https://doi.org/10.33778/kcsa.2022.22.4.179

세션 키 동의를 제공하는 상호인증 패스워드 인증 스킴에 대한 취약점 공격★

서 한 나*, 최 윤 성**

요 약

패스워드 인증 체계 (PAS)는 개방형 네트워크에서 안전한 통신을 보장하는데 사용되는 가장 일반적인 메커니즘이다. 인수분해와 이산 로그 등의 수학적 기반의 암호 인증 체계가 제안되고 강력한 보안 기능을 제공하였으나, 암호를 구성하는데 필요한 계산 및 메시지 전송 비용이 높다는 단점을 가지고 있었다. Fairuz et al.은 스마트 카드 체계를 이용한 세션 키 동의와 관련하여 인수분해 및 이산 로그 문제를 기반으로 한 개선된 암호 인증 프로토콜을 제안했다. 하지만 본 논문에서는 취약성 분석을 통하여, Fairuz et al.의 프로토콜이 Privileged Insider Attack, Lack of Perfect Forward Secrecy, Lack of User Anonymity, DoS Attack, Off-line Password Guessing Attack에 관한 보안 취약점을 가지고 있다는 것을 확인하였다.

Vulnerability Attack for Mutual Password Authentication Scheme with Session Key agreement

Seo Han Na*, Choi Youn Sung**

ABSTRACT

Password authentication schemes (PAS) are the most common mechanisms used to ensure secure communication in open networks. Mathematical-based cryptographic authentication schemes such as factorization and discrete logarithms have been proposed and provided strong security features, but they have the disadvantage of high computational and message transmission costs required to construct passwords. Fairuz et al. therefore argued for an improved cryptographic authentication scheme based on two difficult fixed issues related to session key consent using the smart card scheme. However, in this paper, we have made clear through security analysis that Fairuz et al.'s protocol has security holes for Privileged Insider Attack, Lack of Perfect Forward Secrecy, Lack of User Anonymity, DoS Attack, Off-line Password Guessing Attack.

Key words : Password authentication scheme, Vulnerability analysis, IFP, DLP

접수일(2022년 06월 22일), 수정일(2022년 09월 14일), 게재확정일(2022년 10월 31일)

★ 본 논문 2022년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다.(재단 과제관리번호: 2021RIS-003)

* 인제대학교 컴퓨터공학부 학사과정 (주저자)

** 인제대학교 AI융합대학 조교수 (교신저자)

1. 서 론

패스워드 인증 체계 (PAS)는 개방형 네트워크에서 두 독립체 간의 안전한 통신을 보장하는 가장 간단한 암호 시스템이다. 오늘날, 많은 서비스는 온라인에서 쉽게 이용할 수 있고 사용자가 언제든지 원격으로 접속할 수 있다. 일반적으로 사용자와 서버 간의 통신에는 개인 정보 및 금융 거래와 같은 공공 채널에서 개인 정보를 공유하는 것이 포함된다. 보안 되지 않는 네트워크를 통해 메시지를 전송하면 중요한 정보가 인증되지 않은 당사자에게 유출될 수 있는 보안 위험이 크다. 따라서 PAS는 이러한 보안 위험을 줄이는 메커니즘을 제공한다. 이전과 많은 PAS의 구성은 단방향 해시 함수, 대칭 및 공개 키 암호 시스템에 기초한다. 공개 키 기반 PAS의 보안은 정수 인수분해 문제(IFP), 이산 로그 문제(DLP), 타원 곡선 이산 로그 문제(ECDLP)와 같은 계산 수 이론적 하드 문제를 해결하는 난해성에 의존한다. 해시 기반 체계는 공개 키 기반 체계보다 더 효율적이다. 결과적으로, 해시 기반 체계는 경량 응용 프로그램에서 더 널리 사용된다. 이에 비해 공개 키 기반 체계는 해시 기반 체계보다 더 큰 보안 강도를 제공한다[1-5].

