https://doi.org/10.33778/kcsa.2023.23.4.043

스마트 카드 및 동적 ID 기반 멀티서버 원격 사용자 인증 프로토콜의 취약점 분석★

권 순 형*, 변 해 원**, 최 윤 성***

요 약

많은 기업과 단체들은 원격 접근을 위해 스마트카드 기반 사용자 인증을 사용한다. 그 동안 다양한 연구를 통하여 사용자와 서버 간의 연결을 보호하기 위해 분산된 다중 서버 환경에 대한 동적 ID 기반 원격 사용자 인증 프로토콜들이 제안되었다. 그 중, Qiu 등은 상호 인증 및 키 동의, 사용자 익명성, 다양한 종류의 공격에 대한 저항을 제공하는 효율적인 스마트카드 기반 원격 사용자 인증 프로토콜을 제안하였다. 이후, Andola 등은 Qiu 등이 제안된 인증 프로토콜에 대한 다양한 취약점을 찾아내었고, 그들의 인증 프로토콜에 대한 결점을 극복하고 사용자가 서버에 로그인하기를 원할 때마다 로그인하기 전에 사용자 ID가 동적으로 변경되는 향상된 인증 프로토콜을 제안하였다. 본 논문에서는 Andola 등이 제안한 프로토콜의 동작 과정 및 취약점을 분석하여, Andola 등이 제안한 프로토콜이 offline smart card attack, dos attack, lack of perfect forward secrecy, session key attack에 취약하다는 것을 밝혔다.

Vulnerability Analysis of Remote Multi-Server User Authentication System Based on Smart Card and Dynamic ID

Kwon Soon Hyung*, Byeon Hae won**, Choi Youn Sung***

ABSTRACT

Many businesses and organizations use smartcard-based user authentication for remote access. In the meantime, through various studies, dynamic ID-based remote user authentication protocols for distributed multi-server environments have been proposed to protect the connection between users and servers. Among them, Qiu et al. proposed an efficient smart card-based remote user authentication system that provides mutual authentication and key agreement, user anonymity, and resistance to various types of attacks. Later, Andola et al. found various vulnerabilities in the authentication scheme proposed by Qiu et al., and overcame the flaws in their authentication scheme, and whenever the user wants to log in to the server, the user ID is dynamically changed before logging in. An improved authentication protocol is proposed. In this paper, by analyzing the operation process and vulnerabilities of the protocol proposed by Andola et al., it was revealed that the protocol proposed by Andola et al. was vulnerable to offline smart card attack, dos attack, lack of perfect forward secrecy, and session key attack.

Key words : Authentication Protocol, Remote Multi-Server, Dynamic ID, Vulnerability Analysis

접수일(2023년 07월 28일), 수정일(2023년 08월 11일), 게재확정일(2023년 08월 22일)

★ 본 과제(결과물)는 2023년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다. (2021RIS-003).

* 인제대학교 컴퓨터공학부 학사과정 (주저자)

** 인제대학교 AI융합대학 및 BK21대학원 디지털항노화헬스케어학과 조교수

*** 인제대학교 AI빅데이터학부 조교수 (교신저자)

1. 서 론

현재의 디지털 글로벌 시대에서는 다양한 플랫폼들, 예를 들면 전자 상거래 시장, 디지털 미디어, 소셜 네트워크, 그리고 금융 및 거래 플랫폼 등이 사람들을 연결하고 있다. 이러한 기업들은 사용자들에게 접근성, 확장성, 데이터 공유 및 통신 성능을 제공하여 더 나은 연결성을 실현하기 위해 노력하고 있다. 이 디지털 환경은 거의 모든 분야를 연결하기 때문에 기업들은 원격 접근을 통해 특정 서비스를 제공하고 있다. 그러나 보안이 불안정한 통로를 통해 안전한 통신이 중요하며, 이를 해결하기 위해 다중 서버 인증 프로토콜의 필요성이 더욱 부각되고 있다. 기업들은 클라우드나 제 3자 서버를 통해 서비스를 제공하면서 사용자 인증을 위해 비밀번호 테이블이나 인증 테이블에 비밀번호를 저장하는 방식을 사용한다. 그러나 이로 인해 비밀번호 노출이나 유출이 발생할 수 있다. 이를 해결하기 위해 다양한 연구자들은 스마트 카드 기반의 인증 프로토콜 연구에 집중하고 있다. 스마트 카드 기반 인증은 지식 요소와 소유 요소를 결합하여 이중 인증을 구현하는 방식으로, 사용자의 비밀 비밀번호와 스마트 카드를 사용하여 인증을 수행한다. 이 방식은 효율적이며 휴대성과 보안성이 뛰어나며, 비용 효율적인 접근 방법 중 하나이다[1].

