디지털산업정보학회 논문지 제19권 제1호-2023년 3월
http://dx.doi.org/10.17662/ksdim.2023.19.1.031

클라우드 기반 IoT 환경의 원격 헬스케어 시스템에 대한 보안성 분석*

권 재 민** · 홍 세 웅** · 최 윤 성***

Security Analysis of Remote Healthcare System in Cloud-based IoT Environment

Kwon Jaemin · Hong Sewoong · Choi Younsung

〈Abstract〉

As computer performance is leveled upward, the use of IoT systems is gradually expanding. Although IoT systems are used in many fields, it is true that it is difficult to build a safe system due to performance limitations. To overcome these limitations, many researchers have proposed numerous protocols to improve security issues. Among them, Azrour et al. except. We proposed a new efficient and secure authentication protocol for remote healthcare systems in a cloud-based IoT environment, and claimed that the new protocol could solve the security vulnerabilities of the existing protocols and was more efficient. However, in this paper, through the security analysis of the remote healthcare system in the cloud-based IoT environment proposed by Azrour et al., the protocol of this system was found to be vulnerable to Masquerade attack, Lack of Perfect Forward Secrecy, Off-line password guessing attack, and Replay attack.

Key Words : Security Analysis, Cloud-based IoT, Authetication Protocol, Remote User Authentication

Ⅰ. 서론

컴퓨팅 파워가 상향 평준화됨에 따라 IoT 시스템의 활용도가 점점 넓어지고 있다. 그럼에도 불구하고 IoT 기기의 태생적인 하드웨어적 한계로 인해 IoT 기기에서 단독으로 프로세스를 처리하는 것보다 클라우드 서버라는 근거리에 있는 서버로 일부 프로세스를 대신 처리하고 중계해주는 솔루션을 적용한 IoT와 클라우드 시스템이 결합된 형태가 제조, 유통, 판매 등 산업계의 IoT 시스템, 개인의 Home-IoT 시스템 등 여러 분야에서 여러 형태로 활용되고 있다. 특히, Kim et al. 의 주장처럼 최근 헬스케어 산업에 대한 수요가 늘어나는 추세이며 기술의 발전과 맞물려 Kim et al. 혹은 Jo et al. 의 연구와 같은 헬스케어 산업에서 전술한 시스템을 활용하는 방안이 대두되고 있다[1-5].

이러한 현상은 의료인력의 보조와 분산을 도와 더

* 본 논문 2022년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다. (재단 과제관리번호: 2021RIS-003)
** 인제대학교 컴퓨터공학부 정보보호전공 학사과정
*** 교신저자 : 인제대학교 AI융합대학 조교수
(cys2020@ inje.ac.kr)

욱 많은 사람들이 양질의 헬스케어 서비스를 받을 수 있는 계기가 되어준 반면, IoT와 클라우드의 보안성과 헬스케어 산업의 특성상 개인정보가 포함되어 있다는 점에서 이러한 민감정보가 이전보다 더 쉽게 유출되고, 헬스케어 시스템이 더 위중한, 더 잦은 공격을 당할 수 있는 상황에 놓이게 되었다. 예를 들어, 공격자가 적법한 사용자 간에 공유되는 정보를 쉽게 도청하거나 수정할 수 있고, 적법한 사용자를 가장해 잘못된 프로세스를 진행시키거나 시스템을 마비시킬 수 있다. 게다가 노출된 액세스 포인트와 보편적인 액세스 인터페이스는 그만큼 공격자들도 쉽게 접근이 가능하고, 잘못 설계된 시스템의 인증 프로토콜은 공격자들의 접근을 막지 못하고 오히려 자원 낭비가 될 수 있다. 따라서 사용자를 인증하기 위한 많은 시스템이 새로 제시되어오고 있으며, 기존 시스템의 문제점을 지적하며 보다 향상된 시스템을 제시하기도 한다.

예를 들어, Jin et al. [6] 처럼 안전한 클라우드 서비스를 위한 프레임워크를 제시하는 경우도 있으며, Song et al. [7] 처럼 클라우드 서비스를 위한 상호 인증 프로토콜을 제시하는 경우도 있다. 그 중에서도 Azrour et al. [8] 는 클라우드 기반 원격 헬스케어 시스템에서의 새로운 인증 프로토콜도 이러한 문제를 해결하기 위해 기존 프로토콜에 대한 문제점을 지적하며 Mutual authentication, Data integrity, Verification table, Session key, DoS attack preventation, Perfect forward secrecy, Protecting from off-line password guessing attack, Reply attack tolerance, Avoiding insider attack 등의 면에서 보안적으로 향상된 그들만의 프로토콜을 제안했다.

하지만, 우리는 보안성 분석을 통해 Azrour et al. 의 프로토콜이 Masquerade attack, Lack of perfect forward security, Possibility of off-line password guessing attack, Replay attack 등 여전히 여러 보안 취약점이 있다는 것을 발견했고 이를 밝히고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 Azrour et al.의 클라우드 기반 IoT 환경의 헬스케어 시스템의 프로토콜에 관련된 연구를 설명한 후, 3장에서 Azrour et al. 의 클라우드 기반 IoT 환경의 헬스케어 시스템의 프로토콜의 동작 과정을 분석하며 4장에서 Azrour et al.의 클라우드 기반 IoT 환경의 헬스케어 시스템의 프로토콜 보안성 분석을 통한 취약점을 제시한다. 마지막으로 5장에서 본 논문의 결론을 짓는다.

II. 관련 연구

신기술의 발전으로, 특히 IoT의 발생 이래로 개인정보 보호에 관련된, 접근 권한을 제한하는 시스템 혹은 그에 사용되는 데이터 인증 절차가 점점 중요해지고 있다. 본장에서는 본 논문에서 분석한 Azrour et al. 의 클라우드 기반 IoT 환경의 헬스케어 시스템의 인증 프로토콜과 관련된 인증 프로토콜에 대한 연구를 수행하였다.