1999년, Yang et al[6]은 두 가지 어려운 문제(IFP, DLP)에 기반한 두 가지 새로운 암호 인증 프로토콜을 제안했다. 이 프로토콜을 통해 사용자는 패스워드를 설정할 수 있으나, 패스워드 검증에 대한 사항은 명시하지 않았다. Shen et al.[7]은 [6]이 제안한 프로토콜의 타임스탬프 기반 체계가 위조 및 서버 스푸핑 공격에 취약함을 보여주었다. 따라서, 그들은 타임스탬프 기반 체계를 위해 사용자와 서버 간의 상호 인증 기능을 제안했다. 일부 연구자들 [8]-[15]은 위조 공격을 차단하기 위해 이 체계의 추가 수정을 제안했다. 특히, Liu et al.[11]은 위조 로그인 공격에 저항하고 스마트 카드 계산 비용을 유지하면서도, 시간 동기화 문제를 해결하기 위한 새로운 난수 기반 체계를 제시하였다. Awasthi et al.[12]은 나중에 추가적인 보안 문제를 입증했다. 따라서, 그들은 Shen et al.[7]과 Liu et al.[11]의 연구내용을 바탕으로 프로토콜의 취약점을 해결할 수 있는 보다 효율적인 체계를 제안했다. Shen et al.[7]과 Awasthi et al.[12]의 보안 취약점을 극복하기 위해 Kumari et al.[15]도 보안적으로 향상된 프로토콜을 제안했다. 그들의 프로토콜은 세션 키 동의, 사용자 ID 보호, 로컬 암호 확인과 같은 몇 가지 보안 기능을 제공했다. 그러나 이 프로토콜은 다른 관련 이전 체계보다 훨씬 더 높은 계산 오버헤드를 요구한다. IFP와 DLP를 기반으로 하는 관련 체계가 훌륭한 보안 속성을 제공하지만, 높은 계산 및 전송 비용은 여전히 주요 문제이다. 따라서 Fairuz et al.은 수정된 IFP 및 DLP를 기반으로 하는 새로운 PAS를 제안하여 이전 관련 프로토콜의 계산 비용 개선을 주장했다.

그러나, 본 논문에서 Fairuz et al.의 프로토콜에 대한 취약점 분석을 통해, Fairuz et al.의 프로토콜이 Privileged Insider Attack, Lack of Perfect Forward Secrecy, Lack of User Anonymity, DoS Attack, Off-line Password Guessing Attack에 관한 보안 취약점을 밝혀냈다.

본 논문의 구성은 다음과 같다. 2장에서 Fairuz et al. 프로토콜에 관련된 연구를 설명한 후, 3장에서 Fairuz et al.의 프로토콜 동작 과정을 분석하며 4장에서 Fairuz et al.의 프로토콜에 대한 보안성 분석을 통한 밝혀진 취약점을 설명한다. 마지막 5장에서 본 논문의 결론을 짓는다.

2. 관련 연구

인수분해와 이산 로그에 기초한 많은 암호 인증 프로토콜에 대한 연구를 통해, 이러한 방식은 강력한 보안 속성을 제공했지만, 계산상의 높은 계산 오버헤드를 가진다는 단점이 있었다. 본 논문에서 분석한 Fairuz et al.의 프로토콜은 스마트 카드 체계를 이용한 세션 키 동의와 관련된 수정된 두 가지 어려운 문제를 기반으로 한 개선된 암호 인증 체계를 주장했다. 본장에서는 Fairuz et al.이 제안한 프로토콜의 동작 과정 및 취약점 분석과정에 대한 연구와 관련된 필요한 적대적 모델, BAN 논리에 관해 설명한다.

2.1 적대적 모델

적대적 모델이란 컴퓨터 또는 네트워크 시스템

에서 공격자를 공식화한 것을 말한다. 적대적 모델은 입증 가능한 보안 암호화 체계 또는 프로토콜 설계에 필수적이다. 공격 자원 외에도 적대적 모델에는 적의 의도, 즉 공격 목표와 제한 정책이 포함되어야 한다. 제안된 체계의 보안에 대한 논의는 안전하지 않은 공개 채널을 통해 실행되는 인증 프로토콜에 대한 Dolev-Yao[16] 위협 모델을 기반으로 한다.

- 공격자 A는 전송된 메시지를 속이거나 삭제 또는 변경할 수 있다[17].
- 공격자 A는 전력 모니터링 방법을 사용하여 스마트 카드에 저장된 정보를 얻을 수 있다[18, 19].

2.2 BAN Logic

BAN Logic이란 Burrows-Abadi-Needham Logic의 약자로 정보 교환 프로토콜을 정의하고 분석하기 위한 일련의 규칙이다. 프로토콜에 대한 추론을 위한 중요한 도구이며 가정과 정의를 사용하여 인증 프로토콜을 분석한다. BAN Logic은 단순하기 때문에 널리 사용되지만 BAN이 고려하지 않은 기능을 가진 기존 보안 프로토콜을 분석할 만큼 강력하지 않다는 것을 의미한다. 일반적인 BAN Logic 시퀀스에는 메시지 원본 확인, 메시지 신선도 확인, 원본의 신뢰성 확인 등 세 단계가 포함된다[20]. Fairuz et al.이 제안하는 프로토콜에서는 제안된 체계의 상호 인증 검증은 BAN 논리를 사용하여 안전성을 검증한다.

- Goal 1: $U_i| \equiv (U_i \overset{SK}{\longleftrightarrow} S)$
- Goal 2: $U_i| \equiv S| \equiv (U_i \overset{SK}{\longleftrightarrow} S)$
- Goal 3: $S| \equiv (U_i \overset{SK}{\longleftrightarrow} S)$
- Goal 4: $S| \equiv U_i| \equiv (U_i \overset{SK}{\longleftrightarrow} S)$

3. Fairuz et al.의 프로토콜 분석

본 논문에서 사용한 용어정보는 <Table 1>과 같으며, Fairuz et al.의 프로토콜은 초기화 단계, 등록 단계, 로그인 단계, 인증 단계, 비밀번호 변경 단계 등 5단계로 구성된다.

