http://dx.doi.org/10.7236/JIIBC.2014.14.1.147
JIIBC 2014-1-20

무선 센서 네트워크를 위한 생체 정보 기반 사용자 인증 스킴의 보안 취약점 분석

Analysis on Security Vulnerabilities of a Biometric-based User Authentication Scheme for Wireless Sensor Networks

주영도*

Young-Do Joo*

요 약 스마트카드를 사용하는 원격 사용자 인증 스킴은 일반적으로 패스워드를 기반으로 하여 연구되었고, 지속적으로 보안성을 강화하는 개선안들이 제시되어 왔다. 최근 생체인식 기술의 발달과 함께, 다양한 인간 생체정보(biometrics)를 비밀키 값으로 사용하는 생체정보 기반 사용자 인증 스킴들이 소개되면서, 전통적인 패스워드 기반 인증 스킴보다 상대적으로 안전성과 편리성이 향상된 접근 방법으로 부상하고 있다. 한편 유비쿼터스 시대의 도래와 함께 핵심 기술이 되는 무선 센서 네트워크에 대한 관심이 증대되고 있다. 센서 노드를 이용하여 정보를 수집 처리하는 무선 센서 네트워크는 사회전반으로 응용분야가 확대됨과 동시에 네트워크의 구조적인 보안을 비롯한 다양한 보안 요구사항을 요구한다. 따라서 무선 센서 네트워크 응용계층에서 요구되는 사용자 인증에 대한 연구 또한 서서히 진행되고 있다. 2010년 Yuan 등은 생체정보를 기반으로 무선 센서 네트워크에 적용 가능한 효과적인 사용자 인증 스킴을 제안하였다. 본 논문은 안전성 분석을 통해 Yuan 등의 스킴이 그들의 주장과 달리 여전히 패스워드 추측 공격, 사용자 가장 공격 및 재전송 공격에 취약함을 입증한다.

Abstract The numerous improved schemes of remote user authentication based on password have been proposed in order to overcome the security weakness in user authentication process. Recently, some of biometric-based user authentication schemes to use personal biometric information have been introduced and they have shown the relatively higher security and the enhanced convenience as compared to traditional password-based schemes. These days wireless sensor network is a fundamental technology in face of the ubiquitous era. The wireless sensor networks to collect and process the data from sensor nodes in increasing high-tech applications require important security issues to prevent the data access from the unauthorized person. Accordingly, the research to apply to the user authentication to the wireless sensor networks has been under the progress. In 2010, Yuan et al. proposed a biometric-based user authentication scheme to be applicable for wireless sensor networks. Yuan et al. claimed that their scheme is effectively secure against the various security flaws including the stolen verifier attack. In this paper, author will prove that Yuan et al.'s scheme is still vulnerable to the password guessing attack, user impersonation attack and the replay attack, by analyzing their security weakness.

Key Words : Authentication Scheme, Biometrics, Wireless Sensor Network, Password Guessing Attack, Impersonation Attack

*정회원, 강남대학교 컴퓨터미디어정보공학부 (교신저자)
접수일자 : 2014년 1월 13일 , 수정완료 : 2014년 2월 2일
게재확정일자 : 2014년 2월 7일

Received: 13 January, 2014 / Revised: 2 February, 2014
Accepted: 7 February, 2014
*Corresponding Author: ydjoo@kangnam.ac.kr
Dept. of Computer and Media Information, Kangnam University, Korea