Watro et al. [9] 이 WSN을 위한 RSA 기반 보안 인증 방식을 제안했고 Wong et al. [10] 은 단방향 해시 함수를 이용한 인증 방식을 제안했다. 해당 프로토콜은 Replay attack, Man-in-the-middle attack, Forgery attack, Key impersonation attack 등 기존의 공격에 대한 내성을 가지고 있다고 여겨졌다. 그러나 해당 시스템의 프로토콜의 Insider attack과 Man-in-the-middle attack에 대한 취약점이 발견되면서 Das et al. [11] 이 안전성을 향상시킨 프로토콜을 제시했다. 그리고 Xu et al. [12] 과 Song [13] 은 2009년과 2010년에 RSA 암호화 알고리즘에 기반한 인증 프로토콜을 각각 제시했다.

Elliptic Curve Cryptography(ECC)에 기반한 Xu et al. [14] 의 프로토콜은 인증과 키 합의 방식을 전산적 문제로 해결하는 방안을 제시했는데, 해당 프로

토콜은 동적인 식별자로 기밀성을 보장하는 점도 보여주었다.

그리고 Yen et al. [15] 은 생체 인식 시스템을 기반으로 사용자 인증 시스템을 제안했다. 그러나, 해당 프로토콜은 Replay attack에 취약하며 사용자의 익명성을 보장하지 못한다. 게다가 Mishra et al. [16] 이 Yan의 프로토콜이 Off-line password guessing attack에 대한 취약점이 존재한다고 밝혔다. 이러한 문제점을 바탕으로 Mishra et al.이 임의의 숫자를 사용함으로써 강화된 생체 인식 기반 인증 프로토콜을 제안했다. 그 후, Tan [17] 이 3단계의 상호 인증 프로토콜을 제시했다.

Yoon and Kim [18] 은 무선 센서 네트워크에서 보안 향상을 위한 생체 인식 파라미터 기반 사용자 인증 프로토콜을 제시했다. 해당 방식은 DoS attack, Sensor impersonation attack 등의 공격에서 안전성을 확보했다는 것을 보여주었다.

그리고 2012년, He et al. [19] 은 의료 센서 네트워크에서 활용하기 위한 효과적인 인증 프로토콜을 제시했다. 그러나 해당 방식은 Forgery attack과 Password guessing attack에 대한 취약점이 발견되었다. 게다가 Forward privacy service를 제공하지도 못한다. 2014년, Mishra et al. [20] 은 헬스케어 정보 유기체에 사용하기 위한 카오스 맵계산을 활용, 인증과 키 교환 프로토콜을 제시했다. 그러나 이 방법은 Password guessing attack에 대한 취약점이 있다.

2015년, Jiang et al. [21] 은 Chen et al. [22] 이 제시한 프로토콜이 Password guessing attack에 안전하지 않다는 점을 증명했고 해당 문제를 해결하기 위해 Jiang et al.이 또 다른 인증 방식을 제시했다. 그럼에도 해당 방식은 Password guessing attack과 User impersonation attack에 대한 취약점이 있었다.

그리고 2019년, Azrour et al. [23] 이 Ye et al. [24] 의 프로토콜이 안전하지 않다고 주장했으며, 같은 해, Cheng et al. [25] 이 다양한 분야의 기기에서 공개된 노드의 식별자를 인증하기 위해 Elliptical curve cryptography와 생체 인식을 기반으로 한 인증 방식을 제시했다. 그리고 2021년, Azrour et al. [26] 다양한 공격에 대한 안정성을 보장하고 효율성을 향상시킨 IoT 기기를 위한 새로운 인증 프로토콜을 제시했다. 또한, Azrour et al.[8]은 본 논문에서 분석하는 클라우드 기반 IoT 환경의 원격 헬스케어 시스템의 인증 프로토콜을 제안하였다.

Ⅲ. 클라우드 기반 IoT 환경의 원격 헬스케어 시스템의 인증 프로토콜 동작과정 분석

본 논문에서 사용한 용어 정보는 아래의 <표 1>과 같으며, Azrour et al. 등은 제안한 클라우드 기반 IoT 환경의 원격 헬스케어 시스템의 인증 프로토콜이 아래와 같은 장점을 가진다고 주장한다.

- 같은 값의 세션 키를 서버와 사용자가 각각 제작해 서로를 확인할 수 있다.
- 클라우드 서버가 사용자와 센서 노드의 유효성을 검증해 상호 인증이 가능하다.
- 타임스탬프를 송수신하는 데이터에 합성시켜 공격자의 데이터 변조 공격을 방지할 수 있다.
- 사용자의 비밀번호를 저장하지 않아서 클라우드 서버나 센서 노드 해킹에 성공하더라도 유의미한 정보를 얻을 수 없다.
- 해시 함수와 클라우드 서버의 비밀 키 등을 사용해 역계산 공격에 안전하다.
- 클라우드 서버의 비밀 키와 사용자의 암호화된 ID 등을 이용해 세션 키를 제작해 Perfect Forward Secrecy를 만족시킨다.

3.1 시스템 설정 단계

최고 관리자가 클라우드 서버의 비밀 키 X_S와 해시 알고리즘 h를 결정한다. 그리고 안전한 네트워크에 h와 X_S를 배포한다.

3.2 센서 등록 단계

서비스 중인 헬스케어 시스템에서 새로운 센서 노드(SN_i)를 등록하기 위해 클라우드 서버는 ID_{SNi}와 K_{CS-SNi}를 SN_i의 식별자와 유일 키로써 각각 선택한다. 그리고 센서 노드를 관리하는 게이트웨이 노드가 ID_{SNi}와 $SK_i = h(ID_{SNi} \,||\, K_{CS-SNi})$를 안전한 네트워크를 통해 센서의 메모리에 저장시킨다. 그리고 앞으로 쓰일 ID_{SNi}와 $HSK_i = SK_i \oplus h(X_S \,||\, ID_{SNi})$를 로컬 데이터베이스에 저장한다.