그 동안 원격 사용자를 위한 인증 프로토콜에 대한 연구는 지속적으로 진행되어 왔다. Lamport [2]은 서버가 인증 데이터베이스에 비밀번호를 저장하는 공개 매체 상에서 원격 인증 방식을 제안했다. 그러나 이 방식은 보간 공격에 취약하다. 2000년에 Hwang and Li [3]은 서버가 비밀번호나 인증 정보를 저장하지 않는 ElGamal 공개 키 암호 프로토콜을 사용하는 스마트 카드 기반 원격 사용자 인증 방법을 제안했다. Juang 등 [4]은 사용자 익명성, 낮은 계산 및 통신 비용, 비밀번호 테이블 없음 및 시간 동기화 없음 등의 속성을 갖는 방식을 제안했다. 그러나 Sun 등 [5]은 Juang et al.의 방식이 비밀번호 업데이트, 상호 인증 키 합의 문제, 이중 비밀 키 문제 등에 취약하다고 주장하고 다른 방법을 제안했다. 또한, Li et al.[6]도 Juang et al.의 방식의 취약점을 입증했다. 이와 같이, 연구 커뮤니티는 스마트 카드와 단방향 해싱을 사용하는 여러 단일 서버 사용자 인증 방식을 제시하면서 통신 및 계산 비용을 줄이고 보안을 강화하는 기능을 갖춘 방식들을 제안해 왔다.

그러나 다중 서버 기반의 인증 프로토콜은 사용자 ID가 정적으로 사용되는 것이 공통적인 약점이다. 사용자 ID가 평문으로 전송되기 때문에 사용자의 행동을 추적할 수 있다. Liao and Wang [7]는 로그인 요청이 생성되기 전에 사용자 ID가 동적으로 변경되고, 실제 사용자 ID가 전달되지 않는 방법을 제안했다. 그러나 Hsiang and Shih [8]는 이 방법이 등록 센터 위장 공격, 위장, 내부자 공격, 서버 위조 공격에 취약하다고 입증했다. 그들은 모든 스마트 카드 보안 문제를 해결하고 모든 요구사항을 충족하는 다중 서버 환경을 위한 방법을 제안했다.

Lee et al. [9]는 Hsiang and Shih의 방법이 위장 공격에 취약하다고 보여주었다. 보안성 약점을 보완하기 위해 Lee et al.은 자신들의 방법을 제안했다. 그러나 Li et al. [10]와 Leu and Hsieh [11]은 Lee et al.의 방법이 위장 공격, 오프라인 비밀번호 추측 공격, 서버 위조를 방지할 수 없다고 보여주었다. Shunmuganathan et al. [12]은 Li et al.의 방법이 비밀번호 추측, 위장 문제에 대해 방지할 수 없으며 스마트 카드 도난 문제를 가지고 있다는 것을 입증했다. Hwang [13]는 Saraswathi 방법의 취약점을 발견하고 보안을 강화하는 개선된 방법을 제안했습니다. Qiu et al. [14]는 Hwang et al.의 인증 프로토콜이 완벽한 전달 비밀 보호를 보장하지 못하고, 키 침해 위장 공격에 저항하는 능력이 없다는 것을 입증했다. Qiu는 Hwang et. al.의 방법의 취약점을 견딜 수 있는 향상된 스마트 카드 기반 원격 사용자 인증 프로토콜을 제안했다. 그러나 분석 결과에 따르면, Qiu et al. 의 방법은 악의적인 사용자가 로그인 요청 메시지를 가로채고 스마트 카드를 훔쳐낸 경우 위장 문제에 취약하다. 또한, 비밀번호 추측 문제와 서버 위조에도 취약하며, 이중 인증을 제공할 수 없다. 이에 대해 Andola et al.[1]은 Qiu et al.의 문

제를 해결하기 위해 향상된 스마트 카드와 동적 ID 기반의 원격 다중 서버 사용자 인증 프로토콜을 제안하고 논의하였고, 새로운 프로토콜을 제안하였다.

그러나 본 논문에서는 Andola et al.이 제안한 프로토콜의 동작 과정 및 취약점을 분석하여, Andola et al.이 제안한 프로토콜이 offline smart card attack, dos attack, lack of perfect forward secrecy, session key attack에 취약하다는 것을 밝혔다.

2. 관련 연구

본 장에서는 멀티서버의 요구사항, 인증 프로토콜의 기본적 보안 속성, Challenge-Response Mechanism을 포함하는 기본 개념에 대해 설명한다.

2.1 멀티서버 환경의 요구사항

멀티서버 환경에서 사용자 인증 프로토콜을 구축하기 위해서 다음 요구사항을 충족해야 한다[1].