Ⅰ. 서 론

최근에 무선 센서 네트워크(WSN: Wireless Sensor Network)는 실시간 교통관제, 물류/유통, 지진 측정, 방재 및 환경 등의 다양한 사회분야에 적용될 수 있는 광범위한 응용분야로 확대되고 있다. 무선 센서 네트워크는 적은 메모리, 배터리 용량의 제한, 컴퓨팅 성능의 제약 등 제한적인 하드웨어 자원을 가진 수많은 센서 노드들이 무선통신으로 거미줄처럼 연결된 네트워크로서, 사람 또는 주위의 사물을 인식하고 이들 간 네트워크를 구성하여 위치정보를 파악하여 다양한 통신 목적으로 활용되고 있다. WSN 상의 센서 노드들은 특정 노드를 구분하기 위하여 자신이 제공할 수 있는 데이터에 의해서 지칭된다. 이를 위해서 사용자는 속성기반의 네이밍(attributue based naming)을 이용하여 쿼리(query)를 기술하고 쿼리를 센서 노드에 전송한다. 여기서 속성이란 감시하려는 개체의 특징, 감시대상의 지리정보, 감시 주기 등을 의미한다. 이러한 속성들에 원하는 값을 지정하여 쿼리를 만들어 센서 노드들에게 배포한다. 수신된 쿼리와 일치하는 이벤트를 감지한 노드들만이 데이터를 게이트웨이 노드(Gateway Node)로 전송함으로써 데이터를 전송해야 할 노드들을 그 이외의 다른 노드들과 구분할 수 있게 된다[1]. 그림 1은 무선 센서 네트워크의 계층적 구조의 한 예를 보여주고 있다.

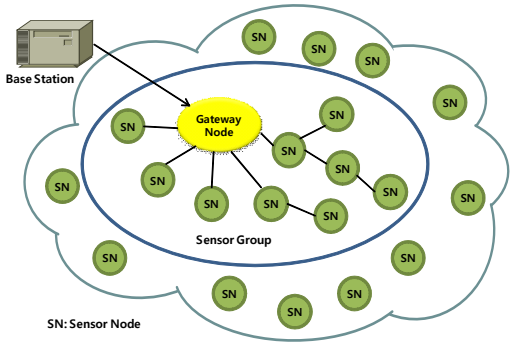

그림 1. 무선 센서 네트워크의 계층적 구조
Fig. 1. Hierarchical Architecture of Wireless Sensor Network

따라서 무선 센서 네트워크에서 수집되는 중요한 기밀 데이터를 허가받지 않은 사용자가 무단으로 획득하는 것을 막기 위한 스마트카드 기반 사용자 인증은 주요한 보안 요구사항으로 등장하고 있다. 일반적으로 사용자 인증은 패스워드 기반으로 보안성을 제공한다. 패스워드 기반의 다양한 사용자 인증 스킴들이 지속적으로 연구되고 개선안이 제안되어 왔으나 여전히 부주의한 패스워드 관리와 고도화된 해킹 공격 기술에 의해 보안상 약점을 무결하게 극복하는 것은 어려운 상황이다. 따라서 최근에 패스워드에 의존하는 사용자 인증의 문제점을 해결하기 위하여 패스워드와 함께 생체정보(biometrics)를 이용하는 사용자 인증 스킴들이 고안되어 사용되고 있다[2-6]. 개인의 생체정보는 지문, 얼굴, 홍채, 망막, 손장문, 정맥 등의 인식을 통해 획득되는 개인의 신체적인 특성을 의미한다. 전통적인 패스워드 기반 인증과 비교하여, 생체정보 키(biometric key)를 사용하는 생체인식 기반 인증은 보다 안전하고 신뢰성 높은 보안상의 장점을 보여준다. 생체인식에 의한 생체정보 키는 특성상 분실, 복제, 도용, 누출 및 배포 등에 따른 보안성이 탁월하게 우수하며, 패스워드처럼 외울 필요가 없으므로 상대적으로 사용자의 편리성을 만족시킨다.

최근에 무선 센서 네트워크의 보안 요구사항과 관련된 인증 기능에 생체정보를 기반으로 한 사용자 인증 방법이 도입되어 소개되고 있다. 2010년 Yuan[7] 등은 생체정보 키를 사용하여 무선 센서 네트워크 응용분야에 적용 가능한 원격 사용자 인증 스킴을 소개하였다. Yuan 등은 별도의 인증 및 패스워드 테이블을 유지함이 없이 그들의 스킴이 패스워드 추측 공격(password guessing attack), 사용자 가장 공격(user impersonation attack), 및 재전송 공격(replay attack)등에 안전하다고 주장하였다. 본 논문은 Yuan 등의 스킴의 안전성을 분석하여 제안된 스킴이 패스워드 추측 공격, 사용자 가장 공격과 재전송 공격에 취약함을 갖고 있음을 밝혀낸다.