<표 1> Azrour et al.의 기호 정의

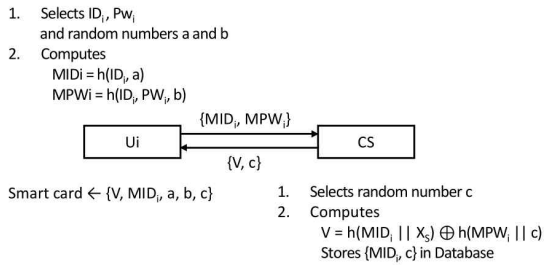
Symbol	Signification
U_i	User(Medical professional)
ID_i	Identity of U_i
PW_i	Password of U_i
SN_i	The sensor node
ID_{SNi}	Identity of sensor node
CS	Cloud server
X_S	Secret key of CS
K_{CS-SNi}	Shared key between CS, SN_i
T_1, T_2, T_3, T_4	The current time
A, B, C, D, a, b, c	Random numbers
h	Hash function
$\oplus$	XOR operator
||	Concatenation operator
’	Elements from exterial
?	Validation

3.3 사용자 등록 단계

클라우드 서버에 계정을 등록하기 위해, <그림 1>에서 보듯이 의학 전문가 U_i는 클라우드 서버에의 등록 절차를 거쳐야한다.

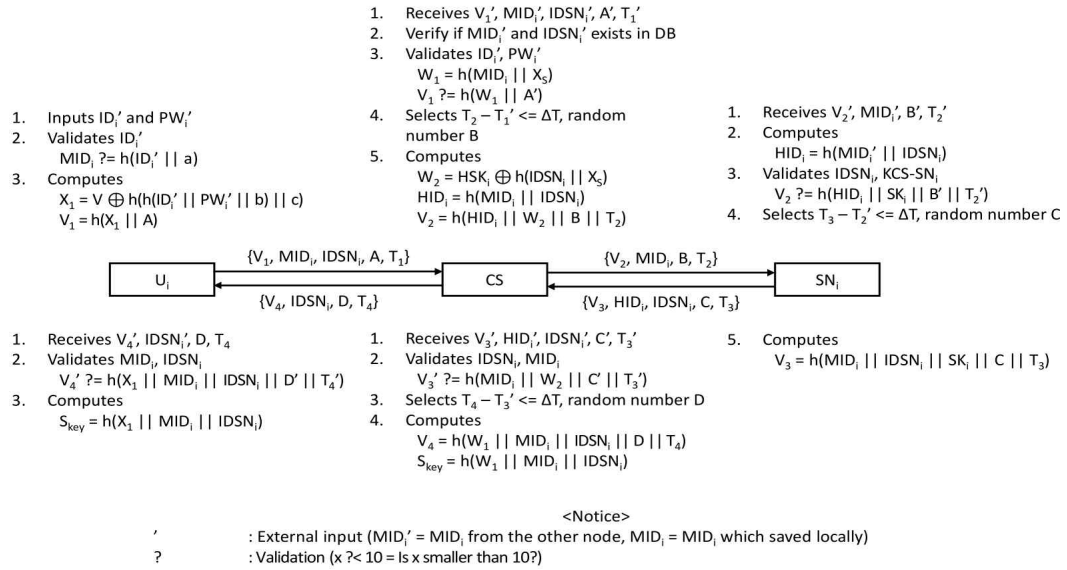
(1) 의학 전문가 U_i가 적절한 ID_i와 PW_i를 결정한다. 그후, 임의의 수 a와 b를 선택해 $MID_i = h(ID_i \,||\, a)$, $MPW_i = h(ID_i \,||\, PW_i \,||\, b)$를 계산한다. 그리고 MID_i와 MPW_i를 클라우드 서버에 안전한 통신망을 이용해 전송한다.

(2) 클라우드 서버 CS가 임의의 수 c를 선택하고 $V = h(MID_i \,||\, X_S) \oplus h(MPW_i \,||\, c)$를 계산한다. 그리고 CS의 로컬 데이터베이스에 MID_i와 c를 저장하고 V와 c를 U_i에게 전송한다.



<그림 1> 사용자 등록 단계

(3) U_i는 V, MID_i, a, b, c를 스마트 카드에 저장한다. Azrour et al.의 논문 원문에는 CS가 U_i에게 c를 전송하는 과정을 생략되어 있다. 하지만 c가 전송되지 않으면 사용자 U_i는 로그인 과정에서 U_i가 입력한 ID_i와 PW_i를 검증이 불가능하므로 [$X_1 = V \oplus h(h(ID_i \,||\, PW_i \,||\, b) \,||\, c)$], 실수로 판단되어 c를 전송하는 것으로 수정하였다. 그리고 HID_i를 저장된다고 명시되어 있으나, MIDi 의 오타로 판단되어 본 논문에서는 MIDi로 수정하여 명시하였다.



<그림 2> 로그인 및 인증 단계

3.4 로그인 및 인증 단계

의학 전문가 Ui는 등록 절차를 완수하면 모든 센서 노드에 접근할 수 있다. 이를 위해, <그림 2>처럼 Ui는 스마트 카드를 삽입해 로그인 단계를 거쳐 인증을 받아야 한다. 자세한 설명은 아래와 같으며, 이러한 로그인과 인증이 끝나면 Ui는 의료 센서 노드와 상호 작용을 실시간으로 할 수 있다.

(1) Ui → CS : {V_1, MID_i, ID_{SNi}, A, T_1}
먼저, U_i가 ID_i'와 PW_i'를 입력하면 스마트 카드가 MID_i *?= h(*ID_i*' // a)*를 수행해 ID_i와 동일한지 검증한다. 여기서 통과하지 못하면 프로세스가 진행되지 않는다. 그리고 스마트 카드는 임의의 수 A를 선택한 후, X_1 *= V ⊕ h(h(*ID_i*' //* PW_i*' // b) // c)*와 V_1 *= h(*X_1 *// A)*를 계산한다. 그리고 클라우드 서버 CS에 {V_1, MID_i, ID_{SNi}, A, T_1}을 보낸다.

