디지털산업정보학회 논문지 제11권 제1호-2015년 3월
http://dx.doi.org/10.17662/ksdim.2015.11.1.059

Security Analysis to an Biometric Authentication Protocol for Wireless Sensor Networks*

Lee Youngsook**

WSN 환경에서 Biometric 정보를 이용한 사용자 인증 스킴의 안전성 분석

이 영 숙

〈Abstract〉

A novel authentication mechanism is biometric authentication where users are identified by their measurable human characteristics, such as fingerprint, voiceprint, and iris scan. The technology of biometrics is becoming a popular method for engineers to design a more secure user authentication scheme. 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 identity individuals in groups that are under surveillance. In this article, we review the biometric-based authentication protocol by Althobati et al. and provide a security analysis on the scheme. Our analysis shows that Althobati et al.'s scheme does not guarantee server-to-user authentication. The contribution of the current work is to demonstrate this by mounting threat of data integrity and bypassing the gateway node on Althobati et al.'s scheme. In addition, we analysis the security vulnerabilities of Althobati et al.'s protocol.

Key Words : Biometric-based Authentication Scheme, Wireless Sensor Network, Smart Card, Data Integrity, Bypassing, User Authentication

Ⅰ. Introduction

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, motion or pollutants and to cooperatively pass their data through the network to a main location [1-4]. Wireless sensor network is composed of large number of sensor nodes that are scattered in hostile unattended environments. The inclusion of wireless communication technology also incurs various types of security threats. It is important that these security concerns be addressed from the beginning of the system design. So understanding security of wireless sensor network is important issue. There

* 이 논문은 2015년 호원대학교 연구비 지원을 받은 것임.
** 호원대학교 사이버수사 경찰학부 부교수

are so many mechanisms are developed to provide the security to sensor network or node. One of the important issues in security of wireless sensor network is main security goal of authenticating between a remote individual and the sensor nodes, between the sensor node and the gateway node, and between the remote individual and the gateway node.

Smart card-based password authentication provides two factor authentications, namely a successful login requires the client to have a valid smart card and a correct password [5-11]. While it provides stronger security guarantees than password authentication, it could also fail if both authentication factors are compromised (an attacker has successfully obtained the password and the data in the smart card). In this case, a third authentication factor can alleviate the problem and further improve the system's assurance. Another authentication mechanism is biometric authentication where users are identified by their measurable human characteristics, such as fingerprint, voiceprint, and iris scan.

In 2013, Althobati et al. [11] proposed an efficient remote user authentication protocol using biometric information [12-15]. The new technology of biometrics is becoming a popular method for engineers to design a more secure user authentication scheme. 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 identity individuals in groups that are under surveillance.

In their article, they claim that the user can be authenticated using a biometric information and establishers the session key to be shared with between the server and the user. In addition to making this claim, Althobati et al. claim to exhibit various merits with its scheme: (1) biometric-based authentication is more reliable than conventional authentication based on a password. (2) their protocol provides mutual authentication between not only gateway and sensor node but also between gateway and user. (3) their protocol was adapted to be efficient and lightweight in terms of computational cost and communication cost to decrease the energy consumption of sensor nodes which have limited energy and resources. (4) their protocol provides confidentiality of messages between all entities (user, gateway, and sensor node); therefore, only authorized users can use these messages, which are confidential against any attack. However, in this article, we uncover Althobati et al.'s protocol does not guarantee its main security goal of mutual authentication. We show this by mounting threat of data integrity and bypassing the gateway node attack on Althobati et al.'s protocol. What we do in this work is to report this security vulnerabilities of Althobati et al.'s protocol.

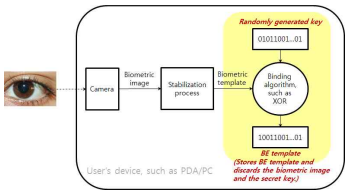
The remainder of this paper is organized as follows. Section 2 reviews Althobati et al.'s user authentication protocol. Section 3 presents weakness on Althobati et al.'s protocol offers. Finally, we conclude this work in Section 4.