- 반복적인 등록 과정을 거치지 않아야 한다.
- 클라이언트 및 서버 측에서 최소한의 계산 비용이 들어야 한다.
- 사용자는 자유롭게 ID와 비밀번호를 선택하고 업데이트할 수 있어야 한다.
- 서버 측에서는 비밀번호 테이블과 인증 테이블을 유지해서는 안 된다.
- 프로토콜은 다양한 공격에 저항해야 한다.
- 시간 동기화가 필요하지 않아야 한다.
- 클라이언트-서버 및 세션 키 합의를 통해 상호 인증을 달성해야 한다.

2.2 인증 프로토콜의 기본적 보안 속성

인증 프로토콜에 대한 다양한 보안 요구사항은 선행 연구에서 제안되었으나 가장 필수적인 보안 속성에는 다음과 같다[15].

- Anonymity : 익명성의 중요성이 점점 더 커지고 있으며, 사용자의 신원이 승인되지 않은 당사자에게 공개되지 않아야 한다.
- Mutual authentication : 상호 인증은 사용자와 서버의 두 당사자가 서로를 인증하는 것을 의미한다. 즉, 사용자와 서버 모두 서로의 신원을 확인해야 한다.
- Session key agreement : 사용자와 서버는 후속 통신을 보호하는 데 사용할 세션 키에 안전하게 교환하여야 한다.
- Perfect forward secrecy : 완전 순방향 비밀성은 서버의 long-term key(비밀 키 등)가 노출되더라도 그 후 통신에서 발생하는 세션 키는 노출되지 않아야 한다는 보안속성이다.

2.3 Challenge-Response Mechanism

Challenge-Response Mechanism(도전-응답 메커니즘)은 인증 프로세스에서 사용되는 보안 기술로, 서버가 클라이언트에게 도전(challenge)을 보내고, 클라이언트는 이에 대한 응답(response)을 생성하여 서버에 제공하는 방식이다. 이를 통해 사용자의 신원을 확인하고 인증을 수행한다 . 사용자의 신원을 검증하고 인증하는 과정에서 사용되는 보안 기술이며, 이 메커니즘은 일회용 비밀번호를 생성하거나 임의의 도전 데이터에 대한 암호화된 응답을 생성함으로써 보안성을 강화한다. 이러한 특성으로 인해 중간자 공격과 같은 공격을 어렵게 만들고, 재사용을 방지하여 보안성을 강화합니다. Challenge-Response Mechanism의 작동 원리는 다음과 같다.

- 서버의 도전: 클라이언트가 인증을 요청하면, 서버는 클라이언트에게 도전 데이터를 보낸다. 이 도전 데이터는 무작위로 생성된 비밀값이거나 암호화된 데이터 등이 될 수 있다.
- 클라이언트의 응답: 클라이언트는 받은 도전 데이터를 기반으로 특정 알고리즘에 따라 응답을 생성한다. 이 응답은 도전 데이터를 가공하여 만들어지는 값으로, 서버만이 이를 검증할 수 있도록 설계된다.
- 서버의 검증: 클라이언트가 생성한 응답을 서버에 제공하면, 서버는 자체적으로 클라이언트의 응답을 검증한다. 이를 통해 클라이언트

가 실제로 도전 데이터를 받아서 올바른 응답을 생성한 것인지 확인하고, 그에 따라 인증을 수행한다.

3. Andola 등의 프로토콜의 동작과정

Andola et al.은 Qiu et al.의 프로토콜의 등록 단계, 로그인 단계, 검증 단계에서 발생하는 보안 문제를 제거하기 위해 사용자가 서버에 로그인하기 전에 사용자 ID를 동적으로 변경하는 향상된 익명 방식을 사용하는 프로토콜을 제안하였으며, 실제 다중 서버 사용자 인증에서 효과적이고 안정하게 사용할 수 있다고 주장한다. Andola et al.의 프로토콜에서 사용되는 용어 정보는 <표 1>과 같다.

<표 1> Descriptions of notations

Notation	Description
U_i	ith user
ID_i	U_i's identity
PW_i	U_i's password
S_j	jth server
RC	Registration centre
SK	Session key
SID_j	S_j's identity
CID_i	U_i's dynamic ID
x	Registration centre master key
y	Registration centre secret number
b	U_i's random number
$\oplus$	XOR operator
$\|\|$	Concatenate operator
$?=$	comparison operator
$\Rightarrow$	Secure medium
$\rightarrow$	Public medium
$h(.)$	One-way hashing function

2.1 등록 단계 분석

제안된 프로토콜의 등록 단계는 (그림 1)와 같으며, 사용자 $User(U_i)$는 아래와 같은 단계를 수행하여 스마트 카드에 기본 정보들을 등록한다.