(2) CS → SN_i : {V_2, MID_i, B, T_2}
U_i의 메시지를 받은 클라우드 서버는 T_2 *-* T_1*' <= ΔT*로 타임스탬프의 유효성을 검증하고 이를 만족하는 T_2를 제작한다. 그리고 W_1 *= h(*MID_i *// *X_S*)*를 제작하고 V_1*' ?= h(*W_1 *// A')*를 검증한다. 해당 검증을 통과하면, 클라우드 서버는 임의의 숫자 B를 제작하고 W_2 *= HSK*$_i$ *⊕ h(*ID_{SNi}*' //* X_S*)*, HID_i *= h(*MID_i *//* ID_{SNi}*')*, V_2 *= h(*HID_i *//* W_2 *//* T_2 *// B)*를 계산한다. 마지막으로 클라우드 서버는 센서 노드에게 {V_2, MID_i, B, T_2}로 구성된 메시지를 보낸다.

(3) SN_i → CS : {V_3, HID_i, ID_{SNi}, C, T_3}
센서 노드 SN_i가 CS의 메시지를 받으면, T_3 *-* T_2*' <= ΔT*인 유효한 타임스탬프를 제작한다. 그리고 HID_i *= h(*MID_i*' //* ID_{SNi}*)*를 제작, V_2 *?= h(*HID_i *//* SK_i *//* T_2*' // B')*를 검증해 적합한 CS에서, 자신에게 온 요청인지 확인한다. 그 후, 임의의 숫자 C를 선택해 V_3 *= h(*MID_i *//* ID_{SNi} *//* SK_i *//* T_3 *// C)*를 계산하고 {V_3, HID_i, ID_{SNi}, C, T_3}를 CS에게 다시 보낸다.

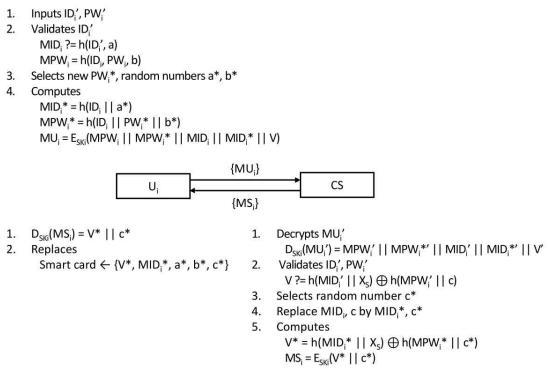
(4) CS → U_i : {V_4, ID_{SNi}, D, T_4}

센서 노드 SN_i의 응답이 클라우드 서버 CS에 도달하면 마지막 타임스탬프 $T_4 - T_3' <= \Delta T$와 $V_3' ?= h(MID_i // W_2 // C' // T_3')$의 검증 과정을 거친다. 해당 검증을 완수하면 CS는 임의의 숫자 D를 선택하고 $V_4 = h(W_1 // MID_i // ID_{SNi} // D // T_4)$를 계산하고 세션 키인 $S_{key} = h(W_1 // MID_i // ID_{SNi})$를 제작한다. 그 후, U_i에게 $\{V_4, ID_{SNi}, D, T_4\}$를 전송한다.

(5) 클라우드 서버의 응답을 받은 U_i는 $T_5 - T_4 <= \Delta T$와 $V_4 ?= h(X_1 // MID_i // ID_{SNi} // D' // T_4')$로 유효성을 검증하고 통과할 시, U_i도 세션 키 $S_{key} = h(X_1 // MID_i // ID_{SNi})$를 제작한다.

3.5 패스워드 변경 단계

Azrour et al.의 프로토콜에서는 의학 전문가인 사용자 U_i가 클라우드 서버와의 통신으로 자신이 월할 때 패스워드 변경 과정을 수행할 수 있다. 하지만 이러한 과정은 공개 인터넷망이나 통신 암호화 기술이 적용되지 않는 일반적 네트워크 환경에서도 이루어질 수도 있기 때문에, 패스워드 변경에서도 패스워드가 유출되지 않도록 설계하였다. 이에 대한 상세는 <그림 3>과 함께 아래에서 설명한다.



<그림 3> 패스워드 변경 단계

(1) $U_i \rightarrow CS : \{M_{Ui}\}$
의학 전문가인 U_i가 로그인을 위해 ID_i와 PW_i를 입력하고 이는 $MID_i ?= h(ID_i // a)$로 검증된다. 검증이 완료되면 사용자는 신규 패스워드인 PW_i*를 선택할 수 있다. 그리고 두 임의의 수 a*와 b*가 선택되고 $MID_i* = h(ID_i // a*)$와 $MPW_i* = h(ID_i // PW_i* // b)$가 새롭게 계산되고 마지막으로 SK_i를 이용해 $M_{Ui} = E_{SKi}(MPW_i // MPW_i* // MID_i // MID_i* // V)$ 암호화하고 클라우드로 전송한다.

(2) $CS \rightarrow U_i : \{M_{Si}\}$
사용자의 요청을 받은 클라우드 서버 CS는 SK_i를 이용해 $D_{SKi}(M_{Ui}) = (MPW_i // MPW_i* // MID_i // MID_i* // V)$로 복호화한다. 그 후, $V ?= h(MID_i' // X_S) \oplus h(MPW_i' // c)$로 올바른 값인지 검증한다. 여기서, Azrour et al.의 논문에서는 V, MID_i, MPW_i의 값이 U_i가 전송한 값인지, CS의 로컬에 저장되어 있는 값인지에 대한 부가적인 설명이 없어서 본 논문에서는 V를 CS의 로컬, MID_i, MPW_i를 U_i가 전송한 값으로 판단해 U_i 로그인의 진위성을 확보했다. 해당 과정이 끝나면 CS는 임의로 c*를 선택하고 로컬의 MID_i와 c를 각각 MID_i*와 c*로 대체한다. 그리고 $V* = h(MID_i* // X_S) \oplus h(MPW_i* // c*)$를 계산하고 $M_{Si} = E_{SKi}(V* // c*)$로 암호화해 U_i에게 전송한다. 여기서도 사용자 등록 단계와 마찬가지로 c를 전송하지 않는 오류를 범했다.

(3) CS가 응답하면 U_i는 마지막으로 $D_{SKi}(M_{Si}) = (V* // c*)$를 복호화하고 V, MID_i, a, b, c를 각각 V*, MID_i*, a*, b*, c*로 대체한다.