Ⅱ. Review of Althobaiti et al.'s Authentication Protocol

This section reviews a novel biometric-based remote user authentication protocol proposed by Althobati et al. [11]. The scheme participants include a gateway node, a remote user, and a server. For simplicity, we denote the gateway node by GW the remote user by U_i, and the server by S. Althobati et al.'s protocol consists of three phases: registration phase, login phase, and authentication phase. The registration phase is performed only once per user when a new user registers itself with the gateway node. The authentication phase is carried out whenever a user wants to gain access to server. The system parameters listed in Table 1 are assumed to have been established in advance before the protocol is used in practice. Assume that the secrete parameter X is generated the gateway GW and the secret key shared between GW and the server S.

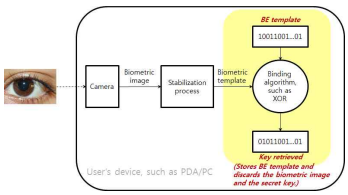
<Table 1> Notation

U_i	device of entity U_i
ID_i	identity of an entity U_i
SID_j	identity of a server S_j
$iris_i$	the feature of the user U_i's iris
K	the secret key of the user U_i
X	the secret parameter generated by GW and securely stored in designated S_j
RM	the response of S_j to the queery of user U_i
$Enc_K(m)$	Encryption of m using an asymmetric key K
$Dec_K(m)$	Decryption of m using an asymmetric key K
$h(\bullet)$	One-way hash function
$\|\|$	Concatenation operation
$\oplus$	XOR operation



<Fig 1> Saving user's secret key

During some initialization phase, the biometric encryption will take place by using a fuzzy commitment scheme as in [16]. Fuzzy commitment scheme overcomes the drawback of traditional biometric systems where there is no need to store neither images nor the template of them in the memory.



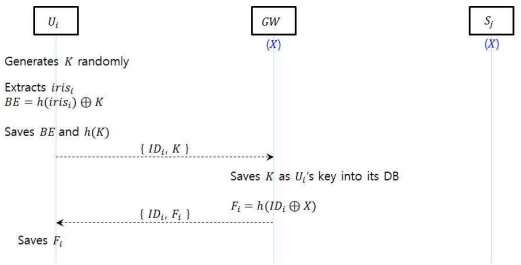
<Fig 2> Retrieving user's secret key

2.1 Registration Phase

This is the phase where a new registration of a user takes place. Althobati et al.'s protocol is performed by extracting the features of iris using an Fig 3 registration phase of Althobaiti al.'s iris recognition system. Additionally, the hash value of the encryption key will be saved with the BE template to be able to reject incorrect keys in an early step, before beginning the process of remote authentication as shown in Fig 1. When the BE template is saved in the user's device, the user can

retrieve his key by capturing an image of his iris via the user's device camera. After that, the features of iris will be extracted by the iris recognition model, then XRed with the BE template to regenerate the user's key as shown in Fig 2. The registration proceeds as illustrated by Fig 3, where dashed lines indicate a secure channel:

R 1. A user U_i who wants to register with the gateway GW, randomly generates an encryption key K, computes $BE = h(iris) \oplus h(K)$ and saves BE and $h(K)$ on U_i's device. Now U_i sends its identity ID_i and the encryption key K the gateway GW via a secure channel.



<Fig 3> Registration of phase Althobaiti al.'s protocol

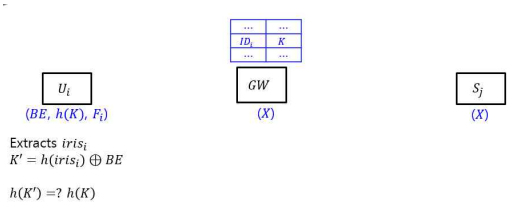
GW saves K into its database and computes $F_i = h(ID_i \oplus K)$.

Then, sends $\langle ID_i, F_i \rangle$ to the user U_i via a secure channel.

R 2. User U_i saves secretly F_i.

2.2 Login Phase

This phase is carried out whenever the user visits a gateway node and wants to gain access to the server S_j.



