The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 6, pp.95-101, Dec. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2016.16.6.95
JIIBC 2016-6-11

스마트 카드 분실 공격에 안전한 사용자 인증 스킴의 취약점 및 개선방안

Weaknesses and Improvement of User Authentication Scheme against Smart-Card Loss Attack

최윤성*

Younsung Choi*

요 약 최근에는 인터넷 및 통신망 기술의 발달과 함께 무선 센서 네트워크 기술에 대한 연구가 활발해지고 있다. 그와 더불어 무선 센서 네트워크 환경을 적법하게 사용하기 위해서, 사용자 및 센서에 대한 인증기술에 대한 중요성도 커져가고 있다. 처음으로 Das가 스마트 카드와 패스워드를 이용한 무선 센서 네트워크 환경에서의 인증 스킴을 제안한 이후로, 취약점 분석 및 안전한 인증기술에 관한 연구가 활발히 진행되고 있다. 그 중 Chen 등은 스마트 카드 분실 공격에 안전한 인증 스킴을 제안하였다. Chen 등이 제안한 스킴은 효율적이지만 여전히 완전 순방향 비밀성 미보장, 익명성 미보장, GW에 의한 세션키 노출 문제와 패스워드 검사가 제공되지 못하여 발생하는 취약점들이 분석되었다. 이를 해결하기 위해서 본 논문에서는 퍼지추출 기술, 타원곡선 암호, 동적 ID 기술 등을 스킴에 적용하여, 보안성이 향상된 사용자 인증 스킴을 제안하고, 제안하는 스킴의 안전성을 분석하였다.

Abstract With the rapid development of Internet and communication network technology, various studies had proceeded to develop the technology of wireless sensor networks. Authentication schemes for user and sensor are critical and important security issue to use wireless sensors legally. First, Das introduce a user authentication scheme using smart card and password for wireless sensor networks, various studies had proceeded. Chem et al. suggested a secure user authentication scheme against smart card loss attack but Chen et al. scheme does not still resolve some security vulnerability such as perfect forward secrecy, session key exposure by gateway node, anonymity, and the password check. To resolve the problems, this paper proposes a security enhanced user authentication using the fuzzy extraction, elliptic curves cryptography and dynamic ID and analyzes the security.

Key Words : Security Analysis, User Authentication, Smart-card Loss Attack

Ⅰ. 서 론

무선 센서 네트워크는 최근 인터넷 및 통신망을 활용하여 실시간 교통관제 및 유통관리에 이용되고 있으며, 화산이나 지진과 같이 사람이 접근하기 어려운 장소의 정보를 측정하는 등 광범위한 분야에서 응용되고 있다[1-3]. 이때 사용자의 인증을 위하여 스마트 카드를 이용하여 상호인증을 가능하고 다양한 취약점을 개선한 스킴들이 제안되고 있다[4]. Das 가 스마트 카드와 패스워드를 이용하여 무선 센서 네트워크 환경에 적합한 인증 스킴

*정회원, 호원대학교 사이버수사보안학부
접수일자: 2016년 9월 2일, 수정완료: 2016년 12월 2일
게재확정일자: 2016년 12월 9일

Received: 2 September 2016 / Revised: 2 December 2016
Accepted: 9 December, 2016
*Corresponding Author: yschoi@howon.ac.kr
Dept. of Cyber Investigation Security, Howon University, Korea

을 제안한 후로 보다 활발한 연구가 진행되고 있다[5]. Nyang 등은 Das의 인증 스킴이 오프라인 패스워드 추측 공격에 취약하다고 분석하였다. 그리고 Khan 등은 Das의 스킴이 무선 센서 네트워크의 게이트웨이 노드를 회피하는 공격이 가능하는 것을 밝혀냈다[6]. 그 후 Vaidya 등은 Khan 등이 제안한 스킴이 스마트 카드 분실 공격에 취약하다고 분석했다. 이러한 문제를 해결하기 위해서 Yuan은 생체정보를 기반으로하는 인증 스킴을 제안하였다[7]. Yeh은 Yuan의 인증 스킴을 개선하여 타원 곡선 암호를 활용하여 보다 안전한 인증 스킴을 제안하였다[8]. 그리고 Chen 등도 무선 센서 네트워크 환경에 적합하고 스마트 카드 분실 공격에 안전한 인증 스킴을 제안하였다[9]. 본 논문에서는 Chen 등이 제안한 인증 스킴의 취약점들을 분석하여 문제점을 밝혀내고, 이를 해결하고 보안성이 향상된 인증 스킴을 제안하고 안전성을 분석하고자 한다.