IV. 보안성 분석

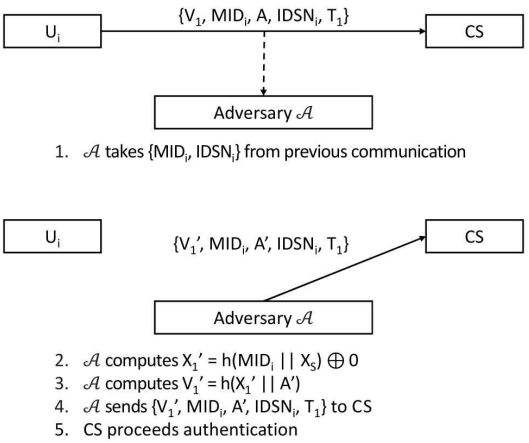
본 장에서는 Azrour et al. 등은 제안한 클라우드

기반 IoT 환경의 원격 헬스케어 시스템에 대한 보안성 분석을 진행한다. 공격자 $\mathcal{A}$는 다음 능력을 가지고 있다.[27-29]

- 공격자 $\mathcal{A}$는 공개된 모든 통신 채널을 제어한다. $\mathcal{A}$는 복제된 새 메시지를 추출, 재생, 업데이트, 폐지 또는 전달할 수 있다.
- 공격자 $\mathcal{A}$는 전력 분석을 통해 스마트카드에 저장된 정보를 입수하거나 유출 할 수 있다.
- 공격자 $\mathcal{A}$는 정당한 사용자 또는 서버로 가장할 수 있다.
- 서버와 사용자에 관한 정보는 기밀이 아니며, 공격자 $\mathcal{A}$는 모르지만 내부자는 알 수 있다.

4.1 Masquerade Attack

보안성 분석을 통해 본 프로토콜은 <그림 4>와 아래의 설명대로 클라우드 서버 CS의 관련자 $\mathcal{A}$, 혹은 CS에서 유출된 X_S를 획득한 공격자 $\mathcal{A}$가 의학 전문가인 사용자 U_i, 그것도 모든 사용자를 사칭할 수 있다는 치명적인 취약점이 존재한다는 점을 밝힐 수 있었다.



<그림 4> Masquerade Attack

(1) 공격자 $\mathcal{A}$는 U_i가 적법한 인증 절차를 거친 후, CS와 상호인증을 하기 위해 전송할 때, MID_i와 V_1, A, ID_{SNi}, T_1를 탈취할 수 있다. 해당 인증 절차에서 사용되는 V_1은 U_i의 카드에 저장되어있는 V와 U_i가 입력한 ID_i', PW_i' 등을 포함한 해시값과 합성해 x를 만들고 임의의 값인 A와 합성해 제작된다.

(2) 여기서, 해당 프로토콜의 설명에 따르면 $V = h(MID_i \,||\, X_S) \oplus h(MPW_i \,||\, c) = h(MID_i \,||\, X_S) \oplus h(h(ID_i \,||\, PW_i \,||\, b) \,||\, c)$를 도출할 수 있으며, 이러한 V와 U_i가 입력한 $h(h(ID_i' \,||\, PW_i' \,||\, b) \,||\, c)$를 합성해 X_1를 제작하는데, U_i가 올바른 ID_i'와 PW_i'를 입력했을시, $V \oplus h(h(ID_i' \,||\, PW_i' \,||\, b) \,||\, c) = h(MID_i \,||\, X_S) \oplus h(h(ID_i \,||\, PW_i \,||\, b) \,||\, c) \oplus h(h(ID_i' \,||\, PW_i' \,||\, b) \,||\, c) = h(MID_i \,||\, X_S) = X_1$이라는 결과가 나온다.

(3) 이러한 X_1와 임의의 값인 A를 합성해 해시값을 낸게 V_1인데, 이를 CS가 받으면 CS는 $W_1 = h(MID_i \,||\, X_S)$과 U_i에게서 수신한 A를 합성해 $h(W_1 \,||\, A)$의 값과 수신받은 V_1이 같은 값인지 검증 후, 올바르면 나머지 인증 프로세스를 진행한다.

(4) 여기서, X_S를 알고있는 공격자 $\mathcal{A}$가 탈취한 MID_i를 이용해 X_1를 제작, 임의로 선택한 A와 합성해 V_1을 제작, 전송하면 CS는 적법한 사용자로 판단해 인증 프로세스를 거쳐 사용자를 사칭할 수 있다.

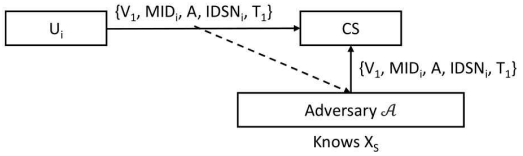
위 과정을 토대로 공격자 $\mathcal{A}$가 이전 통신에서 MID_i와 $IDSN_i$ 탈취하고 유출된 Xs을 사용하여 $h(MID_i||Xs) \oplus 0$을 계산하여 X_1'을 획득하고 획득한 X_1'을 이용하여 $h(X_1'||A')$을 계산하여 V_1'을 획득할 수 있다. 획득한 V1'을 CS에 $\{V_1', MID_i, A', IDSN_i, T_1\}$을 전송하면 사용자 U_i를 사칭하여 CS에 접속할 수 있다.

4.2 Lack of Perfect Forward Secrecy

Azrour et al.은 그들의 프로토콜이 Perfect Forward Secrecy를 보장한다고 주장한다. 하지만 Perfect Forward Secrecy는 비밀키와 같은 장기적 키(Long-Term Key)가 유출되더라도 세션키를 계산하기 어려워야 만족된다[30]. 하지만 Azrour et al.이 제안한 프로토콜에서 공격자가 장기적 키인 X_S를 알고 있을 경우, <그림 5>와 아래의 설명을 통해 세션 키를 임의로 계산할 수 있기 때문에 Perfect Forward Secrecy를 만족하지 못한다.

