

Security and Privacy Protection Protocol for Shared Medical Records

Kuo-Ching Liu^a Hui-Feng Huang^b

^aDepartment of Medical Laboratory Science and Biotechnology

China Medical University, Taichung 404, Taiwan, R.O.C.

kchliu@mail.cmu.edu.tw

^bDepartment of Information Management

National Taichung Institute of Technology, Taichung 404, Taiwan, R.O.C.

phoenix@ntit.edu.tw

摘要

建立病患之電子醫療病歷不僅可以傳送高品質的醫療服務，而且可以節省醫療之浪費。近來，無線射頻 (radio frequency identification 簡稱 RFID) 被廣泛的應用於各個領域，例如：供應鏈管理、存貨倉儲管理、以及藥品辨識之控制等等。然而，假如 RFID 系統沒有提供存取控制以及安全之驗證機制，將會遭遇一些安全上的問題。因為利用 RFID 系統之電子標籤能夠讀取回應的機制，使得非法使用者能取得電子標籤內之重要的訊息，甚至能追蹤使用者之位置或行為。為了保護病患的醫療記錄資訊以及隱私權，我們將提出一個適用於 RFID 系統之安全驗證機制以方便醫護人員於訪視病房時能迅速地借由 RFID 系統取得病患之電子醫療病歷，無須攜帶厚重的紙本病歷，並且能保護患者的醫療行為不被得知。

關鍵字：電子病歷、醫療照護、無線射頻系統、安全

Abstract

Establishing electronic patient care records is essential not only for delivering quality medical care services but also in saving medical expenses. Currently, radio frequency identification (RFID) is being deployed for a wide variety of applications, including supply chain management, inventory, storage, etc. However, RFID systems can have security problems if the tag offers no access control and certificated mechanisms. By utilizing responses from a tag, an adversary may try to obtain the

information of the product and trace the user. The protection of patients' health information is a very important concern in the information age. It must have secure mutual authentication mechanisms to protect electronic archives. In order to obtain appropriate medical information, physicians must efficiently get electronic patient records from a database (medical information system) to hospital wards. In this paper, we present a new idea to apply the radio frequency identification (RFID) system such that the physician can efficiently retrieve the electronic patient records for medical care when they visit patient wards without taking heavy paper records. In addition, the proposed scheme provides anonymous property and guards against patient tracing.

Keywords: electronic patient record, medical care, RFID system, security

1. Introduction

In today's, healthcare system there is an inevitable prerequisite for high quality and efficient well developed care. Established job sharing as well as communication and co-operation between all partners is a requirement for efficient healthcare. Therefore, enabling electronic patient records to be shared between physicians is essential not only for the quality of medical care services but also in saving medical expenses [4,6,8]. However, in Taiwan,

physicians usually visit their patients with paper-based records [4,8]. The paper-based records are disorganized and usually incomplete and can hardly be accessed in time for emergency care. In order to obtain appropriate medical information, physicians must efficiently get electronic patient records from a database (medical information system) to hospital wards. In this paper, we present a new idea to apply the radio frequency identification (RFID) system [1-3,5,7] such that the physician can efficiently retrieve the electronic patient records from a database when they visit patient wards without taking heavy paper records. It is very convenient and efficient for physicians or nurses to retrieve electronic patient records for medical care.

Radio frequency identification (RFID) is an automatic identification system that can remotely store and retrieve data about objects by using small devices called RFID tags. RFID systems consist of radio frequency (RF) tags and RF readers. Tag readers can question tags about their contents by broadcasting an RF signal, without physical contact. RFID devices can be broadly classified in two categories: those with a power supply that actively transmit to a reader are known as “active tags” and un-powered tags that are triggered by a reader are called “passive tags”. Due to low cost and conveniences in identifying an object without physical contact, RFID systems will replace the optical barcode on objects with consumer identification, the RFID systems can be used in lots of applications such as supply chain management, parking garage management, and inventory controls [1-3,5,7].

In our method, we construe a tag t_i for patient ID_i . When the patient ID_i is admitted to a hospital, the physician or nurse only takes a PDA (personal digital assistant) as a tag reader to quest a tag to obtain the health information of a patient through the RFID system. When the tag reader requests a tag to obtain the health information of patient, the back-end sever (database) provides the patient record to the reader according to the tag’s identity. The physician receives the patients’ records through the

RFID system. This is briefly illustrated in Figure 1.