본 논문에서는 2장에서 먼저 Chen 등이 제안한 스킴의 동작과정을 알아보고 취약점을 분석하여 완전 순방향 비밀성 미보장. 익명성 미보장, GW에 의한 세션키 노출, 패스워드 검사 미제공에 대한 문제를 지적한다. 그리고 3장에서는 Chen 등이 제안한 스킴의 취약점을 해결하기 위한 변경사항 및 개선사항을 살펴본 후, 안전성을 향상시킨 인증 스킴을 제안한다. 4장에서는 본 논문에서 제안한 인증 스킴에 대한 안정성을 분석하여 기존의 문제가 해결되었는지 알아본다. 그리고 5장에서 결론을 짓는다.

II. Chen 등이 제안한 인증 스킴의 분석

2장에서는 Chen 등이 제안한 대칭키 기술 기반 인증 스킴의 동작과정과 취약점을 분석한다. Chen 등의 인증 스킴은 User(U_i), Gateway node(GW), Sensor node(S_n) 간의 통신으로 이루어져 있으며, 스킴이 동작하기 전에 GW은 두 가지 비밀값 x_a와 x_s를 가지고 있으며, S_n은 $h(x_s||SID_n)$를 가지고 있다[9].

1. Chen 등이 제안한 인증 스킴의 동작과정

Chen 등의 인증스킴은 등록과정, 패스워드 변경과정, 인증과정, 총 3가지 단계로 구성되어 있다.

[등록과정] (1) U_i는 자신의 식별정보 ID_i와 패스워드 PW_i를 선택하고 랜덤숫자 b를 생성한 후, $\underline{PW_i} = h(PW_i||b)$를 계산한다. 그리고 U_i는 GW에게 ID_i와 PW_i를 안전한 채널을 이용하여 전송한다 (2) GW는 $N_i = h(ID_i||x_a) \oplus PW_i$를 계산한다. 그리고 GW는 스마트카드에 $\{ID_i, N_i, h(\cdot)\}$ 저장한 후, 스마트카드를 U_i에게 전송한다. (3) U_i는 스마트카드를 받은 후, U_i는 스마트카드에 b를 입력하면 등록과정이 마무리된다.

[패스워드 변경과정] (1) U_i는 스마트 카드를 장치에 삽입하고 ID_i와 기존의 패스워드 PW_i와 새로운 패스워드 PW_i^*를 입력한다. (2) 스마트카드는 U_i가 입력한 PW_i와 저장된 PW_i가 동일한지 검사한 후, 같으면 새로운 패스워드 PW_i^*를 저장한다. (3) 그리고 스마트카드는 $PW_i = h(PW_i||b)$와 $PW_i = h(PW_i^*||b)$를 계산하고, $N_i^* = N_i \oplus PW_i \oplus PW_i^*$를 계산한 후, 기존의 N_i를 N_i^*로 교체한다.

[인증과정] (1) U_i는 스마트카드를 장치에 삽입하고 ID_i와 PW_i를 입력한다. 스마트카드는 $PW_i = h(PW_i||b)$, $k = h((N_i \oplus PW_i)||T_1)$를 계산하며, T_1는 사용자의 현재타임스탬프이다. 스마트카드는 랜덤숫자 $R_1 \in \{0, 1\}$를 생성하고, $A_i = E_k(ID_i||R_1||T_1)$를 생성한다. $E_k(\cdot)$는 대칭키 k를 이용하여 ·를 암호화하는 함수이다. 그 후 U_i는 GW에게 $\{ID_i, A_i, T_1\}$를 전송한다. (2) GW는 $\{ID_i, A_i, T_1\}$를 받은 후, 먼저 T_1를 $(T'_1 - T_1) \leq \Delta T$를 이용하여 검증하는데 여기서 ΔT 는 예상지연시간을 뜻한다. GW는 $k = h(h(ID_i||x_a)||T_1)$와 $D_k(A_i) = \{ID_i, R_1, T_1\}$를 계산하며, 이때 $D_k(\cdot)$를 ·값을 대칭키 k를 이용하여 복호화하는 함수이다. 그리고 GW는 복호화된 값인 ID_i와 T_1가 기존에 받은 ID_i와 T_1와 일치하는지 검사한다. 만약 일치하면, GW는 $SK = h(ID_i||h(x_s||SID_n)T_2)$, $B_i = h(h(x_s||SID_n)||SK||SID_n||ID_i||T_2)$를 계산하는데, SK는 U_i와 S_n 간의 세션키로 사용된다. 마지막으로 GW는 S_n에게 $\{ID_i, B_i, T_2\}$ 메시지를 전송한다. (3) S_n은 T_2를 검증하고 $SK = h(ID_i||h(x_s||SID_n)T_2)$를 생성한다. S_n은 $B^*_i = h(h(x_s||SID_n)||SK||SID_n||ID_i||T_2)$를 계산하고 B_i 와 B^*_i 이 일치하는지 확인한다. 만약 일치하게 되면 S_n은 $C_i = h(h(x_s||SID_n)||SK||ID_i||SID_n||T_3)$를 계산한 후, GW에게 $\{C_i, T_3\}$ 메시지를 전송한다. (4) GW는 먼저 T_3를 검증하고 $C_i^* = h(h(x_s||SID_n)||SK||ID_i||SID_n||T_3)$를 계산한 후, C_i와 C_i^* 이 동일한지 확인한다. 동일하면, GW는 $D_i = E_k(ID_i||SID_n||SK||R_1||T_4)$를 계산하고 U_i에게 메시지 $\{D_i, T_4\}$를 전송한다. (5) U_i는 $D_k(D_i)$를 이용하여 D_i를 복호화하여, $\{ID_i, SID_n, SK, R_1, T_4\}$를 도출한다. 그리고 U_i는 기