<Table 1> Notation of Fairuz et al.' protocol

Notation	Description
ID_i, pw_i, SC_i	Identity, password and sm art card of user U_i
$h(\cdot)$	One-way hash function, $h:\{0,1\}^* \rightarrow \{0,1\}^l$
$\Rightarrow$	Secure channel
$\rightarrow$	Public channel
$\|, \oplus$	String concatenation and XOR operators

3.1 초기화 단계

KIC는 다음 단계를 수행하여 서버 S의 공개 및 비밀 매개 변수, 사용자의 비밀 정보 등 글로벌 매개 변수를 설정한다.

① 1024비트 길이의 큰 소수 $p = 2p_1 + 1$와 $q = 2q_1 + 1$를 생성한다. 여기서 p_1과 q_1은 모두 소수이다.
② $n = p \cdot q$ 와 $\phi(n) = (p-1) \cdot (q-1)$ 을 계산.
③ (e, d)가 해당 공용 개인 키 쌍일 때, $e \cdot d \equiv 1 \bmod \phi(n)$인 소수 e와 정수 d를 구한다.
④ 유한체 F_p와 F_q의 원시 요소인 정수 g를 구한다.
⑤ $Z^*_{p_1}$ $Z^*_{q_1}$ 가 곱셈군일 때, 서버 S에 대한 비밀 매개변수 $x \in Z^*_{p_1}$ 또는 $Z^*_{q_1}$와 사용자의 ID 형식을 결정한다.
⑥ 보안 채널을 통해 d, x, ID 포맷을 S로 전송한다. KIC $\Rightarrow S$: {d, x,format for ID}

3.2 등록 단계

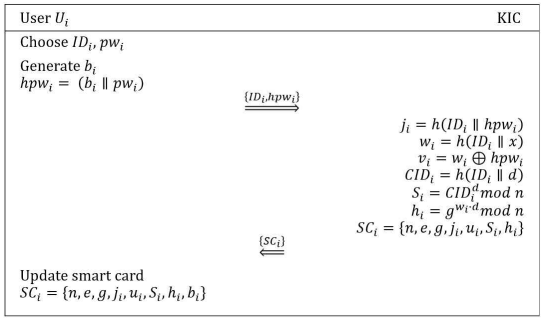
등록 단계는 새 사용자 U_i와 KIC사이의 보안채널을 통해 수행된다. 새 사용자 U_i는 다음과 같이 등록 단계를 시작한다.

① ID_i 및 암호 pw_i를 선택한다.
② 160비트 길이의 임의의 정수 b_i를 선택한다.
③ $hpw_i = h(b_i \| pw_i)$ 계산한다.
④ ID_i와 hpw_i를 KIC로 보낸다.
$U_i \Rightarrow \text{KIC} : \{ID_i, hpw_i\}$

그런 다음 KIC는 다음 단계를 계속한다.

⑤ $j_i = h(ID_i \| hpw_i)$, $w_i = h(ID_i \| x)$,
$v_i = w_i \oplus hpw_i$를 계산한다.
⑥ $CID_i = h(ID_i \| d)$를 생성한다.
⑦ $S_i = CID_i^d \bmod n$, $h_i = g^{w_i \cdot d} \bmod n$을 계산.
⑧ 스마트 카드 SC_i를 U_i로 발급한다.
$\text{KIC} \Rightarrow U_i : SC_i = \{n, e, g, j_i, u_i, S_i, h_i\}$.

다음으로, 사용자 U_i는 값 b_i를 스마트 카드 b_i에 기록한다. $SC_i = \{n, e, g, j_i, u_i, S_i, h_i, b_i\}$. Fig. 1에는 제안된 계획의 등록 단계가 요약되어 있다.



(Figure 1) Registration Phase

3.3 로그인 단계

등록된 사용자 U_i는 서버 S에 접속하기 위해스마트 카드 SC_i를 원격 단말기에 삽입하고 ID_i와 비밀번호 pw_i를 입력한다. 그런 다음 스마트 카드 SC_i는 다음 단계를 진행한다.

