

# Security authentication based position for U-Health application services

Byeong Ho Ahn<sup>1a)</sup>, Jinkeun Hong<sup>2b)</sup>, Donghoon Lee<sup>1c)</sup>,  
and Ki Hong Kim<sup>3d)</sup>

<sup>1</sup> Graduate School of Information Management and Security/  
Center for Information Security Technologies, Korea University,  
1, 5-ka, Anam-dong, Sungbuk-Gu, Seoul, 136–701, South Korea

<sup>2</sup> Division of information & Communication, Baekseok University,  
115 Anseo-dong, Dongnam-Gu, Cheonan-si, Chnumnam, 330–704, Korea

<sup>3</sup> The Attached Institute of ETRI,  
909, Jeonmin-dong, Yuseong-Gu, Taejeon, 305–390, South Korea

a) [bhahn2@ensec.re.kr](mailto:bhahn2@ensec.re.kr)

b) [jkhong@bu.ac.kr](mailto:jkhong@bu.ac.kr)

c) [donghlee@korea.ac.kr](mailto:donghlee@korea.ac.kr)

d) [hong0612@ensec.re.kr](mailto:hong0612@ensec.re.kr)

**Abstract:** To support healthcare organizations responses, many companies have started solutions to be satisfied the specific requirements of healthcare programs, and plans. This paper presents authentication scheme of RFID system based on GPS location in the U-health care services.

**Keywords:** health, wireless, ubiquitous, RFID

**Classification:** Storage technology

## References

- [1] S. Spyrou, P. D. Barnidis, N. Maglaveras, G. Pangalos, and C. Pappas, “A Methodology for Reliability Analysis in Health Networks,” *IEEE Trans. Inf. Technol. Biomed.*, vol. 12, no. 3, pp. 377–386, May 2008.
- [2] C. C. Tan, B. Sheng, and Q. Li, “Secure and Serverless RFID Authentication and Search Protocols,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1400–1407, April 2008.
- [3] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, “Security and privacy aspects of low cost radio frequency identification systems,” *LNCS2802*, pp. 201–212, 2004.
- [4] A. D. Henrici and P. Mauller, “Hash-based enhancement of location privacy for radio frequency identification devices using varying identifiers,” *IEEE PerCom2004*, pp. 149–153.
- [5] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, “Mutual authentication protocol for low cost RFID,” *Encrypt Workshop on RFID and Lightweight Crypto*, 2005.

## 1 Introduction

Ubiquitous health application services such as RFID have joined a new generation including an increasing amount of service, and research area across, rather than within, the boundaries of standard organizations [1, 2]. Today, ubiquitous computing technologies can be used to provide better solutions for healthcare of elderly persons at home or in the hospital. Also, data fusion from multiple sensors shows itself as having the capability to create a system of better monitoring of persons. Therefore, in this paper, we present authentication scheme in the implementation of a ubiquitous healthcare system, one that contains RFID reader based on GPS, and which is managed by patients, nurses, managers, and doctors, for emergency and health condition management. In a ubiquitous environment, the principal service among health care services and patient management services must be supported centering on the patient. In this paper, we propose an authentication mechanism that can access or protect session from the boundary of ranges, which is applied to a GPS location management concept in the client mobile terminal for secure patient care information. Hence, in the point of authentication based on RFID system for emergencies in a secure healthcare network, and its security characteristic is analyzed.

## 2 The framework of healthcare system

The healthcare system, which is based on GPS and RFID, utilizes variable applications for dictation, reviewing patient medical records, and other daily activities. Patients' personal privacy becomes an issue of concern when extra personal information is collected besides IP location, and RFID based on GPS position for enhanced health content personalization. As a central information hub, the healthcare portal client can be tailored to the specific needs and roles of particular users such as patients, doctors, and nurses, providing instant access to proper applications, content, and services that promote collaboration and enhance community. The role contains the minimum number of permissions to instantiate an object and can be assigned to one or more ubiquitous users. Authentication, which is the process of determining who the network users are, is a fundamental challenge for every healthcare institution