존의 값들과 복호화된 ID_i, R_i, T_4가 동일한지 검사한다. 값들이 동일하면, U_i는 GW를 인증하게 되고 세션키 SK를 이용하여 S_n 과 암호화된 통신을 하게 된다.

2. Chen 등이 제안한 인증 스킴의 취약점 분석

[완전 순방향 비밀성 미보장] 완전 순방향 비밀성이란 장기간 사용되는 중요한 비밀정보(Ex. 비밀키) 중 하나가 노출되더라도, 비밀정보를 이용하여 그 이후에 생성되는 세션키의 안전성에는 영향을 미칠 수 없어야 한다는 것을 뜻한다. 하지만 Chen 등의 인증 스킴은 완전 순방향 비밀성을 제공하지 못한다. 만약 악의적인 공격자가 비밀정보 중 하나인 $h(x_s||SID_n)$을 알고 있으면, 정상적인 인증과정에서 공개되는 공개정보인 ID_i와 T_i를 이용하여 세션키 $SK = h(ID_i||h(x_s||SID_n)||T_2)$를 계산해 낼 수 있는 것이다. 더욱이 공격자가 예전 사용자들의 정보인 ID_{pi}와 T_{p2}를 모두 저장하고 있었다면, 공격자는 예전에 사용한 세션키 SK_p를 모두 계산해낼 수도 있다. 그러므로 Chen 등이 제안한 인증 스킴은 완전 순방향 비밀성을 제공하지 못하여 취약한 부분이 존재한다[10,11].

[익명성 미보장] Chen 등이 제안한 인증 스킴에서는 사용자의 식별정보인 ID_i가 평문으로 전송되기 때문에 사용자의 인명성을 제공하지 못한다. 그래서 악의적인 공격자가 GW의 통신과정을 살펴보면 GW에 몇 명의 사용자가 GW에 등록되어 있는지 알아낼 수도 있으며 어떤 사용자와 S_n이 통신하는지도 알 수 있다. 그래서 민감한 정보를 다루는 무선 네트워크 환경에서는 이러한 익명성 미보장은 큰 문제가 될 수 있다[10,12].

[GW에 의한 세션키 노출] Chen 등이 제안한 인증 스킴에서는 세션키 SK를 이용하여 ID_i와 S_n이 비밀통신을 진행한다. 그러므로 SK는 당사자인 ID_i와 S_n만이 계산할 수 있어야 하지만, Chen 등의 스킴에서는 GW가 SK를 계산해 낼 수 있다는 문제가 있다. Chen 등의 스킴의 세션키 $SK = h(ID_i||h(x_s||SID_n)||T_2)$인데, GW는 인증과정에서 ID_i, x_s, SID_n, T_2를 모두 알아낼 수 있기 때문에 SK를 계산해낼 수 있다. 비록 GW가 신뢰할 수 있는 노드라고 하더라도 ID_i와 S_n만이 알아야하는 세션키를 계산해낼 수가 있다면, ID_i와 S_n 간의 비밀통신을 GW가 모두 복호화해낼 수 있다는 것은 문제점이다[10,11].

[패스워드 검사 미제공] Chen 등의 인증 스킴에서는 사용자의 스마트카드가 사용자의 패스워드를 검사하지 못하기 때문에 인증 과정과 패스워드 변경과정에서 문제가 발생한다. 인증과정에서는 스마트 카드가 사용자의 패스워드를 검사하지 않고 패스워드를 포함한 정보들을 이용하여 비밀키값 k를 계산한 후, k를 이용한 $A_i = E_k(ID_i||R_1||T_1)$를 활용하여 GW에서 패스워드를 검사하게 되는데 이때 GW에서는 시간정보 확인, 해쉬함수, 대칭키를 이용한 복호화 과정을 거쳐야 한다. 그러므로 악의적 공격자가 고의로 잘못된 패스워드를 연속적으로 입력한다면, GW의 서비스 과부 문제가 발생하게 된다. 또한, Chen 등이 제안한 스킴의 패스워드 변경과정에는 패스워드를 확인하는 절차가 없어서, 사용자가 기존의 패스워드와 새로운 패스워드를 입력하는 과정에서 Ui가 기존의 패스워드를 잘못 입력하게 되더라도 변경과정을 중단되지 않으며, 잘못된 N_i^* 값이 생성되어, 추후 인증과정에서 사용자가 정상적인 새로운 패스워드를 입력하더라도 GW가 인증하지 못하여 인증이 제대로 이루어지지 못하는 문제가 발생한다[10,12].

