Journal of Digital Convergence
Vol. 18. No. 5, pp. 249-256, 2020

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2020.18.5.249

SIP를 위한 Qiu등의 개선된 패스워드 인증 기법에 대한 보안 분석 및 강화 기법

김현성[1,2]
[1]경일대학교 컴퓨터사이언스학부 교수
[2]말라위대학교 수학과 교수

Cryptanalysis and Remedy Scheme on Qiu et al.'s Enhanced Password Authentication Scheme for SIP

Hyunsung Kim[1,2]
[1]Professor, School of Computer Science, Kyungil University
[2]Professor, Mathematical Sciences Department, University of Malawi

요 약 세션 시작 프로토콜(Session Initiation Protocol, SIP)은 인터넷 프로토콜 기반 네트워크에서 세션 생성과 관리 및 종료하는데 사용되는 신호 프로토콜이다. 이를 통해 음성 기반 전자 상거래나 인스턴트 메시징과 같은 서비스를 구현할 수 있다. 최근에 Qiu등은 SIP를 위한 개선된 패스워드 인증 기법을 제안하고 모든 알려진 공격에 안전하다고 주장하였다. 하지만, 본 논문에서는 Qiu등의 인증 기법이 오프라인 패스워드 추측 공격에 취약하고 서비스 거부의 문제가 있음을 도출한다. 또한, 이러한 문제를 해결하기 위한 강화된 패스워드 인증 기법을 제안한다. 제안한 기법은 서버의 검증자를 사용하지 않고 타원곡선암호의 기본 연산을 활용한다. 정형화된 보안 검증 툴인 ProVerif에 기반한 보안 검증을 제시한다. 보안 분석을 통해 본 논문에서 제안한 강화된 인증 기법이 SIP 상의 다양한 보안 공격에 안전함을 보인다.

주제어 : 세션초기화프로토콜, 인증, 타원곡선암호시스템, 프라이버시, 패스워드

Abstract The session initiation protocol (SIP) is a signaling protocol, which is used to controlling communication session creation, manage and finish over Internet protocol. Based on it, we can implement various services like voice based electronic commerce or instant messaging. Recently, Qiu et al. proposed an enhanced password authentication scheme for SIP. However, this paper withdraws that Qiu et al.'s scheme is weak against the off-line password guessing attack and has denial of service problem. Addition to this, we propose an improved password authentication scheme as a remedy scheme of Qiu et al.'s scheme. For this, the proposed scheme does not use server's verifier and is based on elliptic curve cryptography. Security validation is provided based on a formal validation tool ProVerif. Security analysis shows that the improved authentication scheme is strong against various attacks over SIP.

Key Words : Session Initiation Protocol, Authentication, Elliptic Curve Cryptosystem, Privacy, Password

*This work was partly supported by project for the Collabo R&D Program between Industry, Academy, and Research Institute funded Korea Ministry of SMEs and Startups in 2019 (S2754028) and NRF funded by the Ministry of Education [NRF-2017R1D1A1B04032598]
*Corresponding Author : Hyunsung Kim(kim@kiu.ac.kr)
Received March 11, 2020 Revised April 21, 2020
Accepted May 20, 2020 Published May 28, 2020

1. 서론

세션 시작 프로토콜(Session Initiation Protocol, SIP)은 인터넷 기반 멀티미디어 서비스의 세션을 위한 시그널링 프로토콜(Signaling Protocol)이다. SIP의 역할은 메시지 교환 주체들 간 세션을 제어하기 위한 정보를 교환하는데 있다[1-4]. 하지만, SIP는 기본적인 보안을 제공하지 않기 때문에 다양한 보안 및 프라이버시 공격에 취약하다[5-6].

Franks등이 SIP를 위한 첫 인증 기법을 제안한 이후로 다양한 인증 기법들이 제안되었다[6-11]. 2014년에 Tu등은 기존의 다양한 SIP 인증 기법의 문제점을 해결하기 위한 스마트카드를 이용한 기법을 제안하였다[8]. 하지만 Farash는 Tu등의 기법이 서버 가장 공격에 취약함을 보이고 이를 해결하기 위한 새로운 기법을 제안하였다[9]. Chaudhry등도 Tu등의 기법이 서버 가장공격과 재전송 공격 그리고 서비스 거부 공격에 취약하고 사용자 익명성을 제공하지 못함을 보였다[10]. 특히, Chaudhry등은 Farash의 개선된 기법 또한 재전송 공격에 취약하고 사용자 익명성 또한 제공하지 못함을 보이고 익명성을 제공하기 위한 새로운 기법을 제안하였다. 최근에 Qiu등은 Farash의 기법이 가장 공격에 취약하고 스마트 카드 소유자 검증을 제공하지 못하며 완전한 전방향 보안을 제공하지 못함을 보이고 이를 해결하기 위한 개선된 기법을 제안하였다[11].