(1) 공격자 $\mathcal{A}$가 사용자를 사칭해 인증 프로세스 요청을 보낸다.
(2) CS는 적법한 사용자에게서의 요청으로 인식해 SNi와 인증 프로세스를 거치고 마지막에 세션키를 만들어 사용자와 통신할 준비를 한다.
(3) 공격자 $\mathcal{A}$가 장기적인 키인 X_S를 알고 있으면 공개 통신망을 통해 전송되는 MID_i, ID_{SNi}을 수집하여 사용자와 CS 간의 세션키 $S_{key} = h(x \,||\, MID_i \,||\, ID_{SNi}) = h(h(MID_i \,||\, X_S) \,||\, MID_i \,||\, ID_{SNi})$를 도출할 수 있다. 또한, <그림 5>에서 ID_{SNi}과 MID_i는 과거 통신 내용을 통해 알 수 있으므로, $\mathcal{A}$ 과거의 세션키도 계산해낼 수 있다. 그러므로 Azrour et al.이 제안한 프로토콜은 Perfect Forward Secrecy를 만족하지 못한다.

위 과정을 토대로 공격자 $\mathcal{A}$가 장기적 키인 X_S를 알고 있을 경우 공개 통신망을 통해 전송되는 MID_i, ID_{SNi}을 수집하고 이 수집한 값을 $S_{key} = h(x \,||\, MID_i \,||\, ID_{SNi}) = h(h(MID_i \,||\, X_S) \,||\, MID_i \,||\, ID_{SNi})$ 수식에 대입하여 사용자와 CS 간의 세션키를 획득할 수 있다. 그러므로 Perfect Forward Secrecy를 보장하지 못한다.

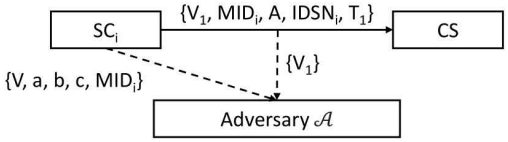


1. $\mathcal{A}$ who related with CS and knows X_S takes $\{V_1, MID_i, A, IDSN_i, T_1\}$ from previous communication
2. $\mathcal{A}$ sends $\{V_1, MID_i, A, IDSN_i, T_1\}$ to CS
3. CS recognizes $\mathcal{A}$ as a proper user and proceeds authentication
4. CS computes $S_{key} = h(W_1 \,||\, MID_i \,||\, IDSN_i)$
5. $\mathcal{A}$ computes $S_{key} = h(h(MID_i \,||\, X_S) \,||\, MID_i \,||\, IDSN_i)$ and pretends U_i consistently

<그림 5> Lack of Perfect Forward Security

4.3 Off-line Password Guessing Attack

U_i가 자신의 스마트카드를 분실하면 공격자 $\mathcal{A}$는 스마트카드의 모든 정보를 얻을 수 있다. Azrour et al.의 프로토콜에서 사용하는 스마트카드에는 U_i가 CS와 상호 인증하는 중요한 정보가 저장되어 있는데, 이는 아래의 설명과 <그림 6>과 같이 공격자 $\mathcal{A}$가 스마트카드에 저장된 정보와 과거 통신 내용에서 탈취한 정보를 사용해 U_i의 ID_i와 PW_i를 추측할 가능성이 있다.



1. $\mathcal{A}$ takes $\{V_1\}$ from previous communication
2. $\mathcal{A}$ takes $\{V, a, b, c, MID_i\}$ from SC_i(U_i's SmartCard)
3. $\mathcal{A}$ inputs ID_i' and PW_i' so that $\mathcal{A}$ can speculate ID_i and PW_i
   MID_i ?= $h(ID_i' \,||\, a)$
   V_1 ?= $h(V \oplus h(ID_i' \,||\, PW_i' \,||\, b) \,||\, c)$

<그림 6> Off-line Password Guessing Attack

해당 시스템의 프로토콜 진행 과정에서 적법한 사용자는 입력한 ID_i'와 스마트카드에 저장되어 있는 a를 이용해 생성한 $h(ID_i' \,||\, a)$를 MID_i와 비교해 ID_i'의

유효성을 검사한다.

여기서 공격자 $\mathcal{A}$는 스마트카드 탈취로 알게 된 U_i의 MID_i, a를 이용, 로그인 과정을 재구성해 MID_i를 재계산할 수 있다. 그리고 공격자 $\mathcal{A}$는 통신 내용 탈취로 알게 된 V_1와 스마트카드 탈취로 알게 된 U_i의 V_1, b, c로 V를 재계산할 수 있다. 재계산된 MID_i와 V는 U_i의 ID_i와 PW_i를 제외하고 모두 알 수 있는 정보들로 구성된다.

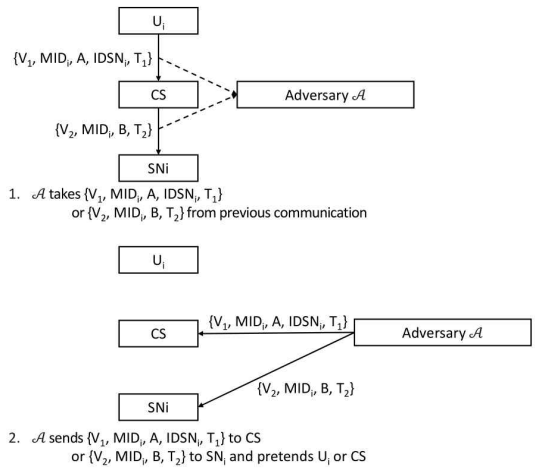
$|D_{ID}|$는 정해진 비트 수 내에서 ID_i로 성립될 수 있는 ID 집합의 크기, 즉 ID의 개수이며, $|D_{PW}|$는 정해진 비트 수 내에서 PW_i로 성립할 수 있는 PW 집합의 크기, 즉 PW의 개수이다. ID_i와 PW_i를 알아내기 위한 추측 공격 실행 시간은 $O(|D_{ID}| * |D_{PW}| * T_h)$이며 T_h는 해시 함수의 실행 시간이다. ID_i와 PW_i는 사용자가 직접 입력하는 단계에서, 인간이 기억할 수 있는 짧은 길이의 문자열로 구성된다는 점을 알 수 있으며, 이로 인해 공격자 $\mathcal{A}$가 무작위 패스워드를 입력하더라도 경우의 수가 적기 때문에 오프라인 패스워드(아이디) 추측 공격에 매우 취약하다. 다시 말해 사람들이 사용하는 ID 및 패스워드의 개수는 평균적으로 $|D_{ID}| <= |D_{PW}| <= 10^6$을 만족할 정도로 $|D_{ID}|$, $|D_{PW}|$의 개수는 매우 제한적이며, ID와 패스워드를 제외한 모든 값을을 알 수 있게 되면 ID와 패스워드를 알아낼 수 있다. 이로 인해 공격자 $\mathcal{A}$는 U_i의 스마트카드 정보와 과거 통신 내용을 이용한 오프라인 패스워드 및 아이디 추측 공격으로 U_i의 ID_i와 PW_i를 계산할 수 있다.[31]