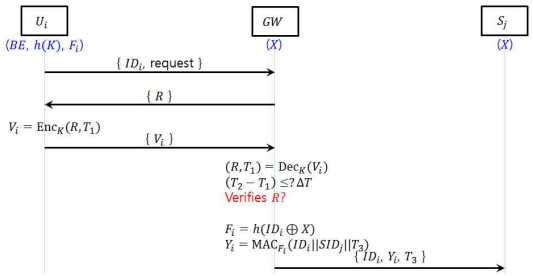
<Fig 4> Login phase of Althobaiti al.'s protocol

L 1. After iris acquisition by camera in the U_i's device, the features of U_i's iris are extracted.

L 2. The iris's features are corrected by error correcting code and hashed by SHA256.

L 3. Then, U_i computes $K' = h(iris) \oplus BE$ and checks that whether K' equals K or not. If the variable is not equal, U_i rejects the login request. Otherwise, the application is proceeded.

L 4. After that, U_i sends <ID_i and request> to the gateway GW node.



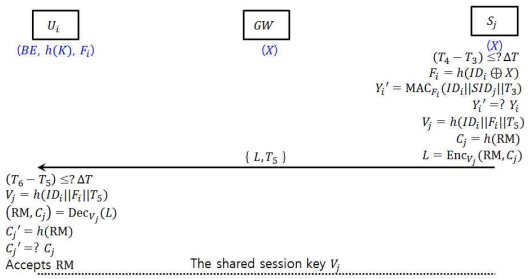
<Fig 5> Authentication phase between U_i and GW

2.3 Authentication Phase

With the login request message $\langle ID_i$ and request>, the scheme enters the authentication phase during which U_i and GW node perform the following steps:

A 1. When the login request arrives $\langle ID_i$ and request>, the GW node generates the random number R and sends it to U_i.

A 2. After receiving <R> from GW, U_i retrieves the current timestamp T_1, computes $V_i = Enc_K(R, T_1)$, and sends V_i to the gateway node GW.



<Fig 6> Authentication phase between U_i and

A 3. Upon receiving R, GW decrypts V_i with key K, verifies that the decryption yields the same R as chosen by own and checks the freshness of the timestamp T_1. GW aborts if the verification and the check T_1 fail. Otherwise, GW retrieves the current timestamp T_3 and computes

$F_i = h(ID_i \oplus X)$,

$Y_i = MAC_{F_i}(ID_i \| SID_j \| T_3)$.

Then, sends the message <ID_i, Y_i, T_3> to the server S_j.

With the gateway's message <ID_i, Y_i, T_3>, the protocol enters the authentication phase during which U_i and S_j perform the following steps:

A 4. The server S_j checks if the timestamp T_3 is fresh. If not, S_j aborts the session. Otherwise, S_j computes $F_i = h(ID_i \oplus X)$ and $Y_i^{'} = MAC_{F_i}(ID_i \| SID_j \| T_3)$ and checks that whether $Y_i^{'}$ equals Y_i or not. If the verification is not equal, S_j aborts the session. Otherwise, S_j retrieves the timestamp T_5 and computes

$V_j = h(ID_i \| F_i \| T_5)$,

$C_j = h(\mathrm{RM})$,

$L = Enc_{V_j}(\mathrm{RM}, C_j)$.

Then, S_j sends the response message <L, T_5> to the user U_i.

A 5. After receiving $\langle L, T_5 \rangle$ from S_j, user U_i checks if the timestamp T_5 is fresh. If not, U_i aborts the session. Otherwise, U_i computes $V_j = h(ID_i \| F_i \| T_5)$ and decrypts L with the key V_j and verifies that the decryption correctly returns C_j^*. IF the verification succeeds U_i checks that C_j^* is equal to $h(\mathrm{RM})$ and if equal accept the response message RM.

Ⅲ. Weakness in Althobaiti al.'s Authentication Protocol

Kocher et al. and Messerges et al. pointed out that the confidential information stored in smart cards could be extracted by physically monitoring its power consumption [17-18]. Therefore, it is fair to say that if a user loses his or her smart card, all information in the smart card may be revealed to the attacker. Althobaiti et al.'s scheme [11] is vulnerable to authentication phase between U_i and S_j. We show this by mounting threat of data integrity and bypassing the gateway node on its protocol.

3.1 Impersonating S to U_i

In [11], the smart card stores various information for user login and authentication. The smart card for the user U_i includes $BE, h(K)$ and F_i. Using these information, an attacker can compute the response message V_j to U_i's login request message <ID_i, Y_i, T_3>. This section described security analysis of Althobaiti et al.'s protocol [18].