본 논문에서는 Qiu등의 패스워드 인증 기법의 보안 분석을 제시한다. 먼저 Qiu등의 인증 기법은 오프라인 패스워드 추측 공격에 취약함을 보이고 Qiu등의 기법의 설계 결함으로 인해 서비스 거부가 가능함을 보인다. 이러한 문제를 해결하기 위해 서버의 검증자를 사용하지 않고 타원곡선암호(Elliptic Curve Cryptography)에 기반한 강화된 패스워드 인증 기법을 제안한다. 본 논문에서 제안한 인증 기법은 Qiu등의 기법 및 기존 SIP를 위한 인증 기법의 문제들을 효율적으로 해결할 수 있음을 보안 검증 및 보안 분석에서 보인다.

2. Qiu등의 개선된 패스워드 인증 기법

Qiu등은 기존 SIP를 위한 인증 기법에 대한 제약 사항을 극복하기 위해 개선된 패스워드 인증 기법을 제안하였다[11]. Qiu등의 인증 기법은 시스템 초기화 단계, 등록 단계, 로긴과 상호 인증 단계, 그리고 패스워드 업데이트 단계로 구성된다. Table 1은 본 논문에서 사용하는 기호를 정의한다.

Table 1. Notations

Notation	Descriptions
E	An elliptic curve
P	A generator over E
W_x, W_y	x and y coordinates of W
S	Server
U	Patient/user
SC	Smart card
ID	Identity of U
PW	Password of U
c_u, a_u	Random numbers of U
k	Secret private key of S
G	Public key of S
b, c_s	Random numbers of U
n_0	An integer of $2^4 \le n_0 \le 2^8$
$\|\|$	The string concatenation operation
$\oplus$	The bitwise XOR operation
$h(\cdot)$	Collision free one way hash function
$\rightarrow$	An insecure channel
$\Rightarrow$	A secure channel
?=	Equivalency verification
sk	Session key between U and S

2.1 시스템 초기화 단계

서버 S는 유한필드 F_p 상의 타원곡선 E와 난수 $k \in Z_p^*$ 그리고 일방향 해쉬 함수 $h(\cdot)$를 선택한다. S는 E의 생성자인 P를 이용하여 $G=kP$를 S의 공개키로서 계산한다. S는 $\{E, P, G, h(\cdot)\}$공개하고 k를 S의 개인키로서 유지한다.

2.2 등록 단계

단계 1. 사용자 U는 자신의 식별자 ID를 선택한다.

단계 2. $U \Rightarrow S$:$\{ID\}$.

단계 3. U로부터 등록 메시지를 받은 후 S는 난수 a_u, $b \in Z_p^*$를 선택하고 초기 패스워드 PW_0를 이용하여 $N=h(k||ID||b)$과 $VPW=h(PW_0||a_u||ID)$를 계산한다. 계속하여 S는 $r_u=N \oplus VPW$와 $A_u=h((h(ID) \oplus VPW) \bmod n_0)$를 계산하고 $\{ID, b\}$를 데이터베이스에 저장한다.

단계 4. $S \Rightarrow U$:$\{SC, PW_0\}$. 여기서 SC는 $\{r_u, P, a_u, A_u, b, G, n_0, h(\cdot)\}$를 저장한다.

단계 5. S로부터 SC를 받은 후, U는 패스워드 업데이트 단계를 이용하여 초기 패스워드를 즉시 바꾼다.

2.3 로긴과 상호 인증 단계

S에 성공적으로 등록된 U는 서비스를 활용하기 위하여 로긴 요청을 S에게 다음과 같이 보낸다.

단계 1. U는 SC를 카드 리더기에 넣고 ID와 PW를 입력한다.

단계 2. SC는 $VPW=h(PW||a_u||ID)$와 $A_u'=h((h(ID)\oplus VPW') \bmod n_0)$를 계산한다. SC는 저장된 A_u와 A_u'를 비교함으로서 사용자의 적법성을 체크한다. 적법하지 않다면 현재 세션을 종료한다.

단계 3. SC는 난수 $c_u\in Z_p^*$를 선택하고 $N=r_u\oplus VPW'$, $V=c_uP$, $W=c_uG$, $f_u=ID\oplus W_x$, $z_u=h(ID||W_y||f_u||N)$를 계산한다.

단계 4. $U \rightarrow S$:{V, f_u, z_u}.

