< q, G_1, G_2, \hat{e}, P, H >$, where q is a generator; Let G_1 denote a cyclic additive group of some large

prime order q and G_2 a cyclic multiplicative group of the same order. $\hat{e}$ is a bilinear map; P is a generator of G_1; Hash function is $H:\{0,1\}^* \rightarrow G_1^*$

2) Pick a random $\beta \in Z_q^*$ as the domain-secret whereby to compute a domain-public-key as $P_{pub} = bP$ .The public trust-domain parameters is defined as follows:

$$\text{Domain-parameter} = (\text{group-parameter}, \text{domain-public-key}) = (< q, G_1, G_2, \hat{e}, P, H >, P_{pub})$$

In the first layer, the secret b in each provincial Ministry of Health domain is saved secretly and the domain parameters can be published. Since the difficulty of calculation about the discrete logarithm problem in additive group, it is not feasible to calculate b from (P, P_{pub}) .

3.3 Pass Model

The pass of medical security system structure uses ID-based cryptography (IBC) (Zhang and Fang, 2006; Zhu et al., 2008). This pass only use dozens of bits, compared with 1 KB length pass of X.509 Digital Certificate (Shamir, 1984). It saves much bandwidth resources. There are three types of passes in medical security system: Hospital passes(H-PASSes), Access point passes (A-PASSes), and temporary client passes (T-PASSes; ITU-T, 1989).

1) Issuance of H-PASSes:

The Ministry of Health information processing system (MoH1) issues an H-PASS as well as a pass-based key to hospital information processing system to H_k :

$$PASSHk = H_k$$

$$K_{Hk} = \beta^{MoH1} H_1^{MoH1}(PASSH_K)$$

Here β^{MoH1} is H_k 's domain secret, H_1^{MoH1} is the hash function of domain-parameter of H_K .

2) Issuance of A-PASSes:

To ensure the clients can access to hospital information processing system, a user have to be registered with the local provincial Ministry of Health . Pass and pass-based key are as follows:

$$PASSA_{n,k} = A_{n,k}$$

$$KA_{Hk} = \beta^{MoH1} H_1^{MoH1}(PASSA_{n,k})$$

Here β^{MoH1} is H_1^{MoH1} 's domain secret, H_1^{MoH1} is the hash function of domain-parameter of MoH1 .

3) Issuance temporary client passes (T-PASSes):

Temporary client passes (T-PASSes) passes is issued by hospital information processing system. The client which has T-PASSes is authenticated by current domain. Pass and pass-based key are as follows:

$$PASS_{Ak,n}^{MoH1} = (A_{Ak,n}^{MoH1}, \text{expiry} - \text{time})$$

$$K_{Ak,n}^{MoH1} = \beta^{MoH1} H_1^{MoH1}(PASS_{Ak,n}^{MoH1})$$

Here β^{MoH1} is operator MoH1's domain secret, H_1^{MoH1} is the hash function of domain-parameter of MoH1.

3.4 Authentication and Key Agreement

The authentication of the cross-domain in health monitoring system is include authentication and key agreement (AKA) between different hospitals of different provinces and between different hospitals of the same province. .

Different hospitals of different provinces AKA

When a user moves from one hospital to another hospital in different provinces, the Different hospitals of different provinces AKA occurs. Without loss of generality, we take $A_{i,m}$ and H_k as an example to explain the AKA process. User access point $A_{i,m}$ used to belong to a provincial MoH2 care range of hospital Hi. For some reason, the care information need to be transferred to the hospital Hk in other provincial MoH1. The application information sent by users should include the network address of hospital HK and the address of the access point AK. The protocol works in the following three steps.

$$H_k \rightarrow A_{i,m}: \quad PASSH_K, domain - params_{MoH1}, S_{kHk}(t_1) \tag{1}$$

$$A_{i,m} \rightarrow H_k: PASSA_{i,m}, S_{kAi,m}(t_2) \tag{2}$$

$$H_k \rightarrow A_{i,m}: PASS_{Ai,m}^{MoH1}, \varepsilon_{PASSA_{i,m}}, m(k_{Ai,m}^{MoH1}) \tag{3}$$

Hospital information processing system Hk sends (1). A i,m checks whether the difference between timestamp t_1 and his local clock time is within an acceptance window, when it receives (1). Then check $S_{kHk}(t_1)$ with $PASS_{Hk}$ and domain-$params_{MoH1}$. And use domain-$params_{MoH1}$ to verify $S_{kHk}(t_1)$.