본 논문의 구성은 다음과 같다. 2장에서는 생체정보 기반의 사용자 인증과 무선 센서 네트워크의 사용자 인증에 대한 관련 연구를 살펴본다. 3장에서는 Yuan 등이 제안한 스킴을 고찰하고 4장에서는 Yuan 등의 스킴이 갖고 있는 보안상 취약점을 분석한다. 마지막으로 5장에서 간략히 결론을 맺는다.

Ⅱ. 관련 연구

스마트카드를 이용하여 원격지에 있는 사용자를 인증하는 연구는 1980년 초 Lamport[8]의 제안 이후 보안성과

효율성을 향상시키며 지속적으로 개선되어 왔다. 초기의 연구들은 패스워드 기반의 사용자 인증이 중심이 되었고 패스워드 인증 테이블을 인증서버에 저장하는 방법으로 제안되었다. 여러 가지 개선된 스킴의 등장에도 불구하고 패스워드 기반의 사용자 인증은 부분적으로 보안 취약점을 갖고 있어 다양한 해킹 공격에 노출되는 단점을 보였다[9-14].

2000년 이후 등장한 생체인식 기반의 사용자 인증 스킴은 이러한 패스워드만을 사용하는 인증 스킴들과 비교하여 보안과 편리성에 있어 신뢰성 높은 접근 방법으로 평가된다. Lee[2] 등은 지문 인식 기반의 스마트카드 사용자 인증 방법을 제시하였다. 하지만 그들의 스킴은 사용자 가장 공격을 막을 수 없는 약점을 갖고 있다. 이후 Li[4] 등은 보다 효율적인 생체인식 기반의 사용자 인증 스킴을 제시하면서, 자기들의 스킴이 자유로운 패스워드 변경, 상호인증 및 부인 방지 등을 제공하는 우수성을 주장하였다. 그러나 Das[6]는 Li 등의 스킴이 생체정보 인증상의 취약성을 비롯한 보안상의 문제가 있음을 보여주었고, 개선된 스킴을 소개하였다. 그러나 Das의 스킴 또한 패스워드 추측공격 및 사용자 가장 공격에 약점을 갖고 있는 것으로 나타났다.

한편 2000년대 초부터 무선 센서 네트워크(WSN)의 보안과 관련된 다양한 연구가 시작되었다. 보안기능과 관련된 암호 알고리즘, 키 관리, 보안 프로토콜, 인증, 시큐어 라우팅 등의 많은 연구가 WSN의 링크 계층과 네트워크 계층에서 활발하게 진행되었으며, WSN 응용계층에 요구되는 사용자 인증은 효과적으로 다루어지지 못했다[15-17]. Watro[18] 등은 RSA와 Diffie-Hellman 알고리즘을 기반으로 한 공개키(public key) 기술을 이용하여 WSN을 위한 사용자 인증 프로토콜을 제안하였다. Watro 등의 스킴에서 공격자는 사용자의 공개키를 획득하여 다른 패러미터 값들과 함께 세션 키를 암호화하여 사용자에게 보내게 되는 경우, 사용자는 암호된 메시지가 센서 노드로부터 온 것으로 믿고 자신의 사설키(private key)로 메시지를 해독하게 된다. 따라서 Watro 등의 스킴에서 공격자가 세션 키를 이용하여 수행하는 임의의 공격을 막는 것이 불가능하다. Wong[19] 등은 WSN에 적용하기 위해 해쉬함수를 활용한 패스워드 기반의 사용자 인증 프로토콜을 제안하였다. 그러나 Wong 등의 스킴은 게이트웨이 노드와 로그인 노드가 등록된 사용자의 패스워드와 아이디를 위한 테이블을 유지해야 하므로, 인증 테이블이 도난(stolen-verifier attack)되었을 경우에 다양한 해킹 공격에 노출되는 치명적인 단점을 갖고 있다.