단계 5. U로부터 {V, f_u, z_u}를 받은 후 S는 $W^*=kV$와 $ID'=f_u\oplus W_x^*$를 계산한 후 데이터베이스를 검색함으로서 ID' ?= ID 를 체크한다. 만약 이들 값이 일치하지 않는다면 S는 사용자의 패스워드 입력이 틀렸다고 판단한다. 틀린 시도가 임계값을 초과한다면 S는 SC가 공격자에 의해 사용되었다고 판단하고 U가 재등록 할 때까지 SC의 서비스 접근을 잠근다. 그렇지 않다면 S는 $z_u^*=h(ID'||W_y^*||f_u||N)$를 계산하고 z_u^* ?=z_u 검증한다. 검증을 성공하면 S는 난수 c_s, $t\in Z_p^*$를 생성하고 $V_s=c_sV$, $sk=h(N||W_x^*||G||V_s||ID||t)$, $Auth_s=h(t||sk||N)$를 계산한다.

단계 6. $S \rightarrow U$:{c_sG, $Auth_s$, t}.

단계 7. {c_sG, $Auth_s$, t}를 받은 후 U는 $V_s^*= c_u(c_sG)$, $sk^*=h(N||W_x^*||G||V_s^*||ID||t)$, $Auth_s^*=h(t||sk^*||N)$를 계산한 후 $Auth_s^*$?= $Auth_s$를 체크한다. 만약 이들 값이 일치하지 않는다면 세션을 종료한다. 그렇지 않다면 U는 세션키 sk^*를 수락한다. 그런 후 U는 $Auth_u=h(t+1||sk^*||N||V_s^*||ID)$를 계산한다.

단계 8. $U \rightarrow S$:{$Auth_u$}.

단계 9. {$Auth_u$}를 받은 후 S는 $Auth_u^*=h(t+1||sk||N||V_s||ID)$를 계산한 후 $Auth_u^*$?= $Auth_u$를 체크한다. 만약 이들 값이 일치한다면 U는 인증된다.

단계 10. 마지막으로 U와 S는 하나의 동일한 세션키 $sk=sk^*$에 동의한다.

2.4 패스워드 업데이트 단계

이 단계는 사용자 U가 자신의 패스워드를 변경하고자 할 때 U와 SC사이에서 다음과 같이 수행한다.

단계 1. 먼저 U는 SC를 카드 리더기에 넣고 ID'와 PW' 그리고 새로운 패스워드 PW^{new}를 입력한다.

단계 2. SC는 $VPW'=h(PW||a_u||ID)$와 $A_u'=h((h(ID)\oplus VPW') \bmod n_0)$를 계산한다. SC는 저장된 A_u와 A_u'를 비교함으로서 사용자의 적법성을 체크한다. 적법하지 않다면 SC는 U의 패스워드 변경을 거절한다.

단계 3. 그렇지 않다면 SC는 난수 $a_u^{new}\in Z_p^*$를 선택하고 $VPW^{new}=h(PW^{new}||a_u^{new}||ID)$, $r_u^{new}=VPW\oplus VPW^{new}$, $A_u^{new}=h((h(ID)\oplus VPW^{new}) \bmod n_0)$를 계산한다. 마지막으로 SC는 a_u^{new}, r_u^{new}, A_u^{new}를 SC에 저장된 a_u, r_u, A_u로 각각 대체한다.

3. Qiu등의 기법에 대한 보안 분석

Qiu등은 공개키 암호시스템의 원리를 기반으로 2장에서 살펴본 바와 같이 새로운 인증 기법을 제안하고 AVISPA 시뮬레이션을 제시하였으며, 이 기법이 모든 알려진 공격에 안전하다고 주장하였다. 하지만, 본 장에서는 Qiu등의 인증 기법이 오프라인 패스워드 추측 공격에 취약하고 적법한 서버가 인증에서 항상 실패함으로서 서비스 거부되는 문제점을 보인다.

3.1 오프라인 패스워드 추측 공격

Qiu등의 인증 기법에 대한 오프라인 패스워드 추측 공격을 위해 다음과 같은 두 가지 가정을 제시한다. 공격자 U_a는 사용자 U의 스마트카드 SC를 훔치거나 일시적으로 접근하여 그 카드 내에 저장되어 있는 정보 {r_u, P, a_u, A_u, b, G, n_0, $h(\cdot)$}를 추출할 수 있다고 가정한다 [12]. 또한 U_a는 서버 S에 침투하여 데이터베이스에 저장된 검증자 {ID, b}를 획득할 수 있다고 가정한다 [13]. 이러한 정보를 획득한 U_a는 다음과 같은 단계로 U의 패스워드 추측 공격을 오프라인으로 진행할 수 있다.