위 과정을 토대로 공격자 $\mathcal{A}$가 U_i의 스마트카드를 획득하게 되면 획득한 스마트카드를 이용하여 U_i의 $\{V, a, b, c, MID_i\}$를 획득할 수 있다. 이 획득한 것들을 이용하여 $h(ID_i'||a)$라는 수식으로 MID_i를 추측하여 획득할 수 있다. 이를 통해 $h(V \oplus h(ID_i'||PW_i'||b)||c)$라는 수식에서 ID_i와 PW_i를 변경하면서 V_1의 값과 비교함으로써 사용자의 ID_i와 PW_i를 유추할 수 있다.

4.4 Replay Attack

Azrour et al. 프로토콜은 모든 인증 과정 중, 수신한 타임스탬프와 임의의 숫자(A, B, C, D)의 중복을 검증하는 단계가 존재하지 않는다. 이는 아래의 설명과 <그림 7>과 같이 공격자 $\mathcal{A}$가 수집한 과거의 통신 내용을 그대로 전송해 아주 간단하게 사용자 U_i, 혹은 클라우드 서버 CS를 사칭할 수 있는 보안 취약점이 된다.

위 <그림 2> 를 보면 U_i가 CS에게 인증받는 수식을 보면 필요한 값들이 $\{V_1, MID_i, IDSN_i, A, T_1\}$이 필요하다. 여기서 V_1을 검증하는 수식(V_1 ?= $h\{W_1||A'\}$)에는 타임스탬프를 사용하여 검증하지 않는다. 그렇기 때문에 U_i가 CS에게 인증받는 수식에 들어가는 T_1 만 현재 시각으로 바꾸어주면 된다.



<그림 7> Replay Attack

이를 방지하기 위해서는 임의의 숫자에 대한 타임스탬프를 추가하거나, 중복 검사 혹은 X_S, SK_i 등의 안전한 키와 규칙 있는 임의의 값, 해시를 통한 유효성 검증하는 간단한 단계를 추가하면 해결할 수 있다.

Ⅴ. 결론

Azrour et al.은 클라우드 기반의 IoT, 특히 헬스케어 분야에서 사용될 수 있는 새로운 원격 사용자 인증 프로토콜을 제안했다. 그들은 해당 프로토콜이 주요 보안 공격으로부터 안전하며 이전의 사용자 인증 프로토콜보다 더 효율적이라고 주장했다. 그러나, Azrour et al.의 프로토콜을 분석하며 이 프로토콜이 Masquerade attack, Lack of Perfect Forward Secrecy, Off-line password guessing attack 에 대한 보안 취약점이 있다는 점을 밝혔다. 본 연구의 결과가 향후 이 시스템에 대한 보안성 연구 및 새로운 시스템의 프로토콜 제안시 필요한 분석자료로 활용될 수 있을 것이라 판단한다.

참고문헌

[1] 김정원 · 신진철 · 박형근, “Zigbee를 이용한 사용자인식기반의 헬스케어 시스템 구현,” 디지털산업정보학회, 디지털산업정보학회 논문지, 제4권, 제3호, 2008, pp.1-8.

[2] 조정원 · 차시호 · 안병호 · 조국현, “홈 헬스케어를 위한 온톨로지 기반 상황인지 플랫폼의 설계 및 구현,“ 디지털산업정보학회, 디지털산업정보학회 논문지, 제5권, 제3호, 2009, pp.77-86.

[3] 조익성, ”스마트 헬스케어 환경에서 복잡도를 고려한 R파 검출 및 QRS 패턴을 통한 향상된 부정맥 분류 방법,“ 디지털산업정보학회, 디지털산업정보학회 논문지, 제17권, 제1호, 2021, pp.7-14.

[4] 김인환 · 남윤철, ”사물인터넷(IoT) 전시 서비스품질이 전시수용에 미치는 영향,“ 디지털산업정보학회, 디지털산업정보학회 논문지, 제17권, 제4호, 2021, pp.13-28.

[5] 박종순 · 박찬길, ”IoT 네트워크에서 스토리지와 트랜잭션 보호를 위한 이중 블록체인 구조,“ 디지털산업정보학회, 디지털산업정보학회 논문지, 제17권, 제4호, 2021, pp.43-52.

[6] 진병욱 · 김종화 · 차시호 · 전문석, “퍼스널 클라우드 환경에서 사용자 관리를 위한 보안 프레임워크의 설계 및 평가,“ 디지털산업정보학회, 디지털산업정보학회 논문지, 제12권, 제1호, 2016, pp.81-87.

[7] 송준호 · 최도현 · 박중오, “안전한 클라우드 서비스를 위한 상호의존적 다중세션 인증 기법 설계,“ 디지털산업정보학회, 디지털산업정보학회 논문지, 제10권, 제3호, 2014, pp.181-196.

[8] Azrour, M. Mabrouki, J. and Chaganti, R., “New Efficient and Secured Authentication Protocol for Remote Healthcare Systems in Cloud-IoT,” Security and Communication Networks, Vol.2021, Article ID 5546334, 2021, pp.1-12.

[9] Watro, R. Kong, D. Cuti, S. Gardiner, C. Lynn, C. and Kruus, P., “TinyPK: securing sensor networks with public key technology,” in Proceedings Of the 2nd ACM Workshop on Security Of Ad Hoc and Sensor Networks, San Diego, CA, USA, 2004, pp.59-64.