① $User(U_i)$는 ID_i와 비밀번호 PW_i를 선택하고 무작위 수 b를 선택한다. 그리고, $User(U_i)$는 $RPW_i = h(b \oplus PW_i)$를 계산하고, 이를 $Server(S_j)$에게 $\{ID_i, PW_i\}$를 보낸다.

② 다음, 등록 요청 $\{ID_i, PW_i\}$를 받은 $Server(S_j)$는 비밀 키 x, y를 선택하고
$A_i = h(x||ID_i)$, $B_i = Z_i \oplus ID_i \oplus RPW_i$,
$C_i = h(RPW_i||ID_i||Z_i) \oplus B_i$,
$E_i = h(A_i||h(x||y)) \oplus Z_i$를 계산한다.

③ $Server(S_j)$는 새로운 스마트 카드에 $A_i, B_i, C_i, E_i, h(y), h()$를 $User(U_i)$에게 보낸다.

2.2 로그인 및 검증 단계 분석

등록된 사용자 $User(U_i)$가 서버에 로그인하기를 원하는 경우, 스마트 카드를 사용하여 서버에 로그인하는 것을 목표로 하며 다음 (그림 1)와 같은 계산을 수행하며, 각 단계마다 값의 유효성 검증을 진행한다.

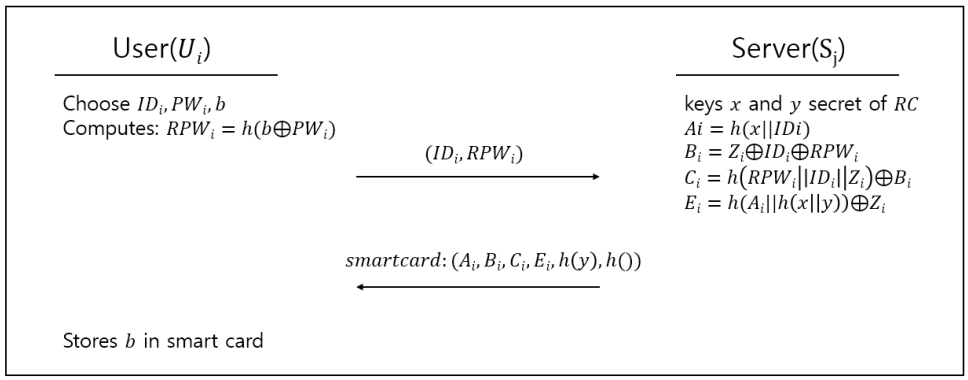
① $User(U_i)$는 ID_i, PW_i, SID_j를 사용하여 $Server(S_j)$에 대한 로그인 요청 메시지를 생성한다.

② 그 과정에서 $Z_i, C_i^{'}$를 계산하여 스마트 카드 안의 C_i값과 비교를 하여 유효성 검사를 진행한다.

③ 계속해서 P_{ij}, CID_i, M_1, M_2값을 생성해 $Server(S_j)$에 전달한다.

④ 전달받은 메시지로 $Server(S_j)$은 $N_i, A_i, E_i, Z_i^{'}, M_1^{'}$를 계산하여 생성하고, 그 중 $M_1^{'}$은 M_1과 비교 검증하여 유효성 검사를 진행한다.

⑤ 이후, $Server(S_j)$에서 N_j생성 및 M_3, M_4값을 생성해 $User(U_i)$로 전달한다.



(그림 1) Proposed registration phase of Andola et al.