단계 1. 먼저 U_a는 검증자 {ID, b}로부터 i ($1\le i\le n$, n은 데이터베이스에 저장된 ID의 총 수)번째 후보 식별자 ID를 선택하고 패스워드 PW' 추측 공격을 수행한다.

단계 2. SC로부터 획득한 a_u와 n_0를 이용하여 $VPW'=h(PW'||a_u||ID')$와 $A_u'=h((h(ID')\oplus VPW') \bmod n_0)$를 계산한다. SC로부터 획득한 A_u와

계산한 A_u'를 비교함으로서 추측 패스워드의 적법성을 체크한다. 적법성 체크에 실패했지만 패스워드 PW'의 크기 범주를 벗어나지 않았다면 다음 패스워드 후보자인 PW'을 선택하여 단계 2를 다시 수행한다.

단계 3. 만약 패스워드 추측 공격의 범위를 벗어난 경우 단계 1을 다시 수행한다. 하지만 계산한 A_u'를 통해 적법성 조건이 만족되면, 이때 추측된 패스워드 PW'는 U의 올바른 패스워드이고 U의 식별자가 ID_i라는 것을 의미한다. 즉, U_a의 오프라인 패스워드 추측공격이 성공한 것을 의미한다.

3.2 서비스 거부

Qiu등의 인증 기법은 적법한 서버 S가 사용자 U에 의한 인증 과정에서 항상 거절당하는 문제가 발생한다. 즉, 기법에서 서버의 적법성 제시 방법에 오류가 있어서 사용자로부터 적법한 서버가 서비스 거부(Denial of service) 당하는 문제가 존재한다. 이러한 문제가 발생하는 이유는 S와 U에서 계산하는 $V_s \neq V_s*$의 매개변수의 차이에서 발생한다.

로긴 및 상호 인증 단계의 단계 5와 단계6에서 S와 U는 다음과 같이 $V_s \neq V_s*$를 계산한다.

단계 5. S는 난수 c_s, $t \in Z_p*$를 생성하고 $V_s=c_sV$,와 관련 값 들을 계산한다. 여기서 $V=c_uP$는 단계 3에서 계산된다. 즉, $V_s=c_sV=c_sc_uP$이다.

단계 6. $\{c_sG, Auth_s, t\}$를 받은 후 U는 $V_s*= c_u(c_sG)$와 관련된 값을 계산한 후 V_s*과 연계된 값을 통해 S를 인증한다. 여기서 G는 시스템 초기화 단계에서 $G=kP$로 설정된 S의 공개키이다. 즉, $V_s*=c_u(c_sG)= c_uc_skP$이다.

4. 강화된 패스워드 인증 기법

본 장에서는 Qiu등이 제안한 패스워드 인증 기법의 보안 문제점을 해결하기 위한 강화된 패스워드 인증 기법을 제안한다. 강화된 인증 기법은 서버에 검증자를 보관하지 않도록 설계된다. 강화된 인증 기법도 시스템 초기화 단계, 사용자 등록 단계, 로긴 및 상호인증 단계 그리고 패스워드 변경 단계로 구성된다.

4.1 시스템 초기화 단계

서버 S는 160비트 이상인 p의 유한필드 F_p 상의 타원곡선 E와 개인키로서 난수 $k \in Z_p*$ 그리고 임의의 길이의 입력($\{0, 1\}*$)을 고정된 길이의 출력(Z_p*)으로 매핑하는 일방향 해쉬 함수 $h(\cdot)$를 선택한다. S는 E의 그룹 생성자인 P를 이용하여 공개키 $G=kP$를 계산한다. S는 $\{E, P, G, h(\cdot)\}$ 공개하고 k를 비밀로 유지한다.

4.2 등록 단계

S로부터 서비스를 등록하고자 하는 U는 다음과 같이 S에 등록 요청을 보낸다.

단계 1. 사용자 U는 자신의 식별자 ID와 패스워드 PW를 선택한다. 난수 $b \in Z_p*$를 선택하고 $VPW=h(PW||b||ID)$를 계산한다.

단계 2. $U \Rightarrow S$:$\{ID, VPW\}$.

단계 3. U로부터 $\{ID, VPW\}$를 받은 후 S는 $N=h(k||ID)$과 $r_u=N \oplus VPW$ 그리고 $A_u= h((h(ID) \oplus VPW) \bmod n_0)$를 계산한다. S는 U를 위해 새로운 SC를 발급하고 $\{r_u, P, A_u, G, n_0, h(\cdot)\}$를 저장한다.

단계 4. $S \Rightarrow U$:$\{SC\}$.