Ⅲ. 보안성이 향상된 사용자 인증 스킴

1. 변경사항 및 개선사항

Chen 등이 제안한 인증 스킴의 취약점이었던 완전 순방향 비밀성 미보장 문제를 해결하기 위해서 본 논문에서는 세션키 SK를 구성하는 요소를 수정하였으며, 익명성 미보장를 해결하기 위해서 일반 ID_i 대신 동적 사용자 ID인 DID_i 방식을 적용하였다. 그리고 GW에 의한 세션키 노출되는 문제는 타원곡선암호 중 ECDDHP (Elliptic Curve Decisional Diffie-Hellman Problem)을 이용하여 U_i와 S_n 만이 세션키를 계산할 수 있도록 하였고, 패스워드 검사를 제공하지 못하는 문제를 해결하기 위해서 퍼지추출 방식을 활용한 생체정보 인증기법을 적용하여서 스마트카드 분실 공격에 원천적인 취약점이 있는 패스워드 인증방식을 대체하였고 이를 통해 제안하는 인증 스킴은 패스워드 변경과정이 필요없게 되어 등록과정, 인증과정만으로 구성할 수 있게 되었다. 앞으로 설명할 제안하는 스킴의 등록과정, 인증과정, 그리고 4 장의 안전성 분석을 통해서 변경사항 및 개선사항을 상세히 살펴보겠다. 그리고 Chen 등의 스킴에서 설명한 수식 혹은 용어들은 추가적인 설명은 생략하며, 새롭게 사용된 것들에 관하여 설명을 추가하도록 하겠다.

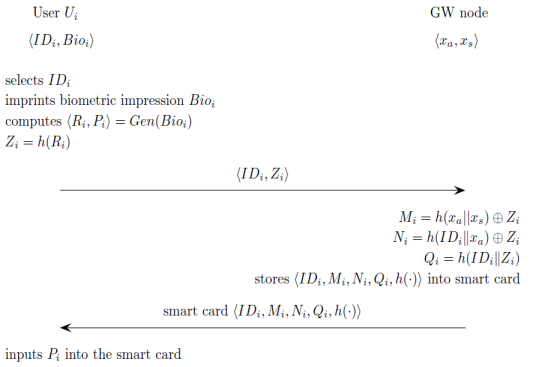

그림 1. 제안하는 스킴의 등록과정
Fig. 1. Registration phase of proposed scheme

2. 제안하는 스킴의 등록과정

(1) U_i는 자신의 식별정보 ID_i를 선택하고 생체정보 Bio_i를 장치를 통해 추출한다. 그리고 $Gen(Bio_i) = (R_i, P_i)$ 함수를 통하여 생체정보 Bio_i 에서 정규화된 랜덤 스트링 R_i과 헬퍼 스트링 P_i 를 생성한다. R_i은 Bio_i를 통해 항상 동일하게 생성되는 값이며 $R_i = Rep(Bio_i', P_i)$ 에서 사용자가 조금 다른 Bio_i' 를 입력하더라도 P_i 를 이용하여 정상적인 R_i 을 생성해낼 수 있다. 이때 Gen과 Rep 함수는 Generate와 Reproduce를 뜻한다. (2) 스마트 카드는 $Z_i = h(R_i)$를 계산하고 GW에게 ID_i 와 Z_i를 전송한다. (3) GW는 비밀정보인 x_a 및 x_s 과 사용자가 전송한 정보를 활용하여 $M_i = h(x_a||x_s) \oplus Z_i$, $N_i = h(ID_i||x_a) \oplus Z_i$, $Q_i = h(ID_i||Z_i)$를 생성한 후, 스마트 카드에 ID_i, M_i, N_i, Q_i, $h(\cdot)$를 저장한 후 스마트 카드를 사용자에게로 전달한다. (4) U_i 가 GW에게 전송받은 스마트 카드에 P_i 값을 추가적으로 저장하면 등록과정이 완료된다.

