스마트카드를 이용한 패스워드 기반 인증시스템 정형분석

(Formal Analysis of Authentication System based on Password using Smart Card)

김 현 석 † 김 주 배 † 정 연 오 † 한 근 희 †† 최 진 영 †††
(Hyun-Seok Kim) (Ju-Bae Kim) (Yeon-Oh Jeong) (Keun-Hee Han) (Jin-Young Choi)

요 약 인터넷의 범용적인 사용으로 많은 사용자들이 분산된 컴퓨팅 환경에서 원격 서버에 접속하는 일이 빈번해 지고 있다. 하지만 인증된 보호시스템 없이 안전하지 않은 채널을 통한 데이터의 전송은 재생공격이나 오프라인 패스워드 공격 및 가장공격등과 같은 문제점들에 노출되어 있다. 이에 따라 악의적인 공격들을 막기 위해 스마트카드를 이용한 인증프로토콜들에 대해 활발히 연구되고 있다. 본 논문은 패스워드 기반 사용자 인증시스템의 취약성을 분석하고 이에 대해 개선된 사용자 인증 시스템을 제안한다.

키워드 : 스마트카드, 패스워드 인증, 오프라인 추측공격, 정형검증

Abstract Due to widely use of internet, a lot of users frequently access into remote server in distributed computing environment. However, transmitting the information using vulnerable channel without authentication security system can be exposed to replay attack, offline password attack, and impersonation attack. According to this possibility, there is research about authentication protocol to prevent these hostile attacks using smart card. In this paper, we analyze vulnerability of user authentication system based on password and propose modified user authentication system.

Key words : Smart card, Password authentication, Offline guessing attack, Formal verification

1. 서 론

최근 유비쿼터스 컴퓨팅 환경에서는 개인 정보보호 및 프라이버시에 관심이 대두되고 있다. 특히 스마트카드를 이용한 원격 인증 시스템에서 개인정보보호를 위한 일환으로 사용자 인증 시스템에 대한 연구가 진행되고 있다[1,2]. 대표적으로 패스워드와 키기반의 인증 프로토콜이 있는데 두 기법 모두 스마트카드를 이용하여 보안시스템의 안전성을 보장하고자 하였다[3-6].

위 인증기법 중 Bellovin과 Merritt[7]는 패스워드 추측 공격에 대항할 수 있는 패스워드 기반의 EKE (Encrypted Key Exchange) 기법을 제안하였다. 이 기법은 인증을 위해 사용자의 패스워드를 서버에 저장하였는데, 이 경우 서버의 패스워드 파일이 공격 당할 경우 공격자가 쉽게 정당한 사용자로 위장할 수 있다. 이러한 문제점을 해결하기 위해 서버에 패스워드를 그대로 저장하는 대신 패스워드로부터 유도된 검증자(Verifier)를 저장하고 이를 이용하는 기법들[8,9]이 제안되었다. 이와 같은 연구들은 스마트카드가 temper-resistant한 성질을 갖는다는 가정 하에 활발히 연구되어지고 있다[1-15]. 특히 스마트카드를 이용한 원격 사용자 인증 프로토콜을 살펴보면, 사용자가 서버에 등록하기 위한 정보들이 존재하고, 서버는 이러한 정보들을 이용해 검증테이블에 저장 및 스마트카드에 저장한 후 이를 사용자에게 발급한다. 본 논문에서는 2008년에 Chen와 Lee[10]가 제안

· 이 논문은 2008 한국컴퓨터종합학술대회에서 '스마트카드를 이용한 패스워드 기반 인증 시스템 정형분석'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 고려대학교 컴퓨터학과
hskim@formal.korea.ac.kr
jbkim@formal.korea.ac.kr
yojeong@formal.korea.ac.kr
†† 정 회 원 : 행정안전부 정보보호정책과
keunhee@mogaha.go.kr
††† 종신회원 : 고려대학교 컴퓨터학과 교수
choi@formal.korea.ac.kr

논문접수 : 2008년 8월 25일
심사완료 : 2009년 4월 11일

한 스마트카드를 이용한 패스워드 기반의 원격 사용자 인증 프로토콜을 분석하여 그 취약성을 분석하고 개선된 프로토콜을 제안한다. 제안된 프로토콜에서는 Chen과 Lee의 프로토콜에서와 같이 처리비용이 큰 지수연산이나 비대칭 암호화 연산 없이 XOR 연산과 해쉬함수만을 사용하는 효율적인 인증절차를 수행한다는 장점을 유지하고 있다.