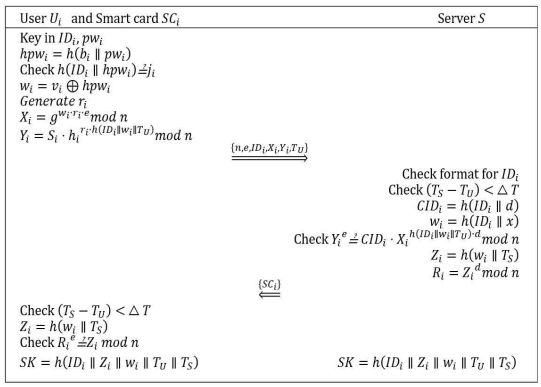
① $hpw_i = h(b_i \| pw_i)$를 계산.
② $h(ID_i \| hpw_i) \stackrel{?}{=} j_i$ 체크. 방정식이 유지되지 않으면 로그인 단계를 중단하고, 그렇지 않으면 다음 단계로 진행한다.
③ $w_i = v_i \oplus hpw_i$ 추출.
④ 160비트 길이의 임의의 정수 r_i 생성.
⑤ $X_i = g^{w_i \cdot r_i \cdot e} \bmod n$ 계산.
⑥ $Y_i = S_i \cdot h_i^{r_i \cdot h(ID_i \| w_i \| T_U)} \bmod n$ 계산.
⑦ 로그인 요청 메시지를 S로 전송.
$U_i \rightarrow S$: 로그인 요청 $= \{n, e, ID_i, X_i, Y_i, T_U\}$.

3.4 인증 단계

서버 S는 사용자 U_i로부터 로그인 요청이 수신되면 다음과 같은 단계를 실행한다.

① $(T_S - T_U) < \Delta T$ 를 확인한다. 여기서 ΔT는 허용되는 시간 전송이다. 시간 차이가 유지되지 않으면 로그인 요청을 거부한다.
② ID_i의 형식이 올바른지 확인한다. ID_i 형식이 올바르지 않으면 로그인 요청을 거부한다.
③ $CID_i = h(ID_i \| d)$ 및 $w_i = h(ID_i \| x)$를 계산한다.
④ $Y_i^e \stackrel{?}{=} CID_i \cdot X_i^{h(ID_i \| w_i \| T_U) \cdot d} \bmod n$ 체크. 방정식이 유지되지 않으면 로그인 요청을 거부한다.
⑤ $Z_i = h(w_i \| T_S)$ 및 $R_i = Z_i^d \bmod n$ 계산.
⑥ 응답 요청 메시지를 U_i로 보낸다.
$S \rightarrow U_i$: 응답 요청 $= \{R_i, T_S\}$.
사용자 U_i가 응답 인증 요청을 수신하면 사용자 U_i는 다음 단계를 수행한다.
⑦ $(T_c - T_S) < \Delta T$ 체크. 시차가 유지되지 않으면 서버 S와의 연결을 끊는다.
⑧ $Z_i = h(w_i \| T_S)$ 계산.
⑨ $R_i^e \stackrel{?}{=} Z_i \bmod n$ 체크. 방정식이 유지되지 않으면 서버 S와의 연결을 끊는다.
⑩ 그렇지 않으면 사용자 U_i와 서버 S가 세션키 $SK = h(ID_i \| Z_i \| w_i \| T_U \| T_S)$에 동의한다.

Fig. 2에는 제안된 계획의 로그인 단계, 인증단계가 요약되어 있다.



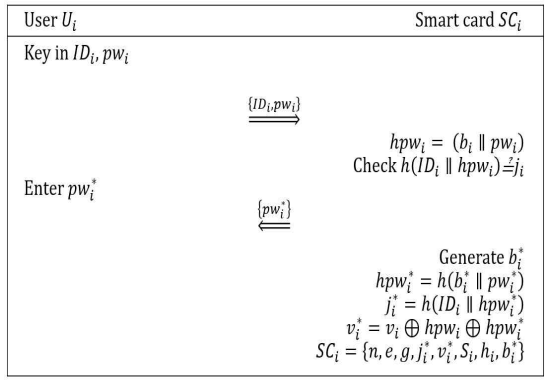
(Figure 2) Login and Authentication Phase

3.5 비밀번호 변경 단계

제안된 체계는 사용자가 KIC와 상호 작용하지 않고 로컬 암호 변경 기능을 지원한다. 사용자 U_i가 스마트 카드 SC_i를 원격 단말기에 삽입하고 ID_i 및 암호 pw_i를 제출하면 스마트 카드 SC_i가 다음 단계를 계속 진행한다.

① $hpw_i = h(b_i \| pw_i)$ 계산한다.
② $h(ID_i \| hpw_i) \stackrel{?}{=} j_i$ 체크. 방정식이 유지되면 사용자 U_i에 새 암호 pw_i^*를 입력하도록 요청한다.
③ 랜덤 정수 b_i^*를 생성한다.
④ $hpw_i^* = h(b_i^* \| pw_i^*)$ 및 $j_i^* = h(ID_i \| hpw_i^*)$를 계산한다.
⑤ $v_i^* = v_i \oplus hpw_i \oplus hpw_i^*$를 계산한다.
⑥ b_i, j_i 및 v_i를 각각 b_i^*, j_i^* 및 v_i^*로 대체한다.
⑦ 스마트 카드, $SC_i = \{n, e, g, j_i^*, v_i^*, S_i, h_i, b_i^*\}$를 업데이트한다.

다만 사용자 U_i의 스마트 카드 SC_i를 분실하거나 도난당한 경우 등록 단계에서 자세히 설명한 대로 새 스마트 카드를 발급받으려면 신규 등록이 필요하다. Fig. 3에는 제안된 계획의 비밀번호 변경 단계가 요약되어 있다.