3. 제안하는 스킴의 인증과정

(1) U_i는 스마트카드를 장치에 장착하고 자신의 ID_i와 Bio_i^*를 입력한다. 스마트카드는 $R_i^* = Rep(Bio_i^*, P_i)$, $Z_i^* = h(R_i^*)$, $Q_i^* = h(ID_i||Z_i^*)$을 계산한 후, 스마트 카드에 저장된 Q_i와 새롭게 계산한 Q_i^*를 비교하여 일치여부를 확인한다. 그리고 스마트 카드는 타임스탬프 T_1을 생성한 후 스마트 카드에 저장된 N_i 값을 활용하여 대칭키 값인 $k = h((N_i \oplus Z_i^*)||T_1)$ 계산한다. 그리고 랜덤넘버 r_i를 생성하고 $X = r_i \times P$를 계산하고 $A_i = E_k(ID_i||X||T_1)$을 계산한다. 스마트카드는 M_i와 Z_i를 이용하여 $h(x_a||x_s) = M_i \oplus Z_i$를 계산한 후, 이를 이용하여 동적 ID_i인 $DID_i = ID_i \oplus h(x_a||x_s) \oplus T_1$을 계산한다. 그리고 스마트카드는 GW에게 $\{DID_i, A_i, X, T_1\}$을 전송한다.

(2) GW는 $\{DID_i, A_i, X, T_1\}$를 받은 후, 먼저 T_1를 $(T'_1 - T_1) \leq \Delta T$를 이용하여 T_1의 최신성을 확인한다. 그리고 $ID_i = DID_i \oplus h(x_a||x_s) \oplus T_1$ 를 통해 사용자의 ID_i를 계산하고 이를 이용하여 $k = h(h(ID_i||x_a)||T_1)$와 $D_k(A_i) = \{ID_i, R_1, T_1\}$를 계산한다. 그리고 GW는 복호화된 값인 ID_i 및 T_1가 전송받은 ID_i 및 T_1와 일치하는지를 확인한다. 그후 GW는 S_n과의 인증과정을 위하여 $B_i = h(h(x_s||SID_n)||X||SID_n||DID_i||T_2)$를 계산한다. 마지막으로 GW는 S_n에게 $\{ID_i, B_i, X, T_2\}$ 메시지를 전송한다.

(3) Sn은 $(T'_2 - T_2) \leq \Delta T$를 이용하여 T_2를 검증한 후, $B_i^* = h(h(x_s||SID_n)||SK||SID_n||ID_i||T_2)$를 계산하고 B_i와 B_i^* 이 일치여부를 확인한다. 그리고 S_n은 랜덤넘버 r_s를 생성하고 이를 이용하여 $Y = r_x \times P$ 와 $W_{su} = r_s \times X$ 를 계산하고 타임스탬프 T_3를 생성한다. 이를 이용하여 S_n은 $SK = h(DID_i||SID_i||h(x_a||x_s)||X||Y||W_{su}||T_3)$를 계산하여 U_i와 S_n 간의 세션키로 사용한다. S_n은 GW와의 인증을 위해 $C_i = h(h(x_s||SID_n)||Y||DID_i||SID_n||T_3)$를 계산한 후, GW에게 $\{C_i, Y, T_3\}$ 메시지를 전송한다.

(4) GW는 먼저 $(T'_3 - T_3) \leq \Delta T$ 이용하여 T_3를 검증하고 $C_i^* = h(h(x_s||SID_n)||SK||ID_i||SID_n||T_3)$를 계산한 후, 전송된 C_i와 C_i^* 이 동일한지 확인한다. GW는 자신의 타임스탬프 T_4를 생성하고 기존의 k값을 활용하여 암호화하여 $D_i = E_k(DID_i||SID_n||Y||T_3||T_4)$를 계산한 후에는 U_i에게 메시지 $\{D_i, Y, T_3, T_4\}$를 전송한다.

(5) U_i는 $(T'_4 - T_4) \leq \Delta T$를 이용하여 T_4의 최신성을 확인하고 $D_k(D_i)$를 이용하여 D_i를 복호화한 후, $\{DID_i, SID_n, Y, T_3, T_4\}$를 도출한다. 그리고 U_i는 기존의 값들 및 전송되어온 값이 복호화된 DID_i, Y, T_3, T_4 와 동일한지 검사한 후, 동일할 경우 U_i는 GW를 인증하게 되고 GW가 보내온 SID_n 값도 신뢰하게 된다. 그 후 U_i는 $W_{us} = r_i \times Y$를 계산한다. 이것은 S_n이 계산한 $W_{su} = r_s \times X$와 같은 값을 계산하게 되는데 그 이유는 $X = r_i \times P$ 이며 $Y = r_s \times P$ 이므로 $W_{us} = W_{su} = r_i \times r_s \times P$ 로 동일하게 된다. U_i은 $SK = h(DID_i||SID_i||h(x_a||x_s)||X||Y||W_{su}||T_3)$를 계산하여 세션키로 이용하기 때문에, U_i와 S_n은 인증과정 이후에는 세션키를 이용하여 암호화 통신을 할 수 있게 된다.