3.1.1 Threat of data integrity

First, Althobaiti al.'s protocol does not provide data integrity. We demonstrate this weaknesses by mounting a type of a server impersonation attack where an adversary U_a can easily compute forged response message to U_i's login request message. We now proceed to describe the server impersonation attack.

Step 1. Now when U_i sends the login request message <ID_i, Y_i, T_3> to the server S_j. The adversary U_a posing as S_j intercepts this login request and sends to U_i a forged response message.

Step 2. The adversary U_a, who has obtained BE, $h(K)$, and F_i stored in its smart card, generates timestamp T_5', and computes $C_j = h$ (RM), V_j = $h(ID_i \| F_i \| T_5)$, and L' = Enc_{V_j} (RM, C_j). Then sends the response message <L', T_5> to the user U_i.

Step 3. Since, from U_i's point view, L' and T_5' are indistinguishable from L and T_5 of an honest execution, U_i believes that the message L' and T_5' is from S_j. Hence, U_i operates as specified in protocol using the received messages from U_a. Finally, the adversary U_a and the user U_i are able to compute common secret session key V_j.

3.1.2 Bypassing the gateway node

Now, Althobaiti al.'s protocol may bypass the gateway node. This weakness is due to the fact that L' is computed using the confidential information stored in smart card. Before describing the attack, we note that the secret values stored in a smart card could be extracted by monitoring its power consumption [8, 10].

We demonstrate this weaknesses by mounting a type of a server impersonation attack using of bypassing the gateway node. against the protocol. The attack scenario is detailed as follows.

Step 1. When U_i initiates the authentication phase with the login request message <ID_i and request >, the adversary U_a posing as S_j intercepts this message and sends a forges the server S_j's response message as follows: U_a who has obtained the login message, <ID_i and request > first, generates a random number R_A' sends <R_A'> in response to $U_i's$ login request message.

Step 2. Receiving the message R_A', U_i computes V_i = $Enc_K(R_A', T_1)$ and sends V_i to the gateway node GW.

Step 3. The attacker U_a intercept the message V_i

so that it is discarded. U_a generates the timestamp T_5 and computes $V_a = h(ID_i \| F_i \| T_5)$ using extracted the secret value F_i and

$C_a = h(\mathrm{RM_a})$,

$L' = ENC_{V_a}(\mathrm{RM_a}, C_a)$. Then the attacker U_a sends the message $<L', T_5>$ to the user U_i.

The forged response $<L', T_5>$ will pass the verification test by U_i. Hence, U_i believes U_a as the authentic server.

Step 4. Finally, the adversary U_a and S_j are able to compute common secret session key.

3.2 Security analysis

The security vulnerabilities of Althobaiti et al.'s protocol are attributed to the following fact:

- To forge a valid response message $< L', T_5>$ of U_a posing as S, it suffices to obtain the information stored in a smart card; BE, $h(K)$, and F_i.
- To forge a valid response message $<L', T_5>$ of U_a bypassing the gateway node, it suffices to obtain the information stored in a smart card; F_i.

Security analysis : Through the attack, mutual authentication is completely compromised. From the viewpoint of session-key secrecy, the effect of our attack is the same as that of a server impersonation attack. At the end of the attack, U_i believe that they have established a secure session with each other sharing a secret key, while in fact they have shared their keys with the attacker U_a. Althobaiti et al.'s protocol fail to achieve important security properties such as mutual authentication, session-key security, data integrity, and message confidentiality resistance against impersonation attacks. A summary of security results for existing it's protocol is given in Table. 2.

<Table 2> Security analysis

considerations on security	the result of the review
gateway node bypassing attacks	not secure
server impersonation attack	not secure
session key establishment	not provide
mutual authentication	not provide
data integrity	not provide
message confidentiality	not provide

Ⅳ. Conclusion

This work has considered the security of Althobaiti et al.'s authentication protocol [11] using biometric information. We demonstrate this by a server impersonation attack that completely compromises mutual authentication of the protocol. In addition, we have demonstrated the security analysis to the protocol. We hope that similar security vulnerabilities as identified in this work can be avoided in the future design of the Biometric-based authentication protocol.