단계 5. S로부터 SC를 받은 후, U는 $MB=h(ID||PW) \oplus b$를 계산하고 SC에 저장한다.

4.3 로긴과 상호 인증 단계

U는 S의 서비스를 활용하기 위하여 Fig. 1과 같이 로긴 요청을 S에게 다음과 같이 보낸다.

단계 1. U는 SC를 카드 리더기에 넣고 ID'와 PW'를 입력한다.

단계 2. SC는 $b'=MB \oplus h(ID'||PW')$과 $VPW'= h(PW'||b'||ID')$ 그리고 $A_u'=h((h(ID') \oplus VPW') \bmod n_0)$를 계산한다. SC는 $A_u?=A_u'$를 체크함으로서 사용자의 적법성을 체크한다. 적법하지 않다면 현재 세션을 종료한다.

단계 3. SC는 난수 $c_u \in Z_p*$를 선택하고 $N'=r_u \oplus VPW'$, $V=c_uP$, $W=c_uG$, $f_u=ID' \oplus W_x$, $z_u =h(ID'||W_y||f_u||N')$를 계산한다.

단계 4. $U \rightarrow S$:$\{V, f_u, z_u\}$.

단계 5. U로부터 $\{V, f_u, z_u\}$를 받은 후 S는 $W*=kV$와 $ID*=f_u \oplus W_x*$와 $z_u*=h(ID*||W_y*||f_u||N)$를 계산하고 $z_u* ?=z_u$ 검증한다. 검증이 실패하면

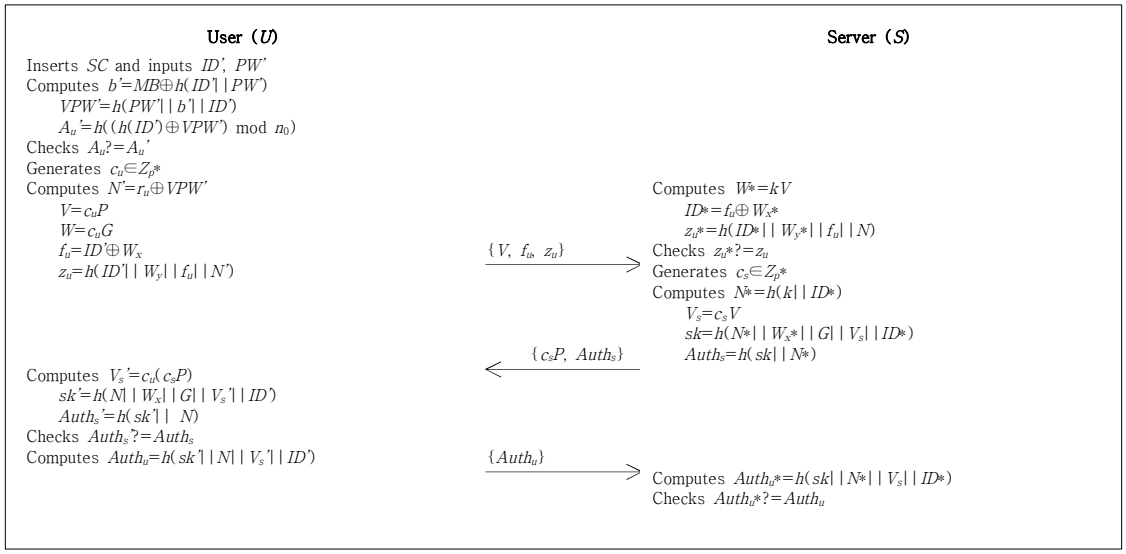

Fig. 1. Login and mutual authentication phase

세션을 종료한다. 검증 성공은 인증 성공을 의미하고 S는 난수 $c_s \in Z_p^*$를 생성하고 $N^*=h(k||ID^*)$, $V_s= c_sV$, $sk=h(N^*||W_x^*||G||V_s||ID^*)$, $Auth_s= h(sk||N^*)$를 계산한다.

단계 6. $S \rightarrow U$:{c_sP, $Auth_s$}.

단계 7. {c_sP, $Auth_s$}를 받은 후 U는 $V_s'=c_u(c_sP)$, $sk'=h(N'||W_x||G||V_s'||ID')$, $Auth_s'=h(sk'||N)$를 계산한 후 $Auth_s' ?= Auth_s$를 체크한다. 만약 이들 값이 일치하지 않는다면 세션을 종료한다. 그렇지 않다면 U는 세션키 sk'를 수락한다. 그런 후 U는 $Auth_u=h(sk'||N'||V_s'||ID')$를 계산한다.

단계 8. $U \rightarrow S$:{$Auth_u$}.