2010년 Yuan[7] 등은 Wong 등의 스킴이 갖고 있는 보안 취약점인 stolen-verifier 공격을 견디어 낼 수 있는 사용자 인증 방법을 제시하였다. Yuan 등은 생체정보 키와 해쉬함수를 사용하여 다른 스킴에 비해 상대적으로 높은 보안성을 시도하였다.

Ⅲ. Yuan 등의 인증 스킴 고찰

이 장에서는 2010년에 Yuan 등이 제안한 WSN에 적용 가능한 생체인식 기반 사용자 인증 스킴을 살펴본다. Yuan 등의 스킴은 등록 단계(registration phase), 로그인 단계(login phase), 인증 단계(authentication phase), 그리고 패스워드 변경 단계(password change phase)에 걸친 4개의 단계로 구성된다. 표 1은 본 논문에서 사용된 약어표기 및 정의를 요약한 것이다.

표 1. 약어 표기 및 정의
Table 1. Abbreviation Notation and Definition

표기	정의
U_i	사용자 (User i)
GW-Node	WSN의 게이트웨이 노드
ID_i	사용자 i의 아이디
PW_i	사용자 i의 패스워드
B_i	사용자 i의 생체 정보
S	GW-Node의 비밀키 값
h()	단방향 해쉬(hash) 함수
$x \oplus y$	x 와 y에 대한 Exclusive-OR 연산
$x \| y$	x 와 y에 대한 Concatenation 연산

■ 등록 단계

이 단계는 사용자 U_i가 센서 네트워크로부터 데이터를 액세스하기 전에 네트워크상에 있는 게이트웨이 노드에 등록을 하기 위해 실행되며, 다음의 과정을 수행한다.

(1) 사용자 U_i는 자신의 생체정보 B_i를 특정한 장치에 입력하고 자신이 아이디 ID_i와 패스워드 PW_i를 안전한 채널을 이용하여 게이트웨이 노드에 제공한다.

(2) 사용자의 등록요청을 수신한 게이트웨이 노드는 식 (1)에 의해 R_i를 계산한다.

$R_i = h(ID_i \| PW_i \| E_i) \oplus h(S)$ (1)

여기서 $E_i=h(B_i)$이며 S는 게이트웨이 노드에게만 알려져 있는 비밀 키 값이다.

(3) 게이트웨이 노드는 개별정보 ID_i, R_i, $h(PW_i)$, E_i, X를 저장한 스마트카드를 안전한 채널을 통해 사용자 U_i에게 발급한다. 여기서 X는 게이트웨이 노드에서 생성되고 일부 지정된 센서 노드들에게 저장되는 비밀 패러미터 값이다. X 값을 알고 있는 지정 센서 노드들은 사용자들과 데이터를 교환하는 일을 담당한다.

■ 로그인 단계

사용자 U_i가 WSN으로부터 데이터를 액세스하기 원할 때 로그인 단계가 실행되며, 다음의 과정을 수행한다.

(1) 사용자는 발급받은 스마트카드를 카드 리더기에 넣고 자신의 생체정보를 검증하기 위하여 생체정보 B_i를 특정한 장치에 입력한다.

(2) 사용자는 $E_i^*= h(B_i)$를 계산하고 스마트카드로부터 E_i를 읽어온다. E_i^*와 E_i의 값이 다를 경우 사용자는 생체정보 검증을 통과하지 못하고 사용자 인증에 실패한다. 반면에 두 개의 값이 동일한 경우에 사용자는 올바른 ID_i와 PW_i를 입력하여 다음의 과정을 계속한다.

(3) 스마트카드는 식 (2)와 (3)에 의해 D_i와 M_i를 계산한다.

$D_i = h(ID_i \| PW_i \| E_i) \oplus h(X \| T)$ (2)

$M_i = h(R_i \| X \| T)$ (3)

여기서 T는 현재의 시간을 나타내는 타임스탬프(timestamp)이다.

(4) 사용자는 메시지 $\{D_i, M_i, T\}$를 게이트웨이 노드에 전송한다.

■ 인증 단계

로그인 요청 메시지를 수신한 게이트웨이 노드는 사용자 U_i를 인증하기위해 다음 과정을 수행한다.