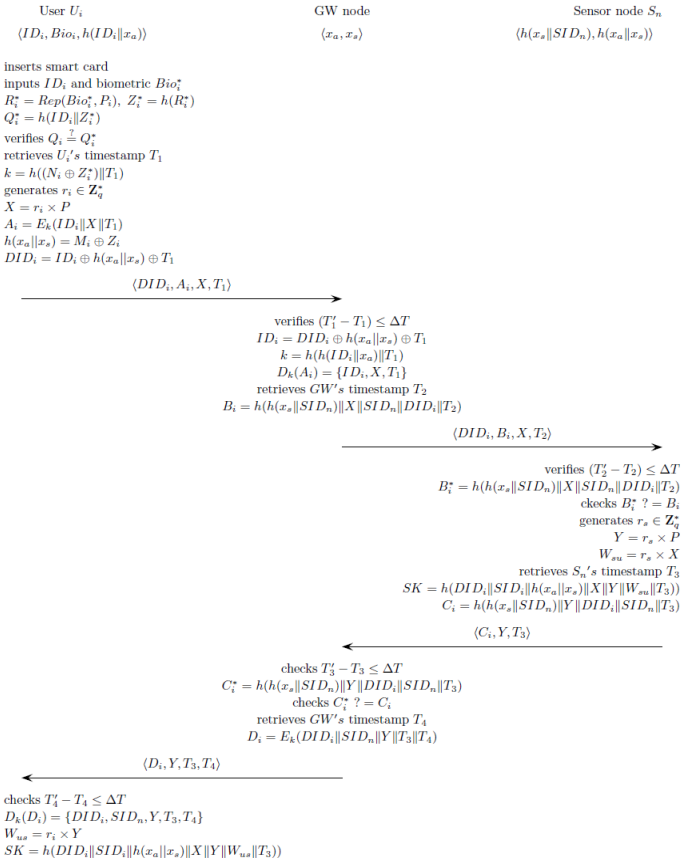

그림 2. 제안하는 스킴의 인증과정
Fig. 2. Authentication phase of proposed scheme

Ⅳ. 안전성 분석

1. 스마트카드 분실 공격

스마트카드 분실 공격이란 사용자가 자신의 스마트카드를 분실하거나 악의적인 공격자가 사용자의 스마트카드를 훔쳤을 때 발생할 수 있는 정보 누출 혹은 정보를 이용한 악의적인 행동을 뜻한다. 제안하는 스킴에서는 스마트카드에 {ID_i, M_i, N_i, Q_i, h(·)}가 저장되어 있어서 고급 기술을 가진 공격자는 전력분석 혹은 차분공격을 통해 스마트카드 안에 저장된 내용을 추출해낼 수 있다. 하지만 본 논문에서 제안하는 스킴의 스마트카드 안에 비밀정보는 $h(x_a||x_s)$와 x_a인데 $M_i=h(x_a||x_s)\oplus Z_i$, $N_i=h(ID_i||x_a)\oplus Z_i$ 처럼 U_i의 생체정보가 있어야 계산해낼 수 있는 값 [$Gen(Bio_i) = (R_i, P_i)$, $Z_i = h(R_i)$]이기 때문에 모두 사용자의 생체정보를 알아야 계산해 낼 수 있기에, 공격자는 추출한 ID_i 값만을 이용해서는 비밀정보를 알아낼 수 없으며 스마트카드 분실 공격을 진행할 수 없다.

2. 완전 순방향 비밀성 보장

본 논문에서 제안하는 스킴에서의 세션키는 $SK = h(DID_i||SID_i||h(x_a||x_s)||X||Y||W_{su}||T_3)$로 구성되어 있다. 그래서 악의적인 공격자가 비밀정보 중 x_a, x_s 중 하나만 알아서는 SK를 도출해낼 수 없으며, $h(x_a||x_s)$를 알아내더라도 $W_{su} = r_i \times r_s \times P$를 계산해낼 수 없어 세션키를 도출해 낼 수가 없다. 그래서 제안하는 스킴에서는 중요한 비밀정보 중 하나가 노출되더라도, 비밀정보를 이용하여 생성되는 세션키의 안전성에는 영향을 미칠 수 없기 때문에 완전 순방향 비밀성을 보장하고 있다.