본 논문의 구성은 다음과 같다. 2장에서 패스워드 기반 스마트카드에 대한 관련 연구 및 보안 요구사항들을 정의하고, 3장에서는 이러한 프로토콜의 안전성을 분석하기 위한 정형검증 도구를 소개한다. 4장에서는 Chen과 Lee에 의해 제안된 프로토콜의 안전성을 분석하고 5장에서 개선된 프로토콜을 정형검증 도구를 통해 제안 및 검증한다. 마지막으로 6장에서 결론 및 향후 연구방향을 제시한다.

2. 관련 연구 및 시스템 보안 요구사항 관련 연구

패스워드 기반의 인증 프로토콜의 개념은 1992년 S. Bellovin과 M. Merritt에 의해 제안되었다[7]. 그리고, 그 후 많은 변형 프로토콜과 다양한 환경에 적용 가능한 프로토콜이 제안되었다. MacKenzie는 2002년 처음으로 임계치 PAKE를 제안[3]하였고, Perlman과 Kaufman은 PAK 프로토콜을 이용한 가상 소프트 토큰(virtual soft token)의 아이디어를 제안하였다. 또한 Victor Boyko, Philip MacKenzie와 Sarvar Patel는 PAK 프로토콜과 여러 가지 PAK 변형 프로토콜들을 제안하였으며[4,5], Diffie-Hellman 키 분배 프로토콜 기반의 PAK 프로토콜, 서버 클라이언트 모델에서 클라이언트의 계산량 감소를 위해 제안된 PAK-R, PAK-EC 프로토콜, 상호 인증 과정을 암시적인 방법으로 최적화한 PPK 프로토콜, 서버 타협에 강한 PAK-X 프로토콜 등이 그것이다. 그리고 최소한의 연산량을 위해 해쉬와 XOR 연산만으로 이루어진 Peyravian-Zunic[6] 프로토콜의 개선 프로토콜이 제안되었다. 본 논문에서 Chen과 Lee의 개선된 Peyravian-Zunic 프로토콜을 분석하고자 한다.

2.2 스마트카드 인증 시스템의 보안 요구사항

패스워드 기반의 스마트카드를 이용한 인증 시스템의 필수적인 보안 요구사항에 대해 사용자의 카드 및 카드 단말기, 서버의 구성환경에 대해 많은 문헌들[1-15]에 의해 다음과 같이 3가지 보안 요구사항을 정의할 수 있다.

- Replay attack(재생공격) : 인증단계에서 메시지 값을 차후 재전송에 이용하더라도 사용자나 공격자는 이를 인식하여 공격을 방지할 수 있다.
- Offline guessing attack(오프라인 추측 공격) : 사용자와 서버와의 통신에서 패스워드 값이 직접 보내지지 않는다. 따라서 공격자는 통신채널을 통해서 패스워드를 얻을 수 없다.
- Impersonation attack(가장 공격) : 공격자가 정당한 로그인 정보를 위조하기 위해서는 암호화된 메시지 값 안에 포함된 정당한 사용자 생성값과 서버의 비밀값을 알아야만 한다. 또한 공격자는 메시지를 도청하여 저장해 두고 재사용하여 사용자를 가장하고자 하지만 서버의 비밀값이 노출되지 않기 때문에 재사용하더라도 공격이 가능하지 않다.