User(U_i)		Server(S_j)
inserts smart card inputs ID_i, PW_i, SID_j $Z_i = ID_i \oplus h(b \oplus PW_i) \oplus B_i$ $C_i' = h(h(b \oplus PW_i)\|\|ID_i\|\|Z_i) \oplus B_i$ checks if $C_i' \stackrel{?}{=} C_i$ If yes, generates N_i and computes $P_{ij} = h(N_i\|\|h(y)\|\|SID_j) \oplus A_i$ $CID_i = E_i \oplus h(N_i\|\|SID_j\|\|A_i)$ $M_1 = h(Z_i\|\|N_i\|\|E_i)$ $M_2 = N_i \oplus h(SID_j\|\|h(y))$	$\xrightarrow{(P_{ij}, CID_i, M_1, M_2)}$	RC provided $h(y)$, $h(x\|\|y)$ $N_i = M_2 \oplus h(SID_j\|\|h(y))$ $A_i = h(N_i\|\|h(y)\|\|SID_j) \oplus P_{ij}$ $E_i = CID_i \oplus h(N_i\|\|SID_j\|\|A_i)$ $Z_i' = h(h(x\|\|y)\|\|A_i) \oplus E_i$ check if $M_1' = h(Z_i'\|\|N_i\|\|E_i) \stackrel{?}{=} M_1$ If yes, generate N_j and compute $M_3 = h(Z_i\|\|N_i\|\|SID_j\|\|CID_i)$ $M_4 = N_i \oplus N_j \oplus A_i$
	$\xleftarrow{(M_3, M_4)}$	
$N_j = M_4 \oplus A_i \oplus N_i$ check if $M_3' = h(Z_i\|\|N_i\|\|SID_j\|\|CID_i) \stackrel{?}{=} M_3$ If yes, compute $M_5 = h(Z_i\|\|N_j\|\|SID_j\|\|CID_i)$	$\xrightarrow{(M_5)}$	check if $M_5' = (Z_i\|\|N_j\|\|SID_j\|\|CID_i) \stackrel{?}{=} M_5$ If yes, $SK = h(Z_i\|\|SID_j\|\|N_i\|\|N_j\|\|CID_i)$
$SK = h(Z_i\|\|SID_j\|\|N_i\|\|N_j\|\|CID_i)$		

(그림 2) Proposed login and verification phase of Andola et al.

⑥ 전달받은 메시지로 $User(U_i)$은 $N_j, M_3^{'}$를 생성하고 $M_3^{'}$은 전달받은 M_3과 비교 검증을 진행한다.

⑦ 만약 값이 동일하다면 계속해서 M_5와 세션키 SK를 생성하여 $Server(S_j)$로 M_5을 전달한다.

⑧ 마지막으로 $Server(S_j)$는 전달받은 M_5와 계산하여 생성한 $M_5^{'}$를 비교 검증하고 세션키 SK를 생성하여 로그인을 완료한다.

4. Andola 등 프로토콜의 취약점 분석

Andola et al.는 그들의 프로토콜이 Offline password guessing attack, Replay-attack, Smart card stolen problem, Session key agreement, Two factor security, Mutual authentication, Good reparability, Password update 등의 위험으로부터 저항할 수 있다고 주장했다. 하지만 본 논문에서는 보안 분석을 통해, Andola et al.이 제안한 프로토콜이 ffline smart card attack, dos attack, lack of perfect forward secrecy, session key attack의 보안 문제점이 존재함을 밝혀냈다.

4.1 Offline Smartcard Attack

임의의 공격자 A가 오프라인 상에서 $User(U_i)$의 스마트 카드를 습득하면 (그림 3)와 같은 과정으로 사용자 $User(U_i)$의 ID_i와 PW_i를 알아낼 수 있다.

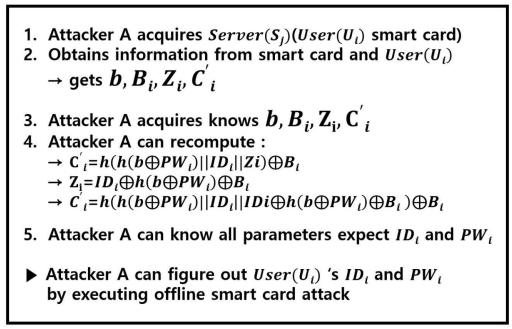
① Andola et al.의 프로토콜 로그인 단계에서는 스마트 카드 리더기가 사용자 $User(U_i)$가 입력한 정상적인 사용자의 ID_i와 PW_i를 이용하여 $C_i^{'} = h(h(b \oplus PW_i) \| ID_i \| Z_i) \oplus B_i$ 과정을 통해 만들어진 $C_i^{'}$과 스마트 카드에 저장된 C_i를 비교하여 $User(U_i)$의 신뢰성을 비교한다.

② 하지만, 임의의 공격자 A는 오프라인 스마트카드 공격으로 $User(U_i)$의 스마트 카드 정보 b, B_i를 알아낼 수 있다.

④ 또한, $C_i^{'} = h(h(b \oplus PW_i) \| ID_i \| Z_i) \oplus B_i$과 $Z_i = ID_i \oplus h(b \oplus PW_i) \oplus B_i$을 이용하여 다음과 같은 식을 생성할 수 있다.

$$C_i^{'} = h(h(b \oplus PW_i) \| ID_i \| ID_i \oplus h(b \oplus PW_i) \oplus B_i) \oplus B_i$$

③ 임의의 공격자 A는 위와 같은 식 변형을 통해 ID_i, PW_i를 제외한 나머지 정보를 알 수 있다.