3. 익명성

제안하는 스킴에서는 ID_i가 통신과정에서 평문으로 전송되지 않는다. $DID_i = ID_i \oplus h(x_a||x_s)\oplus T_1$를 이용하여

ID를 포함한 동적 ID 정보를 전송함으로써, 인증과정의 합법적인 구성원만이 ID_i를 추출하여 신원확인 및 대칭키 생성에 사용할 수 있다. 악의적인 공격자는 통신과정에서 수집한 DID_i 만을 가지고는 ID_i를 계산해 낼 수 없다. 그건 $h(x_a||x_s)$ 값이 생체정보와 스마트카드를 소유한 정상적인 사용자와 GW, S_n 만이 알 수 있는 정보이기 때문이다. 그리고 특히, DID_i에는 타임스탬프 T_1 정보가 포함되어 매번 변경되기에 악의적인 공격자가 GW의 통신과정을 살펴보더라도 GW에 몇 명의 사용자가 GW에 등록되어 있는지 알아낼 수 없으며 어떤 사용자와 S_n이 통신하는지도 알 수 없으므로 익명성이 보장되고 있다.

4. 세션키 안전성

(1) 세션키는 실제로 암호화 통신을 진행할 구성원만 계산해낼 수 있어야한다. 하지만 Chen 등이 제안하는 인증 스킴에서는 암호화 통신을 진행하는 U_i와 S_n 뿐만 아니라 GW도 세션키를 계산할 수 있는 문제가 있었다. 하지만 본 논문에서 제안하는 인증 스킴의 세션키는 $SK = h(DID_i||SID_i||h(x_a||x_s)||X||Y||W_{su}||T_3)$로 구성되어 있어서 U_i와 S_n만이 세션키를 계산해 낼 수 있다. 악의적인 공격자는 $h(x_a||x_s)$와 W_{su}를 알아낼 수 없기 때문에 세션키를 계산해 낼 수 없으며, 많은 정보를 가진 GW라도 W_{su}를 알 수 없기 때문에 세션키를 계산해 낼 수 없다. 그 이유는 $X = r_i \times P$ 및 $Y = r_s \times P$ 은 공개된 정보지만 $W_{us} = W_{su} = r_i \times r_s \times P$ 이기 때문에, W_{su} 및 W_{us}는 Y 와 r_i를 아는 U_i, 그리고 X와 r_s를 아는 S_n만이 계산해 낼 수 있기 때문이다. 그래서 본 스킴에서는 ID_i와 S_n 간의 세션키를 이용한 비밀통신은 악의적 공격자뿐만 아니라 신뢰성이 높은 GW라도 복호화해낼 수 없어서 안전하다.

5. 사용자 인증 단계의 오류를 통한 공격

Chen 등이 제안한 인증 스킴에서는 사용자의 스마트카드가 사용자의 패스워드를 검사하지 못하기 때문에 인증 과정과 패스워드 변경과정에서 악의적인 공격자가 고의적으로 잘못된 패스워드를 입력해서 GW의 서비스를 방해하는 문제와 잘못된 패스워드로 변경되더라도 확인이 안되는 문제가 발생하였다. 그리고 패스워드를 이용한 방식은 패스워드 노출에 대한 근본적인 문제를 가지고 있기 때문에 본 논문에서는 패스워드가 아닌 생체정보를 활용한 인증 방식으로 변경하였다. 생체정보를 통한 인증은 약간의 생체정보의 변화에서 인증오류가 발생하는 일이 발생하거나, 잘못된 생체정보를 인증하는 문제가 발생할 수 있다. 이러한 문제를 보완하기 위해서 본 스킴에서는 퍼지추출 기술을 이용한 생체정보 인증을 추가하여 사용자 인증의 정확성을 높혔다. 그건 퍼지추출 기술을 활용한 함수 $R_i = Rep(Bio_i', P_i)$을 이용하여 사용자가 조금 다른 Bio_i' 를 입력하더라도 P_i 를 이용하여 정상적인 R_i 을 생성해낼 수 있기 때문이다. 또한 패스워드를 사용하지 않기 때문에 패스워드 변경과정이 없으며, 스마트 카드 안에도 패스워드 정보를 저장하고 있지 않기 때문에 스마트 카드로 인한 정보의 노출이 방지할 수 있다. 그리고 잘못된 패스워드 입력으로 인한 인증 오류 및 GW의 서비스 과부하 문제도 방지할 수 있다.

V. 결 론

본 논문에서는 Chen 등이 제안한 스마트 카드 분실 공격에 안전한 사용자 인증 스킴에 대한 취약점을 분석하여 완전 순방향 비밀성 미보장, 익명성 미보장, GW에 의한 세션키 노출, 패스워드 검사 미제공의 문제가 있다는 것을 지적했다. 이를 해결하기 위해 ECDDHP, 퍼지추출 기술, 동적 ID 기술을 활용하여서 보안성이 향상된 인증 스킴을 제안하고 스킴의 안전성을 분석하여, 본 논문에서 제안한 스킴이 스마트 카드 분실 공격뿐만 아니라, 다양한 공격에 안전하다는 것을 증명하였다.