(Figure 3) Password Change Phase

3.6 Fairuz et al.의 프로토콜의 Ban Logic 분석

Fairuz et al. 제안된 계획은 다음과 같이 이상화된 형태로 변환한다.

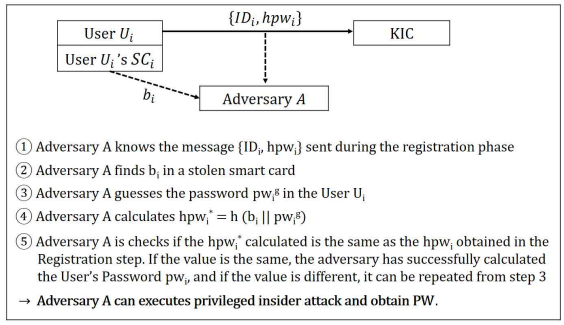
- Message 1: $U_i \rightarrow S : ID_i, \langle X_i, Y_i, T_U \rangle_{w_i}$
- Message 2: $S \rightarrow U_i : \langle R_i, T_S \rangle_{w_i}$
- $A_1 : U_i \mid \equiv \#(T_U, T_S)$
- $A_2 : S \mid \equiv \#(T_U, T_S)$
- $A_3 : U_i \mid \equiv (U_i \overset{w_i}{\longleftrightarrow} S)$
- $A_4 : S \mid \equiv (U_i \overset{w_i}{\longleftrightarrow} S)$
- $A_5 : S \mid \equiv U_i \Rightarrow T_U$
- $A_6 : U_i \mid \equiv S \Rightarrow T_S$

보안 증명 분석은 목표, 초기 상태 가정 및 BAN 논리에 기초하여 제시된다[20].

Fig. 4에서처럼 보안 증명 분석은 목표, 초기 상태 가정 및 BAN 논리에 기초하여 제시된다[20]. 이를 통해 Fairuz et al.은 자신들이 제안한 스킴의 수학적 안전성을 검증하였다.

From Message 1	From Message 2
S1: S ◁ (IDi ,(Xi , Yi , TU)wi).	S8: Ui ◁ (Ri , TS)wi
S1 및 A4인 경우 규칙 메시지 적용	S8 및 A3인 경우 규칙 메시지 적용
S2: S |≡ Ui |~ (Xi , Yi , TU).	S9: Ui |≡ S |~ (Ri , TS).
신선도 결합 규칙과 A2 산출량에 의해	신선도 결합 규칙과 A1 산출량에 따라
S3: S |≡ #(Xi , Yi , TU).	S10: Ui |≡ #(Ri , TS).
S2, S3 및 넌스 검증 규칙에서	S9, S10 및 넌스 검증 규칙에서
S4: S |≡ Ui |≡ (Xi , Yi , TU).	S11: Ui |≡ S |≡ (Ri , TS).
관할 규칙 S4와 A5에 따르면	관할 규칙인 S11,와 A6에 따르면
S5: S |≡ (Xi , Yi , TU).	S12: Ui |≡ (Ri , TS).
S4, A2 및 세션 키 규칙에서	S11, A1 및 세션 키 규칙에서
S6: S |≡ (Ui ←SK→ S) (Goal 3).	S13: Ui |≡ (Ui ←SK→ S) (Goal 1).
S6, A2, 및 넌스 검증 규칙에서	마지막으로 S13, A1 및 넌스 검증 규칙에서
S7: S |≡ Ui |≡ (Ui ←SK→ S) (Goal 4).	S14: Ui |≡ S |≡ (Ui ←SK→ S) (Goal 2).

(Figure 4) BAN Logic Analysis of Fairuz et al.'s Protocol



(Figure 5) Privileged Insider Attack on Fairuz et al.'s Protocol.

4. Fairuz et al. 프로토콜의 취약점 분석

공격자 A가 안전한 보안 모델에 관한 모든 능력을 갖추고 있다고 가정한다.

4.1 Privileged Insider Attack

Privileged Insider Attack이란 공격자가 등록 단계에서 보내지는 메시지를 가로채거나 얻어서 사용자의 패스워드를 찾아내는 공격을 말한다. Fig. 5에서는 Fairuz et al. 프로토콜에 대한 Privileged Insider Attack을 설명하고 있다. Fairuz et al. 프로토콜은 공격자 A가 등록 단계에 전송되는 메시지를 얻었을 때 사용자 U_i의 패스워드 pw_i를 알아낼 수 있다.

① 공격자 A는 등록 단계에서 전송되는 메시지를 획득하여 $\{ID_i, hpw_i\}$를 알아 낸다..

② 공격자 A는 훔친 스마트카드 안에서 b_i를 추출한다.

③ 공격자 A는 사용자 U_i의 패스워드 pw_i^g를 추측한다.