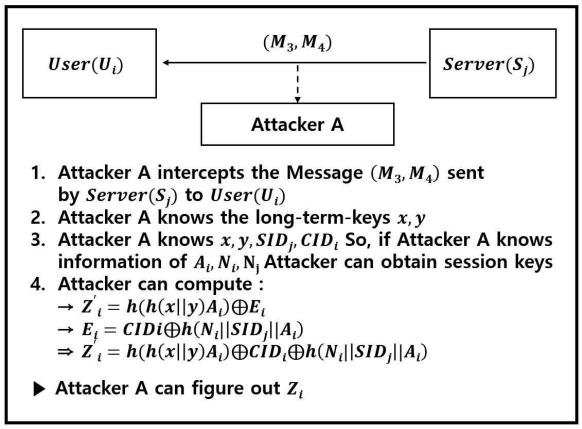
(그림 3) Offline smartcard attack on Andola et al. protocol

4.2 Lack of Perfect Foward Secrecy

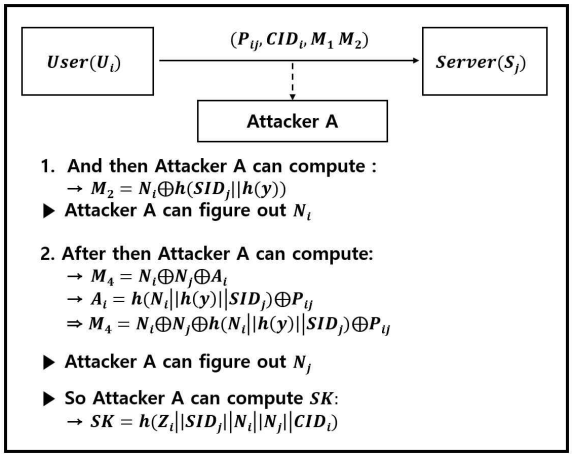
인증 프로토콜의 동작과정 상에서 long-term key 집합 중 하나가 노출되어도 이전 세션키의 기밀성은 유지되어야 한다. 하지만, (그림 4), (그림 5)과 같이 임의의 공격자 A가 서버의 long-term key인 x, y를 알고 있는 경우 계산을 통해 $User(U_i)$가 과거에 생성한 SK를 알아낼 수 있다.

① 해당 프로토콜에서 세션 키를 구하는 공식은 다음과 같다.
$SK = h(Z_i \| SID_j \| N_i \| N_j \| CID_i)$

② 임의의 공격자 A는 SID_j, CID_i는 공개정보로써, M_2, M_4는 $User(U_i)$와 $Server(S_j)$ 통신하는 메시지를 가로채 그 값들을 확보할 수 있다. 따라서 공격자 A는 나머지 Z_i, N_i, N_j를 알면 세션 키를 확보할 수 있다.



(그림 4) Lack of perfect forward secrecy on Andola et al. protocol – 1



(그림 5) Lack of perfect forward secrecy on Andola et al. protocol – 2

③ 이때, 프로토콜의 다음과 같은 식 병합 및 변환을 통해 Z_i, N_i, N_j를 확보할 수 있다.

④ Andola et al.의 프로토콜 로그인 단계 중 $Server(S_j)$의 프로토콜 동작에서

$Z_i' = h(h(x||y)A_i) \oplus E_i,$

$E_i = CID_i \oplus h(N_i||SID_j||A_i)$를 이용하여

$Z_i' = h(h(x||y)A_i) \oplus CID_i \oplus h(N_i||SID_j||A_i)$

과 같은 식을 도출해낼 수 있다.

⑤ 위의 식에서 임의의 공격자 A는 세션키를 계산하는데 필요한 x, y, CID_i, SID_j에 대한 정보를 알고 있으므로, A_i, N_i만 알면 이전 Z_i를 계산하여 세션 키를 확보할 수 있다.

⑥ 이후, $M_2 = N_i \oplus h(SID_j||h(y))$식에서 임의의 공격자 A는 M_2, SID_j, y의 값들을 확보하고 있어 N_i를 계산할 수 있다.

⑦ 또한, $M_4 = N_i \oplus N_j \oplus A_i,$

$A_i = h(N_i||h(y)||SID_j) \oplus P_{ij}$식을 병합하여 아래와 같은 식을 도출해낼 수 있다.

$M_4 = N_i \oplus N_j \oplus h(N_i||h(y)||SID_j) \oplus P_{ij}$

⑧ 위 식에서 임의의 공격자 A는 N_j를 제외한 모든 값을 확보하고 있기 때문에 N_j값을 구할 수 있다.

⑨ 임의의 공격자 A는 SK 계산에 필요한 Z_i, N_i, N_j를 모두 얻을 수 있다.