3. Casper와 FDR 도구

3.1 CSP(Communicating Sequential Process)

CSP[12]는 프로세스 알제브라 언어로서, 병렬성을 갖는 통신프로토콜의 동작을 효율적으로 명세하기 위한 언어이다. 최초 일반 통신 프로토콜 및 제어 시스템의 명세를 위해 사용되어졌으나, 점차 보안 프로토콜의 명세를 위한 영역으로 확대되어 가고 있다. CSP에서 제공하는 pure synchronization(|||)과 Interleaving parallelism (||) 개념을 사용하여 분산 시스템 환경하에서 동작하는 클라이언트 서버와 공격자 모델을 정형적으로 표현할 수 있는 장점을 갖고 있다. 예를 들어, 분산시스템 환경하에서 동작하는 보안 시스템은 다음과 같이 간략히 표현할 수 있다.

SYSTEM = CLIENT1 ||| CLIENT2||| SERVER || INTRUDER

3.2 Casper(A Compiler for the Analysis of Security Protocols)

CSP(Communication Sequential Process)[12]언어를 이용하여 보안프로토콜 행위를 명세하고 FDR[13] 정형검증 도구를 이용하여 보안속성을 검증하는 연구가 진행되었다. 하지만, CSP 언어를 이용한 정형명세과정은 정형적 설계 방법에 익숙치 않은 보안프로토콜 설계자에게는 매우 복잡한 명세언어라는 단점을 갖고 있었다. 이에 따라, 보안프로토콜의 행위를 간략히 명세할 수 있도록 Casper[11] 도구가 개발되었다. Casper로 보안프로토콜의 행위와 검증속성을 명세하게 되며, 자동변환기능을 이용해 CSP 명세코드를 생성할 수 있다. 결국, 자동 생성된 CSP 명세코드를 FDR 정형검증도구에 입력하여 보안프로토콜을 검증하게 된다.

3.3 FDR(Failure Divergence Refinement)

FDR[13]도구는 CSP 명세언어를 입력으로 받아들이는 모델체킹 도구로서, CSP 명세언어로 기술된 보안프로토콜 모델이 보안성 및 인증속성과 같은 보안속성들을 만족하는지 검증하게 되며, 만일 만족하지 않을 경우에는 CSP 이벤트로 기술된 반례(counterexample)을 보여주어 보안상 취약점 분석을 용이하게 한다.

FDR 도구는 3가지의 검증방법을 지원하고 있다.

- Trace refinement : 안전성(safety) 검증
- Failures refinement : 교착상태(deadlock) 검증
- Failures - Divergence : 라이브락(livelock) 검증

4. 모델체킹을 이용한 스마트카드 인증 프로토콜 분석 및 검증 결과

이 장에서는 Chen과 Lee가 제안한 Peyravian-Zunic [6]의 개선 프로토콜을 분석하고자 한다.

4.1 스마트카드 인증 프로토콜 분석

Peyravian-Zunic[6]이 제안한 효율적인 인증 프로토콜은 추측공격이 가능함에 따라 재사용공격이 가능하게 되었으며 Chen과 Lee는 이러한 공격의 취약성을 막기 위한 개선 프로토콜을 제안하였다. 본 장에서는 스마트카드를 이용하고 XOR과 해쉬함수 연산만으로 구성되는 효율적인 인증 프로토콜을 분석한다. 제안된 프로토콜을 사용자 등록 단계, 로그인 및 인증 단계로 구별하여 설명한다. 사용자는 서버에 로그인을 하기 위해 자신의 스마트카드를 서버에 미리 등록해야 하는데 그 과정을 알아보기 위해 사용자 U의 경우를 예를 들어 설명한다.

표 1 표현법

IDi	사용자의 식별자
S	서버의 식별자
K	서버의 비밀키 값
PW	사용자의 패스워드
HPW	패스워드 요약값
r, s	사용자 및 서버의 난수값
T	사용자의 난수값의 집합
H	해쉬함수

사용자 소유 정보 : ***IDi, H(IDi(+)K), N, H(), PW***
서버 소유정보 : ***v = H(HPW(+)H(IDi(+)K)), IDi***
공개정보 : ***H(), IDi, S***
스마트카드 저장정보 : ***H(IDi(+)K), H(), N***