(1) 게이트웨이 노드는 T와 T^* 간의 시간 차이의 유효성을 검증한다. 여기서 T^*는 게이트웨이 노드가 로그인 요청 메시지를 받은 시점의 타임스탬프이다. 즉 ΔT값이 WSN의 전송지연의 예상시간 간격이라고 정의하면, $(T^*-T) > \Delta T$인 경우에 사용자 인증은 실패한다. 한편 $(T^*-T) \leq \Delta T$이면 다음 단계를 계속 수행한다.

(2) 게이트웨이 노드는 식 (4)와 (5)에 의해 L_i와 M_i^*를 계산한다.

$L_i = D_i \oplus h(X \| T)$ (4)

$M_i^* = h((L_i \oplus h(S)) \| X \| T)$ (5)

(3) 만약 계산된 값 M_i^*가 M_i와 같다면 게이트웨이 노드는 로그인 요청을 받아들인다. 아닌 경우에는 로그인 요청은 거절된다.

(4) 다음에 게이트웨이 노드는 식 (6)과 같이 Y_i를 계산한다.

$Y_i = h(D_i \| I_n \| X \| T_g)$ (6)

여기서 I_n은 사용자 U_i의 쿼리에 응답하는 센서 노드를 지칭한다. T_g는 게이트웨이 노드의 현재 시간을 나타내는 타임스탬프이다. 게이트웨이 노드는 공개된 채널을 통해 메시지 $\{D_i, Y_i, T_g\}$를 센서 노드 I_n에 전송한다. 하지만, Y_i 값이 I_n과 게이트웨이 노드가 알고 있는 비밀 값 X에 의해 생성되기 때문에, I_n은 메시지 $\{D_i, Y_i, T_g\}$가 적법한 게이트웨이 노드로부터 전달된 것임을 확신한다.

(5) 센서 노드 I_n은 유사한 방법으로 T_g에 대한 시간 차이가 유효한지 검증한다. 그 다음, $h(D_i \| I_n \| X \| T_g)$를 계산하여 Y_i와 동일한 값인지를 확인한다. 위의 두 가지 검증을 통과하게 되는 경우 마침내 센서 노드 I_n은 사용자 U_i의 쿼리에 응답하여 게이트웨이 노드에 데이터를 전송한다.

■ 패스워드 변경 단계

이 단계는 사용자가 자신의 패스워드를 변경하고자 할 때 실행되며 다음의 과정을 수행한다.

(1) 사용자 U_i는 스마트카드를 카드 리더기에 넣고, 자신의 생체정보를 입력하여 생체정보 B_i 검증을 통과하게 되면 자유롭게 패스워드를 바꿀 수 있다. 다시 말해 $E_i=h(B_i)$인 경우에 사용자는 자신의 이전 패스워드 PW_i와 새로운 패스워드 PW_i^*를 입력한다.

(2) 스마트카드는 식 (7), (8), (9)에 의해 다음을 계산한다.

$a_1 = h(ID_i \| PW_i \| E_i)$ (7)

$a_2 = a_1 \oplus R_i = h(S)$ (8)

$R_i^* = h(ID_i \| PW_i^* \| E_i) \oplus a_2$ (9)

궁극적으로, 스마트카드는 R_i와 $h(PW_i)$를 R_i^*와 $h(PW_i^*)$로 각각 변경한다.

Ⅳ. Yuan 등의 스킴의 보안 취약점 분석

Yuan 등의 인증 스킴에 대한 안전성을 분석하기 위해, Kocher[20] 등과 Messerges[21] 등의 연구를 통해 입증된 바와 같이 공격자는 합법적인 사용자로 가장하여 스마트 카드에 저장된 정보들을 전력소비를 모니터링함으로 불법적으로 추출할 수 있다고 가정한다. 이에 따라 누출된 정보를 바탕으로, 사용자와 게이트웨이 노드가 상호 통신하는 메시지가 공격자에 의해 위조될 수 있다. 이 장에서는 Yuan 등의 인증 스킴이 다음에 기술할 패스워드 추측 공격, 사용자 가장 공격 및 재전송 공격에 보안 취약성을 갖고 있음을 증명한다.