단계 9. {$Auth_u$}를 받은 후 S는 $Auth_u^*=h(sk||N^*||V_s||ID^*)$를 계산한 후 $Auth_u^* ?= Auth_u$를 체크한다. 만약 이들 값이 일치한다면 U는 인증된다.

단계 10. 마지막으로 U와 S는 하나의 동일한 세션키 $sk=sk$'에 동의한다.

4.4 패스워드 업데이트 단계

U는 자신의 패스워드를 변경하고자 할 때 SC를 이용하여 다음과 같이 수행한다.

단계 1. 먼저 U는 SC를 카드 리더기에 넣고 ID'와 PW' 그리고 새로운 패스워드 PW^{new}를 입력한다.

단계 2. SC는 $b'=MB⊕h(ID'||PW')$과 $VPW'= h(PW'||b'||ID')$ 그리고 $A_u'=h((h(ID')⊕ VPW') \bmod n_0)$를 계산한다. SC는 $A_u ?= A_u'$를 체크함으로서 사용자의 적법성을 체크한다. 적법하지 않다면 SC는 U의 패스워드 변경을 거절한다.

단계 3. 그렇지 않다면 SC는 $MB^{new}=b'⊕h(ID'||PW^{new})$, $VPW^{new}=h(PW^{new}||b'||ID')$, $r_u^{new}=VPW⊕VPW^{new}$, $A_u^{new}= h((h(ID')⊕VPW^{new}) \bmod n_0)$를 계산한다. 마지막으로 SC는 MB^{new}, r_u^{new}, A_u^{new}를 SC에 저장된 MB, r_u, A_u로 각각 대체한다.

5. 보안 검증

ProVerif는 정형화된 Dolev-Yao모델에 기반한 자동화된 암호학적 기법 검증 툴이다[14]. ProVerif를 통해서 상호 인증과 보안성 및 프로세스들 간의 등가성과 같은 인증 기법의 보안적 특성들을 성공적으로 체크할 수 있다. 제안한 기법의 ProVerif 코드는 https://github.com/hs-kim-andre/kim-kiu.ac.kr/blob/master/myproverif.pv에서 확인할 수 있다. Fig. 2는 ProVerif 버전 1.96을 사용한 검증 결과를 보여준다.

제안한 기법의 보안 검증을 위하여 다음 단계를 순차적으로 진행하였다. 먼저, U와 S간 공개 통신 채널 ch를 정의하였다. 세션키 sk의 안전성을 검증하기 위하여 $svalueA$와 $svalueB$가 사용되었다. 또한 제안한 기법의

상호 인증을 검증하기 위하여 4개의 이벤트 SUbegin(entity), USbegin(entity), SUend(entity), USend(entity)가 선언되었다. 그런 후, U와 S 각각의 인증 단계에 대한 데모를 진행하였다. 마지막으로, 전체 프로그램에 대한 모델을 제시하였다.

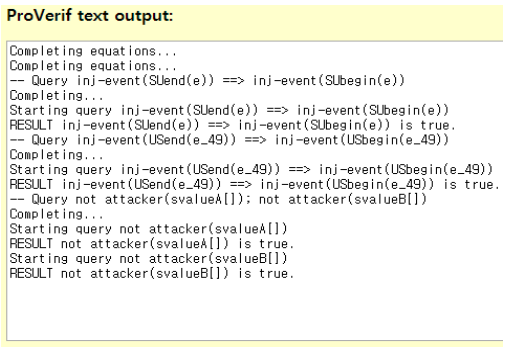

Fig. 2. Simulation results for the ProVerif

Fig. 2는 제안한 기법이 세션키의 안전성을 달성하였고 개체 간 상호 인증을 성공적으로 달성하였음을 보여준다.

6. 보안 분석

본 장에서는 강화된 패스워드 인증 기법이 Qiu등의 기법에서 노출된 보안 문제를 효율적으로 해결함을 보인다. 또한, 제안한 기법이 일반적인 보안 특징을 고려함을 보인다. 효율적인 분석을 위해서 공격자 U_a가 공개 통신 채널을 감시할 수 있고 주고 받는 메시지의 삽입과 삭제 그리고 변경할 수 있는 능력이 있다고 가정한다. 특히, U_a가 스마트카드에 저장된 유용한 정보를 획득할 수 있다고 가정한다. Table 2는 제안한 인증 기법과 기존의 기법들과의 보안 특성에 대한 비교를 보여준다.