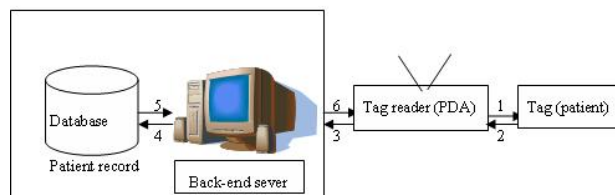


Figure 1 RFID System for patient record

However, the current RFID system allows any reader to access any tag. The exposed private information stored in the tag could be jeopardized [1-3,5,7]. Then, the widespread deployment of RFID systems into patient (consumer products) identification may expose potential security threats and risks either to corporations or individuals. Corporate espionage is a concern. A scheme could be developed to request unprotected RFID systems to gather information illegally, cheat tags to provide wrong information, or send Denial-of-Services (DoS) attacks to competitors. If a medical unit receives false messages and all efforts of the working staff are implemented under false pretenses, the loss of resources and manpower would be great. Therefore, the security of the RFID is becoming more and more important. It must have mutual authentication mechanisms to identify the legal tag (patient) and legal tag reader. In addition, the most important security requirement for patient (user) privacy is untraceability [1,5,7]. With an untraceability property, an attacker cannot track tags by using interactions with tags. It can protect the patient from tracing over wide areas. The protection of patients’ health information is a very important concern in the information age. With anonymity, tags will not expose their identifications to eavesdroppers without authentication.

To cope with the security threats, several security protocols had been proposed to enhance the security of RFID systems. Most of them cannot be applied to the RFID system because of cost limitation and limited resources dictate that RFID tags cannot afford the cost

expensive public key encryption or symmetric encryption [1-3,5,7]. For light-weight calculation power and protecting the privacy of a patient, we propose the RFID mutual authentication scheme based on synchronized secret information. Moreover, our scheme could protect a patient (user) from tracing and provide the anonymity property.

The remainder of this paper is organized as follows. In the next section, we will propose the mutual authentication protocol between the physician and patient based on the RFID system. The security analysis of our scheme is presented in Sections 3. And some conclusions will be made in the last section.

2. The proposed Scheme

This section will propose a new efficient mutual authentication protocol for RFID systems. The assumption, initial setup, and authentication process are described as follows:

Assumption and Initial Setup

Assume reader R connects with a legal back-end sever that has database D . The communication between the reader and the back-end sever is secure. The back-end sever and tag can operate the XOR ($\oplus$) operator and compute a common one-way hash function $h()$.

In the initialization stage, tag T is loaded with an initial identifier ID (the identity of a tag or the patient), a secret key k , and a hash function $h()$. In the same measure, the back-end database contains the same data stored in tag T ; including the ID of the tag, the secret key k and the hash function $h()$. The back-end database contains fields IDR , K , and K_{last} , which save the ID , the current k , and the preceding k_{last} (the previous secret information which is replaced by the current k), respectively. In addition to the content of tag T and the reader R have the PRNG (Pseudo Random Number Generator) to generate a random number for the authentication process.

Initially, the fields IDR and K are set up with the patient ID and the initial secret key k of each tag T ,

respectively; and all values of the field K_{last} are null. The role of K_{last} is to prevent desynchronization.

Authentication Process

We will depict the process of our authentication protocol as follows:

- Step 1. Reader R generates and saves a new pseudorandom number s by utilizing PRNG, and sends s to tag T .
- Step 2. Tag T also generates a new pseudorandom number r_1 and computes $r_2 = h((r_1 \oplus k) + s)$. Then, tag T sends r_1 and r_2 to the reader R .
- Step 3. After receiving r_1 and r_2 , reader R delivers r_1 , r_2 , and s to the back-end server.
- Step 4. When the back-end server receives the authentication request from the reader, it iteratively picks up any entry information (ID , k , k_{last}) from its database. It then computes and checks whether any of the two equations $r_2 = h((r_1 \oplus k) + s)$ and $r_2 = h((r_1 \oplus k_{last}) + s)$ hold. (1) This process is repeated for each entry until it finds a match. If it can match an entry, then authentication of the tag succeeds, and the server performs the next step; otherwise, it sends a "failure" message to the reader R to stop the process.
- Step 5. If the back-end server successfully authenticates the tag in the step 4, it computes $r_3 = h((r_2 \oplus k) + s)$ or $r_3 = h((r_2 \oplus k_{last}) + s)$ depending on which value k or k_{last} satisfies in the verification equation (1) in step 4. It also updates the value of field K into $h(k)$ and the value of field K_{last} into k if $r_2 = h((r_1 \oplus k) + s)$ in equation (1), if it holds; otherwise, it does not update the information of fields K and K_{last} . Then, the server sends r_3 and the patient's information (Data) of tag T to reader R .

Step 6. The reader retrieves the information (Data) of patient and forwards r_3 to tag T . Upon receiving r_3 , tag T computes $r_3' = h(r_2 \oplus k \oplus s)$ by using its secret key k , and then checks if $r_3' = r_3$. If it holds the current secret key k of tag T is replaced by $h(k)$.

In our scheme, we construct a hash chain of secret information as follows: The hash chain starts from secret t , the second secret k_2 is $h(t)$, and the other i -th element k_i is $h(k_{i-1})$. The above processes are briefly illustrated in Figure 2.