References

[1] Eunju Kim, Jong-Woong Park, Sung-Han Sim, Development of Wireless Smart Sensing Framework for Structural Health Monitoring of High-speed Railway Bridges, Journal of the Korea Academia-Industrial cooperation Society, Vol. 17, No. 5 pp. 1-9, 2016 DOI: http://dx.doi.org/10.5762/KAIS.2016.17.5.1

[2] Sunho Kim, Kangwoo Lee, Yonghee Lee, A study on implementation of standard protocol for communication of health signals in mobile environment, The Journal of The Institute of Internet, Broadcasting and Communicatioin, Vol. 16, No. 5, pp.125-129, Oct. 31, 2016. DOI: http://dx.doi.org/10.7236/JIIBC.2016.16.5.125

[3] Young-Do Joo, Analysis on Security Vulnerabilities of a Biometric-based User Authentication Scheme for Wireless Sensor Networks, The Journal of The Institute of Internet, Broadcasting and Communication, VOL. 14 No. 1, pp.147-153, Feb. 28, 2014.
DOI: http://dx.doi.org/10.7236/jiibc.2014.14.1.147

[4] Young-Hwa An, Young-Do Joo, Security Enhancement of Biometrics-based Remote User Authentication Scheme Using Smart Cards, The Journal of The Institute of Internet, Broadcasting and Communication, VOL. 12 No. 1, pp.231-237, Feb. 28, 2012.
DOI: http://dx.doi.org/10.7236/jiwit.2012.12.1.231

[5] M. L. Das, "Two-factor user authentication in wireless sensor networks" IEEE Transactions on Wireless Communications, vol. 8, no. 3, pp. 1086 - 1090, 2009.
DOI: http://dx.doi.org/10.1109/twc.2008.080128

[6] M. K. Khan and K. Alghathbar, "Security analysis of 'two-factor user authentication in wireless sensor networks'," in Advances in Computer Science and Information Technology, vol. 6059 of LNCS, pp. 55 - 60, Springer, Germany, 2010.
DOI: http://dx.doi.org/10.1007/978-3-642- 13577-4_5

[7] J. J. Yuan, "An enhanced two-factor user authentication in wireless sensor networks," Tele communication Systems, vol. 55, no. 1, pp. 105 - 113, 2014.
DOI: http://dx.doi.org/10.1007/s11235-013-9755-5

[8] H. L. Yeh et al. "A secured authentication protocol for wireless sensor networks using Elliptic Curves Cryptography," Sensors, vol. 11, no. 5, pp. 4767 - 4779, 2011.10.
DOI: http://dx.doi.org/10.3390/s110504767

[9] L. Chen, W. Fushan, and M. Chuangui, "A Secure User Authentication Scheme against Smart-Card Loss Attack for Wireless Sensor Networks Using Symmetric Key Techniques," International Journal of Distributed Sensor Networks, 2015.
DOI: http://dx.doi.org/10.1155/2015/704502

[10] Younsung Choi, Youngsook Lee and Dongho Won, Cryptanalysis on Symmetric Key Techniques based Authentication Scheme for Wireless Sensor Networks, CSA 2015 (Cebu) Springer, LNEE 373, pp. 7-13, 2015.12.15.
DOI: http://dx.doi.org/10.1007/978-981-10-0281-6_2

[11] Younsung Choi, Junghyun Nam, Donghoon Lee, Jiye Kim, Jaewook Jung and Dongho Won, Security Enhanced Anonymous Multi-Server Authenticated Key Agreement Scheme Using Smart Cards and Biometrics, The Scientific World Journal, Vol.2014,
DOI: http://dx.doi.org/10.1155/2014/281305

[12] Younsung Choi, Donghoon Lee, Jiye Kim, Jaewook Jung, Junghyun Nam and Dongho Won "Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography" Sensors, vol. 14, no. 6, pp. 10081-10106, 2014.
DOI: http://dx.doi.org/10.3390/s140610081

저자 소개

최 윤 성(정회원)

- 2006년 2월 : 성균관대학교 정보통신공학부 학사
- 2007년 8월 : 성균관대학교 전자전기컴퓨터공학부 석사
- 2010년 6월 ~ 2013년 5월 : 육군3사관학교 정보공학과 조교수
- 2015년 8월 : 성균관대학교 전자전기컴퓨터공학부 박사
- 2015년 9월 ~ 2016년 2월 : 성균관대 IT융합원 박사후과정
- 2016년 3월 ~ 현재 : 호원대학교 사이버수사보안학부 조교수

<주관심분야 : 취약점 분석, 정보보안, 디지털포렌식>

※ 본 논문은 2016학년도 호원대학교 교내학술연구비의 지원으로 작성되었습니다.