## 3 Authentication scheme based location on RFID system

### Writing Process

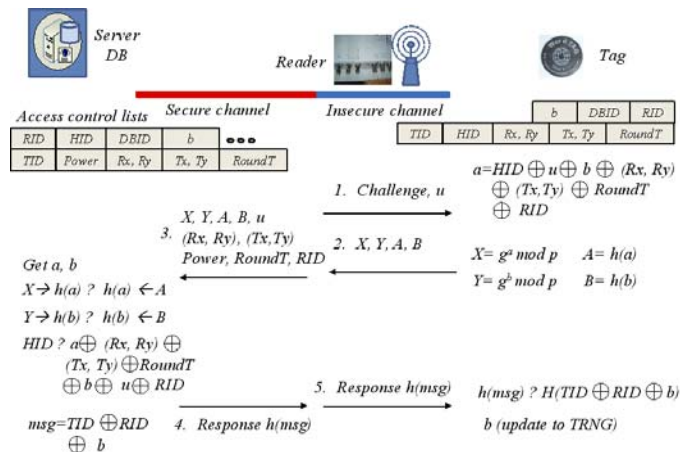
In this process, server manager writes  $b$ ,  $RID$ ,  $DBID$ ,  $TID$ ,  $(Rx, Ry)$ ,  $(Tx, Ty)$ , and  $RoundT$  values in DB and tag.  $(Rx, Ry)$  is reference position values of longitude and latitude of reader,  $(Tx, Ty)$  is reference position values of longitude and latitude of tag, and  $RoundT$  is reference returned time from reader and tag. First reader is connected with PC and knows its location from its GPS module. The location information is wrote at first stage and then is wrote at predefined time after authentication. Initial tag's location  $(Rx, Ry)$  is wrote by the manager and then its location value according to

location movement is stored in tag. Where, location movement value ( $T_x$ ,  $T_y$ ) is calculated with the received power of RSSI, time delay from received tag, and direction of antenna.

$$(T_x, T_y) = \text{optimizing value}\{\text{distance}(\text{received power of RSSI}), \text{time delay from received tag}\}, \text{direction of antenna}\}$$

### Authentication process

In step1, reader broadcasts challenge and random number  $u$  to tag in Fig. 1. In step2, tag computes and transmits to reader values such as,  $X$ ,  $Y$ ,  $A$ ,  $B$ . In this step,  $HID$  is  $h(TID)$ ,  $a$  is  $HID(+)u(+)b(+) (Rx, Ry)(+) (Tx, Ty)(+) RoundT$ ,  $A$  is  $h(a)$ ,  $B$  is  $h(b)$ . Here,  $HID$  is a field for the temporary identification value of RF tag  $T$ .  $h( )$  is one-way hash function.  $h(TID)$  is a hash value of tag ID.  $(+)$  is exclusive-or (XOR) function. As shown in Fig. 1, reader sends  $u$  to the tag. Receiving  $u$  from the reader, tag calculates  $a$ ,  $X$ ,  $Y$ ,  $A$ ,  $B$  and then sends them to the reader. Server DB gets  $a$  and  $b$ , and checks if  $HID$  is validate. After validating the  $HID$ , server DB responds  $h(msg)$  to the reader. Reader sends  $h(msg)$  to the tag and then finally tag checks if  $h(msg)$  is validate.



**Fig. 1.** Authentication Process

In step3, the reader transmits to server DB values such as,  $X$ ,  $Y$ ,  $A$ ,  $B$ ,  $u$ ,  $(Rx, Ry)$ ,  $(Tx, Ty)$ ,  $RoundT$ ,  $RID$ . In step4, the server computes and verifies transmitted data and DB data. First, let be get  $a$ ,  $b$ . In server, there compute and verify  $h(a)$ ,  $h(b)$  and  $a$ ,  $b$  are computed from which is stored data in DB, and transmitted  $X(=h(a))$ , and  $Y(=h(b))$ . Also  $a$ ,  $b$  are derive by doing decryption of  $X$ ,  $Y$ .

Table I show that it is presented security characteristics in according to authentication schemes and the proposed scheme is guaranteed major security characteristics, and can be controlled access of device through position tracking in particular.

In Table II, it is reviewed the efficiency in according to authentication scheme. As shown in Table II, proposed scheme has 5 rounds,  $T_{Hash}(4)$  time(tag) value,  $T_{TRNG}(1)$  and  $T_{GPS}(1)$  time(reader) value, and  $T_{TRNG}(1)$

**Table I.** Security Characteristics in each scheme

<i>Scheme</i>	<i>Anonymity</i>	<i>Forward secrecy</i>	<i>Replay attack</i>	<i>DoS attack</i>	<i>Position tracking</i>
Hash locking(Weis)[3]	X	X	X	O	X
Randomized hash locking (Weis)[3]	X	X	X	O	X
Varying ID locking (Henrici)[4]	O	X	X	O	O
Mutual Auth(Yang)[5]	X	X	O	O	X
Proposed scheme	O	O	O	O	O

**Table II.** The Efficiency in each scheme

<i>Scheme</i>	<i>Round</i>	<i>Time(tag)</i>	<i>Time(Reader)</i>	<i>Time(Server)</i>
Hash locking (Weis)	6	0	-	0
Randomized hash locking (Weis)	5	$T_{\text{Hash}}/T_{\text{PRF}}(1), T_{\text{RNG}}(1)$	-	$T_{\text{Hash}}(n)/T_{\text{PRF}}$
Varying ID locking (Henrici)	5	$T_{\text{Hash}}(3)$	$T_{\text{RNG}}(1)$	$T_{\text{Hash}}(2)$
Mutual Auth(Yang)	5	$T_{\text{Hash}}(2)$	$T_{\text{RNG}}(1)$	$T_{\text{Hash}}(2n)$
Proposed scheme	5	$T_{\text{Hash}}(4)$	$T_{\text{TRNG}}(1), T_{\text{GPS}}(1)$	$T_{\text{TRNG}}(1), T_{\text{GPS}}(1)$

and  $T_{\text{GPS}}(1)$  time(server).