■ 패스워드 추측 공격

일반적으로 대부분의 사용자들은 편리성 때문에 쉽게 기억되는 패스워드를 선택하는 경향이 있다. 그러나 이러한 패스워드는 잠재적으로 패스워드 추측 공격(password guessing attack)에 취약하다. 본 연구에서 가정한 바와 같이 공격자는 적법한 사용자의 스마트카드에 저장된 비밀정보를 추출할 수 있다. 공격자는 등록단계에서 게이트웨이 노드가 발급한 사용자의 스마트카드로부터 $h(PW_i)$를 획득할 수 있다. 획득한 $h(PW_i)$를 이용하여 오프라인 패스워드 추측 공격 시도가 가능하게 된다. 즉 사용자의 올바른 패스워드 PW_i를 찾아내기 위하여 공격자는 $h(PW_i) = h(PW_i^*)$ 인지를 확인함으로, 추측하는 패스워드 PW_i^*가 정확한지를 검증한다. 공격자는 사용자의 패스워드를 찾을 때까지 PW_i^*를 계속 바꾸면서 검증을 반복 수행한다. 궁극적으로 사용자의 정확한 패스워드 PW_i를 찾아낼 수 있다.

■ 사용자 가장 공격(1)

사용자 가장 공격(user impersonation attack)의 첫 번째 유형은 공격자가 적법한 사용자의 스마트카드로부터 등록단계에서 저장된 비밀 정보, ID_i, R_i, E_i, X를 불법으로 추출하고, 패스워드 추측공격에서 성공적으로 획득한 패스워드 PW_i^*를 사용하여 다음과 같이 공격을 수행하는 것이다.

(1) 공격자는 식 (10)과 (11)에 의해 D_i^*와 M_i^*를 계산한다.

$$D_i^* = h(ID_i \| PW_i^* \| E_i) \oplus h(X \| T^*) \quad (10)$$

$$M_i^* = h(R_i \| X \| T^*) \quad (11)$$

여기서 T^*는 현재의 시간을 나타내는 타임스탬프이다.

(2) 그리고 나서 공격자는 위조된 메시지 $\{D_i^*, M_i^*, T^*\}$를 게이트웨이 노드에 전송하여 로그인 요청을 시도한다.

(3) 위조된 로그인 요청 메시지를 받은 게이트웨이 노드는 T^*와 T^{**} 간의 시간 차이의 유효성을 검증한다. 여기서 T^{**}는 게이트웨이 노드가가 로그인 요청 메시지를 받은 시점의 타임스탬프이다. $(T^{**}-T^*) \leq \Delta T$가 만족되므로 공격은 계속 수행된다.

(4) 게이트웨이 노드는 식 (12)와 (13)에 의해 L_i^*와 M_i^{**}를 계산한다.

$$L_i^* = D_i^* \oplus h(X \| T^*) \quad (12)$$

$$M_i^{**} = h((L_i^* \oplus h(S)) \| X \| T^*) \quad (13)$$

(5) 만약 계산된 값 M_i^{**}가 M_i^*와 같다면 게이트웨이 노드는 로그인 요청을 받아들인다. 궁극적으로 게이트웨이 노드는 공격자를 적법한 사용자로 인증하게 되고, 게이트웨이 노드와 센서 노드 간의 인증단계를 통해 센서 노드는 공격자의 쿼리에 응답하게 됨으로 공격 목적을 달성한다.

■ 사용자 가장 공격(2)

사용자 가장 공격의 두 번째 유형은 첫 번째 유형과 같이 사용자의 스마트카드로부터 비밀 정보, ID_i, R_i, E_i, X를 불법으로 추출한 다음, 불법으로 획득한 PW_i^*를 통해 아래의 과정에서 나타난 바와 같이 비밀정보를 구하고, 이어서 공격자가 임의로 선택한 어떠한 패스워드를 사용하여도 공격을 시도할 수 있는 경우에 해당한다.