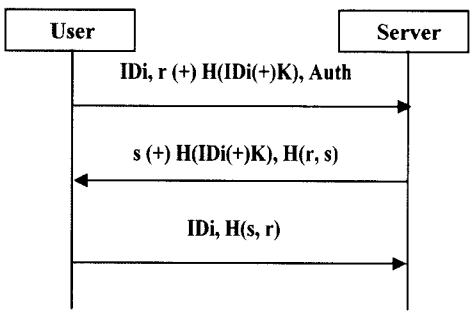

그림 1 Chen-Lee의 인증 프로토콜

[등록 단계]

Step 1. 사용자 U는 자신의 패스워드 PW와 임의의 난수값 N을 선택하여 $HPW = H(IDi, PW, N)$를 계산하고, 자신의 아이디 IDi와 함께 메시지 {IDi, HPW}를 서버 S에게 전송한다.

Step 2. S는 자신의 비밀키 K를 이용하여 $v = H(HPW(+)H(IDi(+)K))$를 계산하고, 이를 검증테이블에 IDi와 함께 저장한 후 스마트카드에 $H(IDi(+)K)$과 $H()$ 두 값을 저장하고 사용자에게 스마트카드를 발급한다.

Step 3. 스마트카드를 발급 받은 사용자 U는 스마트카드에 임의의 난수값 N을 입력하고 등록을 마친다. 사용자 U의 스마트카드에 $H(IDi(+)K)$과 $H(\ )$ 그리고 랜덤값 N이 저장되어 있기 때문에 등록을 마친 사용자 U는 서버에 로그인 하고자 할 때 더 이상 랜덤 값 N을 기억할 필요가 없고 자신의 패스워드만 기억하면 된다.

[로그인 및 인증 단계]

Step 1. U가 자신의 아이디 IDi와 패스워드 PW를 입력하면 스마트카드는 난수값 r을 선택하여 r (+) H(IDi(+) K)과 Auth = H(H(HPW(+)H(IDi(+)K)),r)을 연산 및 생성한 후 IDi값과 함께 S에게 메시지 {IDi, r (+) H(IDi(+)K), Auth}를 보낸다.

Step 2. S는 받은 메시지에서 아이디 IDi와 자신의 K를 이용하여 H(IDi(+)K)를 계산하고 r(+) H(IDi(+)K)를 XOR연산하여 r값을 도출한다. 또한 S는 도출된 r값과 자신의 검증자 v = H(HPW(+) H(IDi(+)K))를 이용하여 받은 Auth' = H(v, r)값을 생성한다. 생성된 Auth'을 U로부터 받은 Auth 값과 비교하여 일치할 경우, S는 난수값 s를 선택하고 s (+) H(IDi(+)K)를 생성하고 그렇지 않으면, 로그인 요청을 거절한다.

Step 3. 메시지를 받은 스마트카드는 s (+) H(IDi (+)K) 메시지를 H(IDi(+)K)와 XOR 연산하여 s 값을 도출해 내고 이 값을 자신의 r값과 H(r,s) 연산하여 받은 H(r,s) 값과 비교하여 타당성을 검증한 후 서버를 인증한다. 마지막으로 검증된 s값을 이용하여 IDi와 H(s,r)을 서버에게 보내어 스마트카드를 인증 받고자 한다. 서버는 받은 H(s,r)을 연산하여 자신이 받은 값과 비교 후 일치하면 인증한다.

본 논문에서는 Chen-Lee 프로토콜을 Casper 도구를 이용해 모델링하였는데 그림 2는 Chen-Lee 프로토콜을 Casper 표현방식으로 모델링한 것으로 8가지 항목 중 자유변수영역과 프로토콜 기술영역, 침입자 영역에 대한 표현이다(지면관계상 3가지 항목만 표현).