#### 4 Security analysis

We define and analysis security requirements as follows: Theorem1 ~ Theorem5.

##### Theorem 1 (Anonymity) proof

In step2 and 4, we will emphasis that it is supported encryption process and difficult to estimate data by the attacker. In step 2, we can present that it can not made an inference a by any attacking, a is  $g^a \bmod p$ , where a is  $HID(+)u(+)b(+) (Rx, Ry)(+) (Tx, Ty)(+) RoundT$ , and it cannot solved HID due to one way hash function property. In step4, from response  $h(msg)$ , we can show that  $h(msg)$  is processed by one way hash function. Where  $h(msg)$  is  $TID(+)RID(+)b$ . So we can be proved about anonymity property.

##### Theorem 2 (Forward Secrecy) proof

If it tries to leak out data on tag by attacker, the previous data cannot be inference from the presented data.

*An attacker controlling all but one reader in a RFID network should not be able to recover TID, b, HID, b, X, Y, h(x), h(msg) shared between the reader/server and the tag. There are no relationships between the current value b and previous value b', between the current value a and the previous value a'. Check  $a = HID(+)u(+)b(+) (Rx, Ry)(+) (Tx, Ty)(+) RoundT$  ?  $a' = HID(+)u'(+)b'(+) (Rx, Ry)(+) (Tx', Ty')(+) RoundT$ . Check  $h(msg)$  is  $TID(+)RID(+)b$  ?  $h(msg')$  is  $TID(+)RID(+)b'$ . Therefore, we show that it cannot be induced a and b from a' and b'.*

### Theorem 3 (Replay attack) proof

During transmission, attacker intercepts RFID data, and the captured data is transmitted by the attacker after a certain time.

*The reader send original values  $u$  and  $(Tx, Ty)$ , and new values  $u'$  and  $(Tx, Ty)'$ . Check  $a = HID(+)u(+)b(+) (Rx, Ry)(+) (Tx, Ty)(+) RoundT$  ?  $a' = HID(+)u'(+)b(+) (Rx, Ry)(+) (Tx, Ty)'(+) RoundT$ .  $h(msg)$  is  $TID(+)RID(+)b$  ? Check  $h(msg')$  is  $TID(+)RID(+)b'$ . Therefore, we show that it cannot be replayed to attack  $a'$ ,  $b'$  and  $h(msg')$ .*

### Theorem 4 (DOS attack) proof

DOS is kinds of attacks such as, jamming and interference on physical layer, blocking and disrupting the operation of RFID reader and server.

*If secret value shared between tag and sever can not be synchronized, response message  $h(msg)$  is failed. But in Server DB, previous value  $b$  is stored, and  $h(msg')$  (is  $TID(+)RID(+)b'$ ) send to reader, and tag. In the tag, to authenticate, it requires  $TID$ ,  $RID$ , and updated  $b'$ . Against dos attack, it can be guaranteed  $msg'$  from one way hash function  $h()$ .*

### Theorem 5 (Position tracking) proof

If the access of communication connection between the tag and the reader/server can be controlled, the link will be guaranteed. If attacker, which is distinguished, will be tried the access of the reader and the server, it can be traced the attacking tag.  $A_r(x, y)$  is included in  $(Rx, Ry)$  reference of  $x$  coordinates (longitude) and  $y$  coordinates (latitude).  $RoundT'$  is new access time for round trip between reader and tag. When the location of tag and reader decides, the reference values are  $RoundT$  and power (received power, which is between reader and tag).

*If  $(Rx', Ry') \in A_r(x, y)$ , it can be accessed the reader.*

*If  $RoundT < RoundT'$  and  $(Rx, Ry) < (Rx', Ry')$ , tag cannot be accessed in reader*

*Location of tag is estimated from reader location  $(Rx, Ry)$ , power and length, which is estimated as followed.*

$$Tag(x, y) = (Rx, Ry) + Avg(Length(RoundT/2), Power).$$

*Where check  $a = HID(+)u(+)b(+) (Rx, Ry)(+) (Tx, Ty)(+) RoundT$  ?  $a' = HID(+)u(+)b(+) (Rx', Ry')(+) (Tx, Ty)(+) RoundT'$ . Therefore, we show that it can be accessed in case of  $a$ , otherwise, cannot be access in case of  $a'$ .*

## 5 Conclusion

Recently, health care applications have been issued in ubiquitous computing services. In this paper, it is presented to the authentication scheme, which is RFID based on GPS location in the hospital and health care center. When we are compared proposed scheme with the conventional scheme in RFID network, it takes robust characteristics in respect of position tracking.

## Acknowledgments

---

This work was supported by the Second Brain Korea 21 Project.