(1) 공격자는 스마트카드로부터 추출한 정보에 의해 식 (14)와 같이 비밀정보 $h(S)^*$를 구해낸다.

$$h(S)^* = h(ID_i \| PW_i^* \| E_i) \oplus R_i \quad (14)$$

(2) 그리고 $h(S)^*$를 이용하여 임의의 패스워드 PW_i'에 대하여 식 (15)와 같이 R_i'를 계산할 수 있다.

$$R_i' = h(ID_i \| PW_i' \| E_i) \oplus h(S)^* \quad (15)$$

(3) 이제부터 임의의 패스워드 PW_i'를 사용하여 공격자는 식 (16)과 (17)과 같이 D_i'와 M_i'를 계산한다.

$$D_i' = h(ID_i \| PW_i' \| E_i) \oplus h(X \| T') \quad (16)$$

$$M_i^* = h(R_i' \| X \| T') \quad (17)$$

(4) 그리고 나서 공격자는 위조된 메시지 $\{D_i', M_i', T'\}$를 게이트웨이 노드에 전송하여 로그인 요청을 시도한다. 뒤따르는 과정은 첫 번째 유형과 유사하게 진행되고 궁극적으로 게이트웨이 노드로부터 적법한 사용자로 인증받는 사용자 가장 공격의 목적을 이룰 수 있다.

■ 재전송 공격

공격자에 의해 가로채기를 당할 수 있는 로그인 요청 메시지 $\{D_i, M_i, T\}$의 재전송 공격(replay attack)을 방지하기 위하여 Yuan 등의 스킴은 $(T^*-T) \leq \Delta T$를 검증하는 방법을 사용한다. 게이트웨이 노드가 재전송된 메시지의 시스템 시간 T^*을 이용하여 시간 차이의 유효성을 통해 재전송을 차단하는 방법은 통상적으로 널리 사용되고 있다. 하지만, 앞에서 살펴본 것처럼 공격자가 스마트 카드의 비밀정보를 추출하여 D_i^*와 M_i^*를 계산하고 위조된 로그인 요청 메시지 $\{D_i^*, M_i^*, T^*\}$를 게이트웨이 노드에 전송하는 경우에 이와 같은 재전송 공격 방지책이 더 이상 유효하지 않게 된다.

V. 결 론

본 논문은 Yuan 등이 제시한 인증 스킴을 살펴보고, 그들의 스킴에서 노출될 수 있는 보안 취약점을 분석하였다. Yuan 등의 스킴은 여전히 패스워드 추측 공격, 사용자 가장 공격 그리고 재전송 공격 노출에 따른 보안성 보장이 불가능하다는 것을, 본 연구는 밝혀내었다. Yuan 등의 스킴은 생체정보를 기반으로 한 사용자 인증 기능을 무선 센서 네트워크에 적용하였다는 점에서 나름대로 의의가 있다고 볼 수 있다. 현재 제공되지 않는 게이트웨이 노드와 센서 노드 간 상호인증(mutual authentication)을 구현하는 연구는 공격자로부터 예상되는 일련의 공격을 차단하기위해 요구되는 필요한 인증 요건의 하나이다. 따라서 향후 연구 과제는 본 논문에서 입증한 보안 취약성을 보완하고, 게이트웨이와 센서 노드간의 상호인증을 통해 서비스 거부 공격(denial-of-service attack) 등을 막을 수 있는 새로운 인증 스킴을 고안하는 것이다.

References

[1] H. Jeong, J. O. Lee, N. S. Park, and J. Y. Lee, et al., "Technical Trends of Sensor Networking", Electronic and Telecommunication Trends, Vol. 22, No. 3, pp. 80-89, 2005.

[2] J. K. Lee, S. R. Ryu, and K. Y. Yoo, "Fingerprint-based Remote User Authentication Scheme Using Smart Cards", Electronic Letters, Vol. 38, No. 12, pp. 554-555, 2002.

[3] H. Lee, and Y. Park, "A Design and Implementation of User Authentication System using Biometric Information", Journal of Korea Academia-Industrial Cooperation Society, Vol. 11, No. 9, pp. 3548-3557, 2010.

[4] C. T. Li, and M. S. Hwang, "An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards", Journal of Network and Computer Applications, Vol. 33, pp. 1-5, 2010.