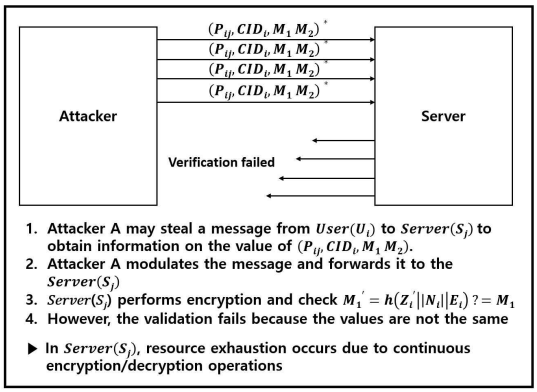
4.2 DoS Attack

DoS (Denial of Service) 공격은 인터넷 서비스를 사용할 수 없게 만드는 형태의 공격으로, 웹사이트, 서버, 네트워크, 애플리케이션 등을 목표로 한다. 이러한 공격은 트래픽 과부하, 리소스 고갈, 프로그램 취약점 등을 이용하여 시스템을 공격하며, 주로 정상적인 사용자들의 접속을 방해하여 서비스를 마비시키는 것이 목표다. 이로 인해 해당 서비스는 다운된 것처럼 보이거나 사용할 수 없는 상태가 될 수 있다. Andola et al. 프로토콜은 (그림 6)과 같이 인증을 위한 메시지를 검증하는데 필요한 과정이 복잡하여 DoS 공격에 취약한 취약점이 있다.

① 공격자 A는 User(U_i)에서 Server(S_j)로 전달되는 메시지를 스니핑하여 전송되고 있는 $(P_{ij}, CID_i, M_1, M_2)$ 값을 얻을 수 있다.

② User(U_i)에서 Server(S_j)로 메시지를 전달할 때 타임스탬프를 같이 보내지 않아 수신된 메시지의 정당성을 확인하지 못한다.

③ 이러한 취약점 때문에 M_1값의 확인 이전에 공격자가 이전 메시지 및 수정된 메시지를 Server(S_j)에 전달해도 Server(S_j)에서는 M_1값 확인 전까지의 연산을 계산할 수 밖에 없는 문제가 있다.



(그림 6) Dos attack on Andola et al. protocol

4.4 Session Key Attack

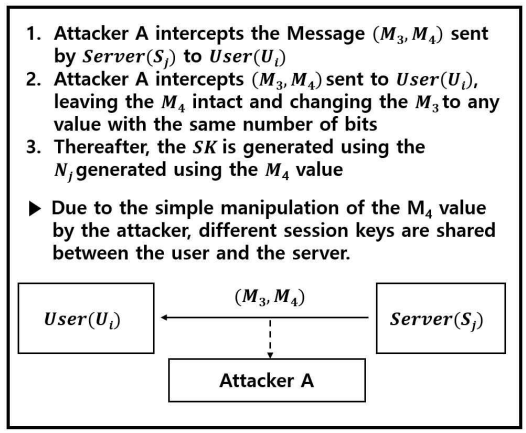
"Session Key Attack"은 암호화 통신에서 사용되는 세션 키(session key)를 탈취하거나 노출시키는 공격을 의미한다. 세션 키는 특정 통신 세션(메시지 교환) 동안 임시적으로 사용되는 암호화 키로, 메시지의 암호화와 해독에 사용된다. 세션 키가 유출되면 공격자는 해당 세션의 통신을 해독하거나 데이터를 변조하며, 재사용되거나 이전에 사용된 키로 인해 새로운 세션을 위조하는 보안 위협이 발생할 수 있다. Andola et al. 프로토콜은 (그림 7)과 같이 공격자가 간단한 메시지 조작만으로 세션키의 공유를 방해하고 잘못된 Session key를 설정하게 할 수 있는 취약점이 존재하고 있다.

① 임의의 공격자 A는 $Server(S_j)$에서 $User(U_i)$에게 보내는 (M_3, M_4)를 가로채어 M_3는 그대로 두고 M_4를 같은 비트 수의 임의의 값으로 변경한다.

② 이때, $User(U_i)$는 $Server(S_j)$에서 받은 M_3값을 이용하여 인증을 한다.

③ 이후, M_4값을 이용하여 생성해낸 N_j를 이용하여 SK를 생성한다

④ 하지만 N_j값이 변경되었기 때문에 잘못된 SK가 계산된다. 이를 해결하기 위해 M_3를 통해 인증할 때 N_j값도 포함하여 인증되어야 한다.