If all of the check is successful, $A_{i,m}$ regards H_k as a legitimate hospital information processing system. Then $A_{i,m}$ sends its pass and the timestamp, which signed by the pass key (as the private key), to H_k .

$A_{i,m}$ can enrol in the local Ministry of Health(MoH) to obtain MoH pass in advance. Then, the H_k can receive and verify every user's certificate of MOH. If H_k recognizes that $A_{i,m}$ is a legal access point, H_k accepts the pass key signature stamp of $A_{i,m}$ and compares with the local time.

If the check of H_k is successful, Ai,m will be accept by Hospital information processing system. H_k can obtains temporary client passes from MoH1:

$$\mathrm{PASS}_{Ai,m}^{MoH1} = (\mathrm{A}_{Ai,m}^{MoH1}, expiry - time)$$

$$\mathrm{K}_{Ai,m}^{MoH1} = \beta^{\mathrm{MoH1}}\mathrm{H}_{\mathrm{i}}^{\mathrm{MoH1}}(\mathrm{PASS}_{Ai,m}^{MoH1})$$

Then the third step (3) can be carried out. Hk sends $\mathrm{PASS}_{Ai,m}^{MoH1}$ plaintext and pass-key $\mathrm{K}_{Ai,m}^{MoH1}$ encrypted under public-key $PASSA_{i,m}$ to Hk in message. After three successful handshakes, $C_{1,1}$ and $R_{1,1}$ may establish the shared system key:

$$K_{Hk,Ai,m}$$

$$= \hat{\mathrm{e}}^{\mathrm{MoH1}}\left(\mathrm{K}_{\mathrm{Ci,m}}^{\mathrm{MoH1}}, \mathrm{H}_{\mathrm{i}}^{\mathrm{MoH1}}\left(\mathrm{PASS}_{\mathrm{Ai,m}}\right)\right)$$

$$= \hat{\mathrm{e}}^{\mathrm{MoH1}}\left(\mathrm{H}_{\mathrm{i}}^{\mathrm{MoH1}}\left(\mathrm{PASS}_{\mathrm{Ai,m}}\right), \mathrm{H}_{\mathrm{i}}^{\mathrm{MoH1}}\left(\mathrm{PASS}_{\mathrm{Ai,m}}\right)\right)^{\beta^{\mathrm{MoH1}}}$$

$$= \hat{\mathrm{e}}^{\mathrm{MoH1}}\left(\mathrm{H}_{\mathrm{i}}^{\mathrm{MoH1}}\left(\mathrm{PASS}_{\mathrm{Ci,m}}^{\mathrm{MoH1}}\right), \mathrm{H}_{\mathrm{i}}^{\mathrm{MoH1}}\left(\mathrm{PASS}_{\mathrm{Ai,m}}\right)\right)^{\beta^{\mathrm{MoH1}}}$$

2) Different hospitals of the same province AkA

Provincial certification happens when the user transfers care responsibility from one hospital to the other hospital in the same province. For example, the user makes a referral care in the same province. In the information processing system of the hospital Hs, the user node As, o of transmitting data transfers to the hospital Hi. First, the user make an application, then send the application information with the network address of Hi and the address of As. The authentication protocol can be divided into two steps.

$$\mathrm{H_i} \rightarrow \mathrm{A_{s,o}}: \quad \mathrm{PASSH_{As,o}}, \mathrm{domain} - \mathrm{cert_{MoH2}}, \mathrm{S_{kAs,o}(t_1)} \tag{4}$$

$$\mathrm{A_{s,o}} \rightarrow \mathrm{H_i}: \mathrm{PASS}_{As,o}^{\mathrm{MoH2}}, \mathrm{t_2}, \mathrm{h_{kAs,oHi}(t_1||t_2)} \tag{5}$$

When As,o receives the message (4), the verification process is similar with Different hospitals of different provinces AKA;

If the inspections succeed, As,o regards Hi as a legitimate hospital information processing system. As,o and Hi establish a shared synchronous key:

$$K_{As,o,Hi} = \hat{e}^{MoH2}(K_{As,o}^{MoH2}, H_1^{MoH2}(\mathrm{PASS}_{Hi}))$$

Join the timestamp t1 and the renewal timestamp t2 together, using one-way hash function such as SHA-1to receive the complete code. Then encrypt $K_{As,o,Hi}$, and sent it to H_i together with t_2 and $\mathrm{PASS}_{As,o}^{MoH2}$.