④ 공격자 A는 $hpw_i^* = h(b_i \| pw_i^g)$를 계산한다.

⑤ 공격자 A는 등록 단계에서 얻은 hpw_i와 계산한 hpw_i^*를 비교한다. 만약 값이 일치한다면 공격자 A는 사용자 U_i의 패스워드 pw_i 추측을 성공한 것이고, 값이 일치하지 않다면 3단계부터 반복 실행한다.

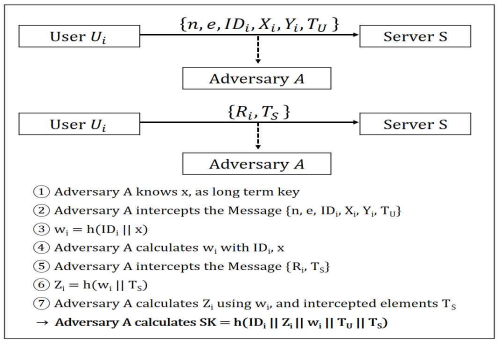
4.2 Lack of Perfect Forward Secrecy

Perfect forward Secrecy란 장기키가 공격자에게 노출되더라도 이전 데이터의 기밀성에 지장을 주지 않는 암호학적 성질을 말한다.

하지만 Fairuz et al. 프로토콜은 공격자 A가 장기키 x를 알고 있을 경우, 공격자 A는 서버 S와 사용자 U_i 사이에서 사용된 세션 키 SK를 계산할 수 있어, Perfect Forward Secrecy를 만족하지 못한다.

Fig. 6는 Fairuz et al. 프로토콜에 대한 Lack of Perfect Forward Secrecy에 대해 설명하고 있다. 공격자 A가 장기 키 x를 안다고 가정한다. 공격자 A는 공개 채널로 전송되는 메시지인 $\{n, e, ID_i, X_i, Y_i, T_U\}$를 획득할 수 있다. 공격자 A가 획득한 메시지 중 하나인 ID_i와 공격자 A가 가진 장기 키 x를 이용하여 세션에 사용된 $w_i = h(ID_i \| x)$를 계산하면 w_i를 알아낼 수 있다. 따라서 공격자 A는 세션 키 SK 계산에 필요한 ID_i와 w_i, T_U를 얻을 수 있다.

공격자 A는 서버 S가 사용자 U_i를 인증하고 세션키를 만들기 위해 다시 전송하는 메시지인 $\{R_i, T_S\}$를 획득할 수 있다. 공격자 A가 획득한 메시지 중 하나인 T_S와 공격자 A가 1단계에서 알아낸 w_i를 이용하여 세션에 사용된 $Z_i = h(w_i \| T_S)$를 알아낼 수 있다. 따라서 공격자 A는 앞으로 통신에 사용할 세션키인 $SK = h(ID_i \| Z_i \| w_i \| T_U \| T_S)$의 계산에 필요한 ID_i, Z_i, w_i, T_U, T_S를 전부 도출할 수 있고, 이를 이용해 공격자 A가 세션 키 SK를 생성할 수 있다.

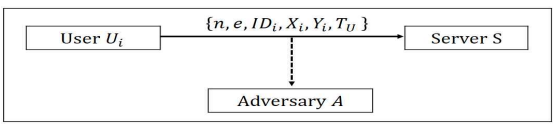


(Figure 6) Lack of Perfect Forward Secrecy on Fairuz et al.'s Protocol.

4.3 Lack of User Anonymity

Anonymity란 익명성, 즉 시스템의 사용자 또는 메시지가 도청 활동을 통해 추적이 불가능한 상태를 말한다. 그러나 Fairuz et al. 프로토콜은 사용자의 익명성을 보장하지 못한다.

Fig. 7는 Fairuz et al. 프로토콜에 대한 Lack of User Anonymity 취약점을 설명하고 있다. 사용자 U_i의 ID_i가 원시 형태로 공개 채널을 통해 전송되므로 공격자 A는 쉽게 노출되어 있는 ID_i를 획득할 수 있다. 그렇게 된다면 공격자 A는 사용자 U_i와 서버 S의 통신 과정을 지켜보며 정보를 얻을 수 있게 된다. 예를 들어 사용자 U_i가 어떤 서버와 통신하는지, 통신의 횟수 등을 알 수 있다.



(Figure 7) Lack of User Anonymity on Fairuz et al.'s Protocol.

4.4 DoS Attack

DoS Attack이란 서버를 악의적으로 공격하여 서버 자원 부족으로 인해 원래 의도한 용도로 사용하지 못하게 하는 공격을 말한다. Fig. 8에는 Fairuz et al. 프로토콜에 대한 Dos Attack 취약점이 요약되어 있다. Fig. 8와 같이, Fairuz et al. 프로토콜은 체크 연산 3번, 해쉬 연산 4번, 모듈러 연산 2번을 수행한다. 따라서 수행해야 하는 높은 연산량 때문에 DoS 공격에 취약해진다.