Table 2. Comparison of security features

Feature / Scheme	S1	S2	S3	S4	S5
Tu et al. [8]	No	Yes	Yes	No	Yes
Farash [9]	No	Yes	Yes	No	Yes
Chaudhry et al. [10]	Yes	Yes	Yes	No	Yes
Qiu et al. [11]	No	Yes	Yes	Yes	No
Proposed scheme	Yes	Yes	Yes	Yes	Yes

S1: Resists off/on-line password guessing attack; S2: Provides mutual authentication; S3: Provides perfect forward secrecy; S4: Provides user anonymity and user un-traceability; S5: Resists denial-of-service attack

6.1 패스워드 추측 공격

제안한 기법에서 패스워드 추측 공격에 성공하기 위해서 U_a는 3.1절에서 살펴본 바와 같이 SC에 저장된 정보 $\{MB, r_u, P, A_u, G, n_0, h(\cdot)\}$를 알더라도 성공적인 로긴 메시지를 만들기 위해서는 정확한 ID와 PW를 알아야 한다. 하지만 U_a가 $A_u ?= A_u'$ 검증을 성공할 수 있는 ID와 PW를 동시에 추측하는 것은 "fuzzy-verifier"에서 제시된 것처럼 불가능하다[15]. 즉, 본 논문에서 제안한 기법은 S에 U의 식별자인 ID를 한정할 수 있는 검증자를 사용하지 않기 때문에 Qiu등의 기법에서 존재하는 패스워드 추측 공격에 효율적으로 대응할 수 있다.

6.2 상호 인증

제안한 기법은 S와 U간의 상호 인증을 제공한다. S는 $z_u^* ?= z_u$과 $Auth_u^* ?= Auth_u$ 검증을 통해서 U를 인증한다. 반면에 U는 $Auth_s' ?= Auth_s$ 검증을 통해서 S를 인증한다.

즉, 본 논문에서 제안한 기법에 대한 U_a의 공격은 적법한 z_u나 $Auth_u$ 아니면 $Auth_s$에 대한 계산에 기반한다. 하지만 U_a가 관련된 검증을 성공하기 위해서는 N에 대한 정보를 알아야 한다. 즉, 제안한 기법의 상호 인증은 해쉬함수의 일방향성에 기반한 안전성을 제공한다.

6.3 전방향 보안

전방향 보안은 U_a가 S의 개인키인 k를 획득할 수 있다고 하더라도 세션키인 sk를 알 수 없도록 함으로서 제공된다. U_a가 한 세션의 메시지인 $\{V, f_u, z_u\}$와 $\{c_sP, Auth_s\}$ 그리고 $\{Auth_u\}$를 획득할 수 있다. 이 세션의 메시지를 통해서 $sk=h(N||W_x||G||V_s||ID)$를 계산하기 위해서는 V와 c_sP를 통해서 V_s를 계산할 수 있어야 한다. 하지만 U_a가 V와 c_sP로부터 c_u와 c_s를 계산하는 문제에 직면한다. 이러한 문제를 타원곡선 이산대수라고 부르고 현재까지 효과적으로 이러한 문제를 푸는 방법이 존재하지 않는다. 또한 U_a가 V로부터 $V_s=c_uc_sP$를 계산하는 것 또한 타원곡선 이산대수 문제에 기반하는 어려운 문제이다. 그러므로 제안한 기법은 전방향 보안을 제공한다.

6.4 사용자 익명성 및 비추적성

제안된 인증 기법에서는 U_a가 한 세션의 메시지인 $\{V, f_u, z_u\}$와 $\{c_sP, Auth_s\}$ 그리고 $\{Auth_u\}$를 획득할 수 있다고 하더라도 U의 식별자를 알 수 있는 효율적인 방법이 없다. 이를 위해서는 $f_u=ID \oplus W_x$를 통해 ID를 추출하는

방법 밖에 없다. 이를 위해서 U_a는 $V=c_uP$로부터 $W=c_uG=c_ukP$를 계산할 수 있어야 한다. 하지만 V로부터 W를 계산하기 위해서는 V로부터 c_u를 계산하거나 $G=kP$로부터 k를 계산해야 하는 타원곡선 이산대수의 문제에 기반하는 어려운 문제이다. 즉, 본 논문에서 제안한 기법은 사용자 익명성을 제공한다.

또한, 제안한 기법은 모든 메시지에 난수 관련된 값을 이용함으로서 세션간의 비연결성을 제공한다. 즉, U_a가 여러 세션의 메시지를 획득하고, 각 세션의 메시지들인 $\{V, f_u, z_u\}$와 $\{c_sP, Auth_s\}$ 그리고 $\{Auth_u\}$를 통해 세션간 연계관계를 확인할 수 있는 효율적인 방법이 없다. 이를 위해서는 f_u를 통해 메시지에 포함된 U의 식별자를 확인할 수 있어야 한다. 하지만, 이는 익명성에서 논의한 것처럼 타원곡선 이산대수 문제이다.