(그림 7) Session key attack on Andola et al. protocol

5. 결 론

Andola et al.은 보안 취약점을 극복하기 위한 향상된 스마트 카드와 동적 ID 기반의 원격 다중 서버 사용자 인증 프로토콜을 제안했다. 그들은 분산 환경의 요구 사항을 만족시키며 상호 키 합의의 정확성을 확인하기 위해 BAN 로직을 사용하여 스킴을 분석했으며, AVISPA를 통해 안전성을 검증하였다고 주장한다. 하지만, 본 논문은 Andola et al.이 제안한 프로토콜에 대한 취약점을 분석하여 offline smart card attack, dos attack, lack of perfect forward secrecy, session key attack에 취약하여 안전하지 않다는 것을 발견하였다. 본 연구 결과를 바탕으로 스마트 카드 및 동적 ID 기반 원격 다중 서버 사용자 인증 프로토콜에서 더욱 향상된 보안성과 신뢰성 그리고 효율적인 성능을 가진 프로토콜이 제안될 수 있을 거라 판단된다.

참고문헌

[1] Andola, Nitish, et al. "An enhanced smart card and dynamic ID based remote multi-server user authentication scheme." Cluster Computing 25.5 (2022): 3699-3717.

[2] Lamport, L.: "Password authentication with insecure communication." Commun. ACM 24(11), 770 - 772 (1981).

[3] Hwang, M.S., Li, L.H.: "A new remote user authentication scheme using smart cards." IEEE Trans. Consum. Electron. 46(1), 28 - 30 (2000).

[4] Juang, W.S., Chen, S.T., Liaw, H.T.: "Robust and efficient password-authenticated key agreement using smart cards." IEEE Trans. Ind. Electron. 55(6), 2551 - 2556 (2008).

[5] Sun, D.Z., Huai, J.P., Sun, J.Z., Li, J.X., Zhang, J.W., Feng, Z.Y.: "Improvements of Juang's password-authenticated key agreement scheme using smart cards." IEEE Trans. Ind. Electron. 56(6), 2284 - 2291 (2009).

[6] Li, X., Qiu, W., Zheng, D., Chen, K., Li, J.: "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards." IEEE Trans. Ind. Electron. 57(2), 793 - 800 (2010).

[7] Liao, Y.P., Wang, S.S.: "A secure dynamic ID based remote user authentication scheme for multi-server environment." Comput. Stand. Interfaces 31(1), 24 - 29 (2009).

[8] Hsiang, H.C., Shih, W.K.: "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment." Comput. Stand. Interfaces 31(6), 1118 - 1123 (2009).

[9] Lee, C.C., Lin, T.H., Chang, R.X.: "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards." Expert Syst. Appl. 38(11), 13863 - 13870 (2011).

[10] Li, X., Ma, J., Wang, W., Xiong, Y., Zhang, J.: "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments." Math. Comput. Model. 58(1 - 2), 85 - 95 (2013).

[11] Leu, J.S., Hsieh, W.B.: "Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards." IET Inf. Secur. 8(2), 104 - 113 (2013).

[12] Shunmuganathan, S., Saravanan, R.D., Palanichamy, Y.: "Secure and efficient smart-card-based remote user authentication scheme for multiserver environment." Can. J. Electr. Comput. Eng. 38(1), 20 - 30 (2015).

[13] Hwang, M.S., Cahyadi, E.F., Chou, Y.C., Yang, C.Y.: "Cryptanalysis of Kumar's remote user authentication scheme with smart card." In: 2018 14th International Conference on Computational Intelligence and Security (CIS), pp 416 - 420. IEEE (2018).

[14] Qiu, S., Xu, G., Ahmad, H., Xu, G., Qiu, X., Xu, H: "An improved lightweight two-factor authentication and key agreement protocol with dynamic identity based on elliptic curve cryptography." KSII Trans. Internet Inf. Syst. 13(2), 978 - 1002 (2019).

[15] Choi, Younsung, et al. :Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics. The Scientific World Journal 2014 (2014).

〔저자소개〕

권 순 형 (**Soon-Hyung Kwon**)
2017년 3월 ~ 현재 인제대학교 컴퓨터공학부 학사과정
email : ksh8895420@naver.com

변 해 원 (Haewon Byeon)

2013년 2월 : 아주대학교 예방의학교실 (이학박사)
2020년 9월 ~ 현재 : 인제대학교 AI융합대학 및 BK21대학원 디지털항노화헬스케어학과 조교수
email : byeon@inje.ac.kr

최 윤 성 (Youn-sung Choi)
2006년 2월 성균관대학교 정보통신공학부 학사
2007년 8월 성균관대학교 전자전기컴퓨터공학부 석사
2015년 8월 성균관대학교 전자전기컴퓨터공학부 박사
2016년 3월 ~ 2020년 2월 호원대학교 사이버보안학과 조교수
2020년 3월 ~ 현재 인제대학교 AI융합대학 AI빅데이터학부 조교수
email : cys2020@inje.ac.kr