Check format for ID_i
Check $(T_S - T_U) <\triangle T$
$CID_i = h(ID_i \| d)$
$w_i = h(ID_i \| x)$
Check $Y_i^e \stackrel{?}{=} CID_i \cdot X_i^{h(ID_i \| w_i \| T_U) \cdot d} mod\ n$
$Z_i = h(w_i \| T_S)$
$R_i = Z_i^d mod\ n$

① Check operation
Check format for ID_i, Check(TS-TU)<△T
Check $Y_i^e \stackrel{?}{=} CID_i \cdot X_i^{h(IDi||wi||TU)\cdot d} \bmod n$
② Hash operation
$h(ID_i||d)$, $h(ID_i||x)$, $h(ID_i||w_i||T_U)\cdot d$, $h(w_i||T_S)$
③ Modular operation
$CID_i \cdot X_i h(ID_i||w_i||T_U)\cdot d \bmod n$, $Z_i^d \bmod n$

(Figure 8) DoS Attack on Fairuz et al.'s Protocol.

4.5 Off-line Password Guessing Attack

Off-line Password Guessing Attack이란 Off-line 상에서 획득한 정보를 이용하 사용자가 자주 선택하는 패스워드에 대한 사전 파일이나 무작위공격 방식을 이용하여 사용자들의 패스워드를 추측하는 공격을 말한다.

Fig. 9에는 Fairuz et al. 프로토콜에 대한 Off-line Password Guessing Attack에 대해 설명하고 있다. 먼저, 공격자는 사용자와 서버 간 송수신되는 메시지들을 저장하고, 메시지로부터 검증 값을 획득한 후, 패스워드 사전을 이용하여 유도된 검증 값과 같은지 여부를 비교 판단하고, 사용자가 설정한 패스워드와 일치하는 값을 찾아낸다.

① Adversary A takes the U_i's SC_i
② So Adversary A gets $\{n, e, g, j_i, u_i, S_i, h_i, b_i\}$
③ Adversary A recalculates the formula used in the authentication process
→ $j_i \stackrel{?}{=} h(ID_i \| h(b_i \| pw_i))$
④ Adversary A knows all formula's parameter except for ID_i, pw_i
→ ID_i pw_i are very limited in practice such as $|D_{id}| \leq |D_{pw}| \leq 10^6$
→ **So, Adversary A can executes off-line password attack and obtain ID_i, pw_i**

(Figure 9) Off-line Password Guessing Attack on Fairuz et al.'s Protocol

사용자 U_i가 자신의 스마트 카드를 분실했을때 공격자 A는 스마트 카드의 정보를 획득할 수 있다. Fairuz et al.의 프로토콜에서 사용하는 스마트 카드에는 사용자와 서버가 상호 인증에 필요한 정보들이 저장되어 있다. 사용자 U_i가 소유하는 스마트 카드는 $\{n, e, g, j_i, u_i, S_i, h_i, b_i\}$를 저장한다. 사용자는 등록된 ID_i와 pw_i를 입력하여 만들어진 j_i를 비교하여 스마트 카드에 저장된 j_i와의 동일성을 체크한다.

- $hpw_i = h(b_i \| pw_i)$
- $j_i \stackrel{?}{=} h(ID_i \| hpw_i)$
- $j_i \stackrel{?}{=} h(ID_i \| h(b_i \| pw_i))$

그러나 공격자는 스마트 카드 탈취로 알게 된 사용자의 $\{n, e, g, j_i, u_i, S_i, h_i, b_i\}$ 정보와 로그인 과정을 재구성하여 j_i를 재계산할 수 있다. 재구성된 j_i는 공격자가 사용자의 ID_i와 pw_i를 제외하고 전부 알 수 있는 정보들로 이루어져 있다.

정해진 비트 수 내에서 ID_i로 성립할 수 있는 아이디의 집합은 $|D_{id}|$이고 정해진 비트 수 내에서 pw_i로 성립할 수 있는 아이디의 집합은 $|D_{pw}|$이다. $O(|D_{id}|*|D_{pw}|*T_H)$는 ID_i, pw_i를 알아내기 위한 추측 공격 실행 시간이고, 여기서 T_H는 해시 함수 실행 시간이다. 암호는 사람이 기억 가능한 짧은 길이의 문자열로 이루어지기에 크기가 작은 각각의 공격자가 가진 사전에서 택하게 되는 경우가 많아 Off-line Password Guessing Attack에 취약하다. $|D_{id}| \leq |D_{pw}| \leq 10^6$을 만족하는 $|D_{id}|$와 $|D_{pw}|$는 매우 제한적이고, 앞서 언급했던 공격이 다항시간 안에 성공할 수 있다. 그러므로, 공격자는 사용자의 스마트카드 정보를 이용한 Off-line Password Guessing Attack을 통해 사용자의 ID_i, pw_i를 계산할 수 있다.