7. 결론

본 논문에서는 Qiu등의 개선된 패스워드 인증 기법이 오프라인 패스워드 추측 공격 취약성과 서비스 거부에 취약함을 보이고 이를 해결하기 위한 강화된 인증 기법을 제안하였다. 본 논문에서 제안한 인증 기법은 서버의 검증자를 이용하지 않고 타원곡선암호에 기반 한 연산을 활용함으로서 안전성을 보증하였다. 특히, 정형화된 보안 검증 툴인 ProVerif에 기반한 보안 검증 결과를 통해 본 논문에서 제안한 인증 기법이 안전하게 세션키를 공유할 수 있고 상호 인증을 제시함을 확인하였다. 이를 통하여 강화된 패스워드 인증 기법이 Qiu등의 인증 기법에 존재하는 문제점을 효율적으로 해결할 수 있음을 보였다.

향후 연구로는 본 논문에서 제안한 기법에 대한 SIP 적용을 위한 구체적인 노력이 추가로 제시되어야 할 필요가 있을 것이다.

REFERENCES

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley & E. Schooler. (2002). SIP: Session Initiation Protocol. *RFC 3261*.

[2] T. Robles, R. Ortiz & J. Salvachja. (2003). Porting the session initiation protocol to IPv6. *IEEE Internet Computing*, *7(3)*, 43-50.

[3] C. Shen, F. Shen, Z. Wu & J. Luo. (2009). Application of session initiation protocol to networked sensor interfaces. *Computer Standards & Interfaces*, *31(2)*, 454-457.

[4] E. Y. Ha. (2014). A Scalable Management Method for Asterisk-based Internet Telephony System. *Journal of Digital Convergence*, *12(8)*, 235-242.

[5] H. U. Kim, H. J. Kim, J. H. Kang & M. S. Jun. (2016). A Study on Analysis and Countermeasure of Security Threat in NFC. *Journal of Digital Convergence*, *14(12)*, 183-191.

[6] H. Kim & S. W. Lee. (2010). Modified Authenticated Key Exchange Protocol for SIP using ECC. *Journal of Security Engineering*, *7(4)*, 279-286.

[7] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen & L. Stewart. (1999). HTTP Authentication: Basic and Digest Access Authentication. *RFC 2617*.

[8] H. Tu, N. Kumar, N. Chilamkurti & S. Rho. (2015). An Improved Authentication Protocol for Session Initiation Protocol using Smart Card. *Peer-to-peer Network and Application*, 8(5), 903-910.

[9] M. S. Farash. (2016). Security Analysis and Enhancements of An Improved Authentication for Session Initiation Protocol with Provable Security. *Peer-to-peer Network and Application*, 9, 82-91.

[10] S. A. Chaudhry, H. Naqvi, M. Sher, M. S. Farash & M. U. Hassan. (2017). An Improved and Provably Secure Privacy Preserving Authentication Protocol for SIP. *Peer-to-peer Network and Application*, *10*, 1-15.

[11] S. Qiu, G. Xu, H. Ahmad & Y. Guo. (2018). An Enhanced Password Authentication Scheme for Session Initiation Protocol with Perfect Forward Secrecy. *Plos One*, *13(3)*, e0194072.

[12] S. Y. Jung & J. Kwak. (2013). Smart Card and Dynamic ID Based Electric Vehicle User Authentication Scheme. *Journal of Digital Convergence*, *11(7)*, 141-148.

[13] H. W. Choi, S. Kim & M. Ryoo. (2019). Cryptanalysis and Solution on Secure Communication Scheme for Healthcare System using Wearable Devices. *Journal of Digital Convergence*, *17(2)*, 187-194.

[14] B. Blanchet. (2001). An efficient cryptographic protocol verifier based on prolog rules. *Proc. of the 14th IEEE workshop on Computer Security Foundations*, 82-96.

[15] D. Wang & P. Wang. (2016). Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound. *IEEE Transactions on Dependable and Secure Computing*, *15(4)*, 708-722.

김 현 성(Hyunsung Kim) [정회원]

· 2002년 2월 : 경북대학교 컴퓨터공학과(공학박사)
· 2002년 3월 ~ 현재 : 경일대학교 사이버보안학과 교수
· 2015년 12월 ~ 현재 : 말라위대학교 수학과 방문교수
· 관심분야 : 인지무선네트워크 보안, 네트워크 보안, 암호 프로토콜, 암호구현, 정보보호
· E-Mail : kim@kiu.ac.kr