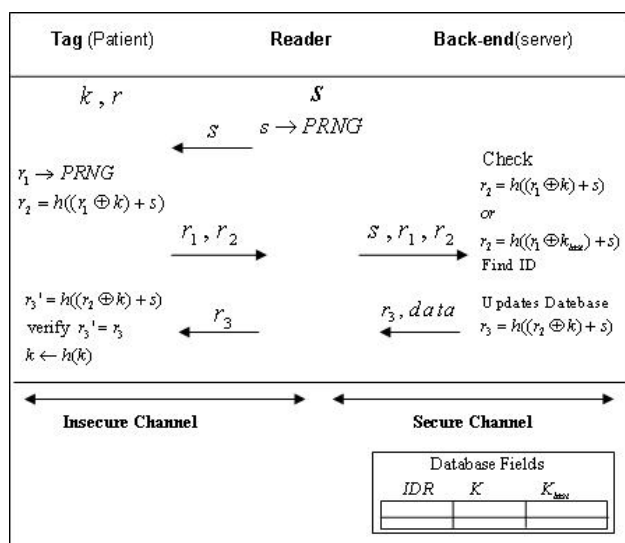


Figure 2 The proposed Scheme

In our scheme, the design of simultaneously maintaining the old key and the new key for each tag (patient) is in the back-end database and can resist the denial-of-services attack (DoS). That is, the back-end database has been replaced by the current (or new) key with $h(k)$; however, when reader R sends the " r_3 " command to tag T , it can suddenly be intercepted or modified by an attacker. Tag T will then hold the old key k . Thus, the shared key between the tag and the server will be out of synchronization. In this situation, if the back-end database only keeps the new key for each tag, then the tag and the reader cannot authenticate each other any more. The DoS attack succeeds. Therefore, in our scheme, the back-end database simultaneously maintains old keys and new keys

which can then resist the DoS attack.

3. Security analysis

In this section, we analyze the security of our scheme. Due to the challenge of response technology and the freshness of random numbers s and r_1 per session, our scheme achieves mutual authentication of the reader (server) and the tag (patient), and can resist the replay attack. Without knowing the secret key k of tag T , an attacker cannot use the same method as in Section 2 to cheat the reader (or back-end server) into passing out fake authentication because it is very difficult for the attacker to make the equation $r_2 = h((r_1 \oplus k) + s)$ hold. Therefore, our scheme can resist a forgery attack.

In our method, the design of simultaneously maintaining the old key and the new key for each tag (patient) in the back-end database can resist the Denial-of-Services attack (DoS). On the other hand, only randomized data (s, r_1, r_2, r_3) are transmitted on the wireless channel between the reader R and tag (patient) T ; and the patient ID information is only transmitted from the back-end server to reader R through the secure channel. Therefore, the privacy and anonymity properties for patient ID are ensured. Moreover, because the secure key k of patient ID is updated after each successful authentication and the new key is generated by applying a function $h()$, the compromise of a tag would not lead to the tracing the previous communications for the same tag (patient). It is very hard for an attacker to access the tags (patients) and trace the tags (patients), hence forward secrecy is achieved. Therefore, the proposed scheme provides mutual authentication for a patient and the server in the RFID system and offers an anonymity property to protect patients from tracing.

4. Conclusions

For light-weight calculation power of a tag and protecting the privacy and confidential information of a patient, we propose a simple and efficient RFID mutual

authentication scheme based on synchronized secret information. Through our authentication protocol, a physician can efficiently retrieve electronic patient records from a database when they visit patient wards without having to carry reams of patient records. It is very convenient and efficient for physicians or nurses to retrieve electronic patient records for medical care. In addition, the proposed method provides the untraceability property that could protect a patient from tracing over World Wide Web.

References

- [1] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks", *Conference on Security and privacy for Emerging Areas in Communication Networks-SecureComm*, September, 2005.
- [2] D. Henrici and P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers", *IEEE International Workshop on Pervasive Computing and Communication Security-PerSec*, pp.149-153, March 2004.
- [3] S. M. Lee, Y. J. Hwang, D. H. Lee, and J. I. Lim, "Efficient authentication for low-cost RFID systems", *International Conference on Computational Science and its Applications-ICCSA*, pp. 619-627, May 2005.
- [4] C. T. Liu, A. G. Long, Y. C. Li, and K. C. Tsai, "Sharing Patient Care Records over the World Wide Web", *International Journal of Medical Informatics*, pp. 189-205, vol. 61, 2001
- [5] D. Molnar and D. Wagner, "Privacy and security in library RFID: issues, practices, and architectures", *ACM Conference on Computer and Communications Security-ACM CCS*, pp. 210-219, October 2004.
- [6] P. Pharow and B. Blobel, "Electronic Signature for Long-Lasting Storage Purposes in Electronic Archives", *International Journal of Medical Informatics*, pp. 279-287, vol. 74, 2005.
- [7] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", *International Conference on Security in Pervasive Computing-SPC*, pp. 454-469, March 2003.
- [8] C. M. Yang, H. C. Lin, P. Chang, and W. S. Jian, "Taiwan's Perspective on Electronic Medical Records' Security and Privacy Protection: Lessons Learned from HIPAA", *Computer Methods and Programs in Biomedicine*, pp. 277-282, vol. 82, 2006.