5. 결 론

Fairuz et al.은 세션 키 동의 방식을 수정된 IFP 및 DLP를 기반으로 개선한 패스워드 인증 프로토콜을 주장하였다. 그러나 본 논문에서는 취약점 분석을 통해 Fairuz et al.의 프로토콜이 Privileged Insider Attack, Lack of Perfect Forward Secrecy, Anonymity, DoS Attack, Off-line Password Guessing Attack에 관한 보안 취약점을 가지고 있다는 것을 밝혀내었다. 본 연구 결과를 활용하여 향후 프로토콜 취약점 및 새로운 프로토콜 제안에 필요한 분석자료가 될 수 있을 것이라 판단한다.

참고문헌

[1] 김병훈, 신제철, 하옥현, "침입탐지시스템 탐지성능 향상 위한 해시기반 패턴 매칭 시스템," 융합보안논문지, 제9권, 제4호, pp.21-27, 2009.

[2] 김성환, 김동성, 송영덕, 박종서, "유비쿼터스 컴퓨팅 보안을 위한 경량 블록 암호 구현," 융합보안논문지, 제5권, 제3호, pp.23-32, 2005.

[3] 황득영, 김진묵 "공장 자동화를 위한 RFID 경량 암호 프로토콜에 관한 연구," 융합보안논문지, 제16권, 제7호, pp.173-180, 2016.

[4] 백용진, 홍석원, 김상복, "클라우드 환경에서 네트워크 가용성 개선을 위한 대칭키 암호화 기반 인증 모델," 융합보안논문지, 제19권, 제5호, pp.47-53, 2019.

[5] 노시춘, "DES(Data Encryption Standard) 속성 진단과 강화된 대칭키 암호 알고리즘 적용방법," 융합보안논문지, 제12권, 제4호, pp.85-90, 2012.

[6] W.-H Yang and S.-P. Shieh, "Password authentication scheme with smart cards", Computers & Security, Vol. 18, No. 8, pp. 727-733, 1999.

[7] J.-J. Shen, C.-W. Lin, and M.-S. Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards", Computers & Security, Vol. 22, No. 7, pp. 591 - 595, 2003.

[8] E.-J. Yoon, E.-K. Ryu, and K.-Y. Yoo,

"Security of Shen et al.'s timestamp-based password authentication scheme," International Conference on Computational Science and Its Applications, Springer, pp. 665 - 671, 2004..

[9] C.-C. Yang and R.-C. Wang, "An improvement of security enhancement for the timestamp-based password authentication scheme using smartcards," ACM SIGOPS Operating Systems Review, Vol. 38, No. 3, pp.91 - 96, 2004.

[10] X. Wang, J. Zhang, W. Zhang, and M. Khan, "Security improvement on the timestamp-based password authentication scheme using smart cards," in 2006 IEEE International Conference on Engineering of Intelligent Systems. IEEE, pp.1 - 3, 2006.

[11] J.-Y. Liu, A.-M. Zhou, and M.-X. Gao, "A new mutual authentication scheme based on nonce and smart cards," Computer Communications, Vol. 31, No. 10, pp.2205 - 2209, 2008.

[12] A. K. Awasthi, K. Srivastava, and R. Mittal, "An improved timestamp-based remote user authentication scheme," Computers & Electrical Engineering, Vol. 37, No. 6, pp.869 - 874, 2011.

[13] T.-H. Chen, G. Horng, and K.-C. Wu, "A secure YS-like user authentication scheme," Informatica, Vol. 18, No. 1, pp.27 - 36, 2007.

[14] Y. An, "Security enhancements of an improved timestamp-based remote user authentication scheme," in Computer Applications for Security, Control and System Engineering. Springer, pp.54 - 61, 2012.

[15] S. Kumari, M. K. Gupta, M. K. Khan, and X. Li, "An improved timestamp-based password authentication scheme: comments, cryptanalysis, and improvement," Security and Communication Networks, Vol. 7, No. 11, pp.1921 - 1932, 2014.

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

[17] J. Xu, W.-T. Zhu, and D.-G. Feng, "An improved smart card based password authentication scheme with provable security," Computer Standards & Interfaces, Vol. 31, No. 4, pp.723 - 728, 2009

[18] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Annualinternational cryptology conference. Springer, pp. 388 - 397, 1999

[19] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-cardsecurity under the threat of power analysis attacks," IEEE Transactionson Computers, Vol. 51, No. 5, pp.541 - 552, 2002.

[20] R. Amin, S. Islam, M. K. Khan, A. Karati, D. Giri, and S. Kumari, "A two-factor RSA-based robust authentication system for multiserverenvironments," Security and Communication Networks, Vol. 2017, 2017.

〔저자소개〕

서 한 나 (Han-na Seo)
2021년 3월 ~ 현재 인제대학교 컴퓨터공학부 학사과정
email : sicehot6@gmail.com

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
2021년 3월 ~ 현재 인제대학교 AI융합대학 조교수
email : cys2020@inje.ac.kr