After receiving (5), H_i checks that $PASS_{As,o,}^{MoH2}$ does not expired and t_2 is fresh enough. If so, it computes a shared key as

$$K_{Hi,As,o} = \hat{e}^{MoH2}(K_{As,o}, H_1^{MoH2}(\mathrm{PASS}_{As,o}^{MoH2})).$$

According to the chapter two, only if As,o is legitimate, the $K_{As,o,Hi}$ and 0 is equal.

$$K_{As,o,Hi}$$

$$= \hat{\mathrm{e}}^{\mathrm{MoH2}}\left(\mathrm{K}_{\mathrm{As,o}}^{\mathrm{MoH2}}, \mathrm{H}_{\mathrm{i}}^{\mathrm{MoH2}}\left(\mathrm{PASS}_{\mathrm{Hi}}\right)\right)$$

$$= \hat{\mathrm{e}}^{\mathrm{MoH2}}\left(\mathrm{H}_{\mathrm{i}}^{\mathrm{MoH2}}\left(\mathrm{PASS}_{Hi}\right), \mathrm{H}_{\mathrm{i}}^{\mathrm{MoH2}}\left(\mathrm{PASS}_{As,o}^{\mathrm{MoH2}}\right)\right)^{\beta^{\mathrm{MoH1}}}$$

$$= K_{Hi,As,o}$$

4 SAFETY ANALYSIS

In connection with the security problem of Health monitoring system, we analysis the security of this protocol as follows:

1. It achieves mutual authentication between the hospital information processing system and clients, and it have a stronger ability of Anti-counterfeit attack. In order to masquerade a client, an attacker must find one public-private key based on IBC to meet the equation:

$$K_{Ai,j}^{MoH} = b^{MoH} H_1^{MoH}(PASSA_{i,j}^{MoH}).$$

Although only using a small number of discrete logarithm, it has not reduce the difficulty of cracking the Public-private key, and is very suitable for these devices whose computing power is relatively weak. Although an attacker can easily obtain public key, the access of a attacker to the private key must calculate domain secrets b in terms of domain parameters. According to difficulty of calculate discrete logarithm in additive groups, it is very difficult to success in the limited time.

2. Achieve anti-replay attacks. Synchronous authentication is introduced, which requires the certification entities to maintain a synchronous clock strictly. This paper employs timestamps to prevent replay attacks, the protocol timestamp for authentication is provided by the counterpart

involved in authentication each time, even if intercepting the original information, an attacker can't implement replay attacks since each timestamp used for authentication is different.

3. To prevent the security risks caused by the session key generated by the communicator. As the protocol known, session key generation is actually using the calculation difficulty of the discrete logarithm in finite field, and this algorithm can make two client securely exchange a key to encrypt the message.

5 CONCLUSIONS

The text, which is intended for health monitoring system with secure authentication problems, designs authentication and key agreement system framework based on the credit card mechanism, and deals with authentication methods used by clients in referral care between different hospitals of different provinces and between different hospitals of the same province. They are both mutual authentication. This security system can also defend against counterfeit attack, location privacy attacks and replay attacks. Encryption technology based on identity is designed to lower the length of the certificate, which can effectively save bandwidth resources. It adapted to resource-constrained characteristics of medical sensors.

ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China (No. 61072039) and (No. 61003250), the Beijing Municipal Natural Science Foundation (No.4102040).

REFERENCES

European Telecommunications Standards Institute (ETSI), 1993. GSM 2.09: Security aspects.

Perkins C., 2002. IP mobility support for IPv4, RFC 3344.

Jianhu He, Qingli Zhou, Hui Tian, 2008. IHE laboratory technical framework, *Chinese Journal of Medical Instrumentation*. 32(6):449~452.

Mathis. H, Jun 1956. Bilinear Transformations, Circuit Theory. 3, Issue:2

Mao, W., 2004. An identity-based non-interactive authentication framework for computational grids. *Hewlett-Packard Laboratories*, Technical Report HPL-2004-96.

Trusted platform module (TPM) security policy. http:// www.trustedcomputinggroup.org.

Yanchao Zhang, Yuguang Fang, 2006 ARSA: An Attack-Resilient Security Architecture for Multihop WMNs, *IEEE*,

Zhu, H., Lin, X., Lu, R., Ho, P.-H., & Shen, X, 2008. Slab: Secure localized authentication and billing scheme for wireless mesh networks. *IEEE Transactions on Wireless Communications*, 7(10), 3858–3868

A. Shamir, 1984. Identity based cryptosystems and signature schemes, in Lecture Notes in Computer Science. Berlin, Germany: *Springer-Verlag*,

ITU-T 1989. Authentication Framework, ITU-T Recommendations X.509, ITU, Geneva,