Reference

[1] Rathod, V., Mehta, M., "Security in wireless sensor network: a survey," GANPAT Univ. J.

Eng. Technol. 1(1), 2011, pp.35-44.

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E., "A survey on sensor networks," IEEE Commun. Mag, 40(8), 102-114.

[3] Youngsook Lee, Jeeyeon Kim and Dongho Won, "Weakness of Tan's Two-Factor User Authentication Scheme in Wireless Sensor Networks Lecture Notes in Electrical Engineering," 203, 2012, pp.707-714.

[4] Das, M. L. "Two-factor user authentication in wireless sensor networks," IEEE Trans Wirel. Comm, 8, 2009, pp.1086-1090.

[5] Ku, W. -C., Chang, S. -T., Chiang, M. -H., "Weaknesses of a remote user authentication scheme using smart cards for multi-server architecture," IEICE Trans. Commun, E88-B(8), 2005, pp.3451-3454.

[6] Li, L. -H., Lin, I. -C., Hwang, M. -S., "A remote password authentication scheme for multiserver architecture using neural networks," IEEE Trans. Neural Netw, 12(6), 2001, pp.1498-1504.

[7] Y. Lee, J. Kim, and D. Won, "Security Improvement to a Remote User Authentication Scheme for Multi-Server Environment," The Korea-Society of Digital Industry& Information Management, 7(4), 2011, pp.23-30.

[8] Tsai, J. -L., "Efficient multi-server authentication scheme based on one-way hash function without verification table," Comput. Secur, 27, 2008, pp.115-121.

[9] Tsuar, W. -J., "An enhanced user authentication scheme for multi-server internet services," Appl. Math. Comput, 170, 2005, pp.258-266.

[10] Tsuar, W. -J., Wu, C--. C., Lee, W. -B., "A flexible user authentication for multi-server internet services," Networking-JCN, LNCS 2093, 2001, pp.174-183.

[11] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, "An Efficient Biometric Authentication Protocol for Wireless Sensor Networks," International Journal of Distributed Sensor Networks, Volume 2013, Article ID 407971, 13 pages.

[12] Z. Cheng, Y. Lee, C. Chang, C. L, "A novel biometric-based remote user authentication scheme using Quadratic Residues," International Journal of Information and Electronics Engineering, 3(4), 2013, pp.419-422.

[13] J. Yuan, C. Jiang, and Z. Jiang, "A biometric-based User Authentication for wireless Sensor Networks," Wuhan university journal of national sciences, 5(3), 2010, pp.272-276.

[14] E. -J. Yoon, K. Y. Yoo, "A new biometric-based user authentication scheme without using password for wireless sensor networks," Proceedings of 2011 IEEE International workshops of enabling technologies: Infrastructure for collaborative enterprises, 2011, pp.279-284.

[15] Y. Lee, "Security Analysis of a Biometric-Based User Authentication Scheme," 10(1), 2014, pp.81-87.

[16] A. Al-Hussain and I. Al-Rassan, "Abiometric-based authentication system for web services mobile user," in Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia (MoMM'10), 2010, pp.447-452.

[17] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis," in Advances in Cryptology-CRYPTO99, 1999, pp.388-397.

[18] T. S. Messergers, E. A. Dabbish, R. H. Sloan, "Examining smart card security under the threat of power analysis attacks," IEEE Trans. Comput, 51(5), 2002, pp.541-552.

■ 저자소개 ■

이 영 숙
Lee Youngsook

2009년 3월~현재 호원대학교 사이버수사경찰학부 부교수
2011년 8월 ~현재 호원대학교 사이버수사경찰학부 학부장
2008년 8월 성균관대학교 컴퓨터공학과 (공학박사)
2005년 2월 성균관대학교 정보보호학과 (공학석사)
1987년 2월 성균관대학교 정보공학과(공학사)

관심분야 : 암호프로토콜 암호이론, 디지털 포렌식, 스마트폰 보안
E-mail : ysooklee@howon.ac.kr

논문접수일: 2015년 1월 24일
수 정 일: 2015년 2월 10일
게재확정일: 2015년 2월 16일