[5] D. S. Wang, and J. Li, "A Novel Mutual Authentication Scheme Based on Fingerprint Biometric and Nonce Using Smart Cards", International Journal of Security and its Application, Vol. 5, No. 4, pp. 1-12, 2011.

[6] A. K. Das, "Analysis and Improvement on an Efficient Biometric-based Remote User Authentication Scheme Using Smart Cards", IET Information Security, Vol. 5, No. 3, pp. 541-552, 2011.

[7] J. Yuan, C. Jiang, and Z. Jiang, "A Biometric-Based User Authentication for Wireless Sensor Networks", Wuhan University Journal of Natural Science, Vol. 15, No. 3, pp. 272-276, 2010.

[8] L. Lamport, "Password Authentication with Insecure Communication", Communications of the ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[9] J. J. Shen, C. W. Lin, and M. S. Hwang, "Security Enhancement for Timestamp-based Password Authentication Scheme Using Smart Cards", Computers and Security, Vol. 22, No. 7, pp. 591-595, 2003.

[10] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Further Improvements of an Efficient Password based Remote User Authentication Scheme Using Smart Cards", IEEE Transaction on Consumer Electronics, Vol. 50, No. 2, pp. 612-614, 2004.

[11] C. J. Fan, Y. C. Chan, and Z. K. Zhang, "Robust Remote Authentication Scheme with Smart Cards",

Computers and Security, Vol. 24, No. 8, pp. 619-628, 2005.

[12] C. W. Lin, C. S. Tsai, and M. S. Hwang, "A New Strong-Password Authentication Scheme Using One-Way Hash Functions", Journal of Computer and Systems Sciences International, Vol. 45, No. 4, pp. 623-626, 2006.

[13] C. Lin, and C. Hung, "Cryptanalysis and Improvement on Lee-Chen's One-Time Password Authentication Scheme", International Journal of Security and its Application, Vol. 2, No. 2, pp. 1-8, 2008.

[14] Y. Joo, and Y. An, "Security Improvement of Remote User Authentication Scheme based on Smart Cards", Journal of Institute of Internet, Broadcasting and Communication, Vol. 11, No. 5, pp. 131-137, 2011.

[15] A. Perrig, R. Szewczyk, and V. Wen, et al., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, Vol. 8, No. 5, pp. 521-534, 2002.

[16] N. Sastry, and D. Wagner, "Security Considerations for IEEE 802.15.4 Networks", ACM Workshop Wireless Security, ACM Press, pp. 32-42, 2004.

[17] M Choi, T. Kim, S. Yeo, and E. Choi, "A Study on the Network Security Level Management", Journal of Korean Institute of Information Technology, Vol. 7, No. 1, pp. 214-219, 2009.

[18] R. Watro, D. Kong, and S. Cuti, et al., "Securing Sensor Networks with Public Key Technology", ACM Workshop Security of Ad Hoc Sensor Network, ACM Press, pp. 59-64, 2004.

[19] K. Wong, Y. Zheng, and J. Cao, et al., "A Dynamic User Authentication Scheme for Wireless Sensor Networks", IEEE International Conference Sensor Networks, Ubiquitous, Trustyworthy Computing, IEEE Computing Society, pp. 244-251, 2006.

[20] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", Proceedings of Advances in Cryptology, pp. 388-397, 1999.

[21] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks", IEEE Transactions on Computers, Vol. 51, No. 5, pp. 541-552, 2002.

저자 소개

주 영 도(정회원)

- 1983년 : 한양대학교 전자통신공학과 학사
- 1988년 : 미국 University of South Florida 컴퓨터공학과 석사
- 1995년 : 미국 Florida State University 전산학과 박사
- 1996년 ~ 2000년 : KT 통신망 연구소 선임 연구원
- 2000년 ~ 2005년 : 시스코 시스템즈 코리아 상무
- 2005년 ~ 2006년 : 화웨이 기술 코리아 부사장
- 2007년 ~ 현재 : 강남대학교 컴퓨터미디어정보공학부 교수

<관심분야 : 정보보안, 네트워크 보안, 정보검색, 데이터베이스>

※ 이 논문은 강남대학교 교내 연구비 지원을 받아 연구된 것임.