[10] Wong, K. H. Zheng, Y. Cao, J. and Wang, S., “A dynamic user authentication scheme for wireless sensor networks,” Sensor Networks, Ubiquitous, and Trustworthy Computing, Vol.1, 2006, p.8.

[11] Das, M. L., “Two-factor user authentication in wireless sensor networks,” IEEE Transactions on Wireless Communications, Vol.8, No.3, 2009, pp.1086-1090.

[12] Xu, Zhu, W.-T. and Feng, D.-G., “An improved smart card based password authentication scheme with provable security,” Computer Standards & Interfaces, Vol.31, No.4, 2009,

pp.723-728.

[13] Song, R., “Advanced smart card based password authentication protocol,” Computer Standards & Interfaces, Vol.32, No.5-6, 2010, pp.321-325.

[14] Xu, X. Jin, Z. P. Zhang, H. and Zhu, P., “A dynamic ID-based authentication scheme based on ECC for telecare medicine information systems,” In Applied Mechanics And Materials, Vol.457, 2014, pp.861-866.

[15] Yan, X. Li, W. Li, P. Wang, J. Hao, X. and Gong, P., “A secure biometrics-based authentication scheme for telecare medicine information systems,” Journal of Medical Systems, Vol.37, No.5, 2013, pp.1-6.

[16] Mishra, D. Mukhopadhyay, S. Kumari, S. Khan, M. K. and Chaturvedi, A., “Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce,” Journal of Medical Systems, Vol.38, No.5, 2014, pp.1-11.

[17] Tan, Z., “A user anonymity preserving three-factor authentication scheme for telecare medicine information systems,” Journal of Medical Systems, Vol.38, No.3, 2014, pp.1-9.

[18] Yoon, E.-J. and Kim, C., “Advanced biometric-based user authentication scheme for wireless sensor networks,” Sensor Letters, Vol.11, No.9, 2013, pp.1836-1843.

[19] He, D. Chen, C. Chan, S. Bu, J. and Vasilakos, A. V., “ReTrust: attack-resistant and lightweight trust management for medical sensor networks,” IEEE Transactions on Information Technology in Biomedicine, Vol.16, No.4, 2012, pp.623-632.

[20] Mishra, D. Srinivas, J. and Mukhopadhyay, S., “A secure and efficient chaotic map-based authenticated key agreement scheme for telecare medicine information systems,” Journal of Medical Systems, Vol.38, No.10, 2014, p.120.

[21] Jiang, Q. Ma, J. Li, G. and Li, X., “Improvement of robust smart-card-based password authentication scheme,” International Journal of Communication Systems, Vol.8, No.2, 2015, pp.383-393.

[22] Cheng, Z.-Y. Liu, Y. Chang, C.-C. and Chang, S.-C., “An improved protocol for password authentication using smart cards,” Vol.22, 2012, no.4.

[23] Azrour, M. Ouanan, M. Farhaoui, Y. and Guezzaz, A., “Authentication Protocol for Internet of Things,” Studies in Big Data, Vol.53, 2019, pp.67-74.

[24] NYe, N. Zhu, Y. Wang, R.-c. Malekian, R. and Qiao-min, L., “An efficient authentication and access control scheme for perception layer of internet of things,” Applied Mathematics & Information Sciences, Vol.8, No.4, 2014, pp.1617-1624.

[25] Cheng, X. Zhang, Z. Chen et al, F., “Secure identity authentication of community medical internet of things,” IEEE Access, Vol.7, 2019, pp.115966-115977.

[26] Azrour, M. Mabrouki, J. Guezzaz, A. and Farhaoui, Y., “New enhanced authentication protocol for internet of things,” Big Data Mining and Analytics, Vol.4, No.1, 2021, pp.1-9.

[27] Eisenbarth, T. Kasper, T. Moradi, A. Paar, C. Salmasizadeh, M. and Shalmani, M., “On the power of power analysis in the real world: A complete break of the KeeLoq code hopping

scheme," In Annual International Cryptology Conference, Springer, Berlin, Heidelberg, 2008, pp.203-220.

[28] Dolev, D. and Yao, A., "On the security of public key protocols," IEEE Transactions on information theory, Vol.29, No.2, 1983, pp.198-208.

[29] Cao, X. and Zhong, S., "Breaking a remote user authentication scheme for multi-server architecture," IEEE Communications Letters, Vol.10, No.8, 2006, pp.580-581.

[30] 최윤성, "퍼지추출 기술을 활용한 스마트 카드 기반 패스워드 인증 스킴," 디지털산업정보학회, 디지털산업정보학회 논문지, 제 14권, 제 4호, 2018, pp.125-134.

[31] Ma, C. G. Wang, D. and Zhao, S. D., "Security flaws in two improved remote user authentication schemes using smart cards," International Journal of Communication Systems, Vol.27, No.10, 2014, pp.2215-2227.

홍 세 웅
Hong Sewoong

2017년 3월~현재
인제대학교 컴퓨터공학부
정보보호전공 (학사과정)
2022년 4월 한국전자통신연구원 연수연구원

관심분야 : 정보보호, 블록체인, 프로토콜, 딥러닝분산컴퓨팅
E-mail : gemail2863@gmail.com

최 윤 성
Choi Younsung

2020년 2월~현재
인제대학교 AI융합대학 조교수
2016년 3월~ 2020년 2월
호원대학교 사이버보안학과 조교수
2015년 8월 성균관대학교
전자전기컴퓨터공학부(공학박사)
2012년 2월 경북대학교 법학박사 수료
2007년 8월 성균관대학교
전자전기컴퓨터공학부(공학석사)
2006년 2월 성균관대학교
전자전기컴퓨터공학부(공학학사)

관심분야 : 정보보호, 디지털포렌식, 산업정보보안
E-mail : cys2020@inje.ac.kr

논문접수일 : 2023년 2월 23일
게재확정일 : 2023년 3월 7일

■ 저자소개 ■

권 재 민
Kwon Jaemin

2018년 3월~현재
인제대학교 컴퓨터공학부
정보보호전공 (학사과정)

관심분야 : 정보보호, 디지털포렌식, 산업정보보안, 웹 취약점 분석
E-mail : gun2475@gmail.com