먼저 자유변수 영역에서, U는 사용자, S는 서버로서 각각 Agent로 나타내고, r, s, n은 난수값, key는 비밀키값의 정보를 표현하고, pw는 Agent x Agent -> Password, 즉, 두 Agent간의 비밀번호를 뜻하는데 예

```
#Free variables

U, S : Agent
r, s, n: Nonce
key : Secretkey
pw : Agent x Agent -> Password
InverseKeys = (key, key), (pw, pw)
H : HashFunction

#Protocol description

0.      -> U   : S
1.  U   -> S   : U, H(U (+) key) (+) r,
                 H(H( H(U, n, pw(U, S)) (+)
                 H(U, key)), r)
2.  S   -> U   : s (+) H(U (+) key), H(r, s)
3.  U   -> S   : U, H(s, r)

#Intruder Information

Intruder = Mallory
IntruderKnowledge = {User, Server, M, N,
pw(Mallory, User), pw(Mallory, Server),
H(User, Key)}
```

그림 2 Casper를 이용한 Chen-Lee 프로토콜 명세

를 들어 전자의 Agent가 비밀번호를 입력했을 때 후자의 Agent가 이 비밀번호를 받는다는 관계를 의미한다. 후자의 Agent 에게 전달할 목적으로 생성된 Password 값이라고 볼 수 있다. InverseKeys는 키 값에 대한 암호화 및 복호화를 표현하며, H는 해쉬함수를 뜻한다.

다음으로 프로토콜 기술 영역은 Chen-Lee 프로토콜을 명세한 부분으로 여기서 (+) 표현은 메시지 1, 2에서 XOR 연산을 표현하고 있다. 마지막으로 침입자 영역에 대한 정보가 제시되어 있다.

4.2 스마트카드 인증 프로토콜 검증 결과

본 장에서는 본 논문에서 제안한 Chen-Lee인증 프로토콜을 2.2절에 제시된 보안 요구사항에 대해 암호학적 안전성을 분석한다.

최근의 스마트카드를 이용한 많은 제안들이 tamper-resistance 특성을 가정으로 두고 있다. 마찬가지로 Chen-Lee 프로토콜 또한 스마트카드의 tamper-resistance 특성을 기본 가정으로 두고 있고 이러한 제안 프로토콜을 이용한 TRD(Tamper-Resistance Device)들에 활용하고자 한다고 주장하였다. 그러나 그러한 가정에 대해 최근 스마트카드에 저장된 비밀값들을 추출하기 위한 많은 방법들[15-18]이 개발되었고 이러한 가정들은 제한적이라 할 수 있다.

Chen-Lee 프로토콜에서는 공격자가 H(IDi(+)K)의 값을 재생 공격 및 오프라인 추측 공격, 가장 공격에 이용함에 따라 스마트카드 정보의 노출 및 추적이 가능하게 하였을 뿐만 아니라 서버로 접속시 비인가자의 인증이 가능한 결과를 초래하였다. 이를 Casper script를 이용하여 명세하기 위해 Chen-Lee 프로토콜의 두 개체간 사용된 정보에 대한 비밀성과 개체간 상호ID에 대한 인증을 만족해야 하며 이는 다음과 같이 표현할 수 있다.

```
Secret(U, pw(U,S), [S])
Secret(S, pw(U,S), [U])

Agreement(U, S, [key, r, s, n])
```

첫번째 표현은 "U는 pw(U,S) 정보를 오직 S와만 알고 있다"라고 풀이할 수 있고 두번째 표현은 "S는 pw(U,S) 정보를 오직 U와만 알고 있다"로 풀이할 수 있다. 세번째 표현은 "U는 key, r, s, n 정보를 통해 S로부터 자신의 개체를 인증받는다"라고 풀이할 수 있다

모델 체커를 이용해 비밀성과 개체인증 속성의 만족여부를 확인한 결과 첫번째 표현에서 U가 전달하는 pw(U,S)에 대해 S와의 비밀성 속성을 만족하지 않았고 이에 따라 결국 두 개체간의 데이터가 누설되었다. 또한 S입장에서의 pw(U,S) 정보도 안전하게 유지되지 못했으므로 비밀성 속성을 만족하지 않았으며 마지막 속성인 개체 인증에서도 key, r, s, n의 정보를 이용해 두 개체간의 인증에 실패했다.

2.2에서 제시된 보안 요구사항에 대해 FDR을 통한위 검증 결과를 토대로 다음과 같이 정리할 수 있다.

- Replay attack(재생공격) : [15-18]에 의한 사실로 공격자는 전력소모를 모니터링 함으로써 스마트카드에 저장된 정보를 추출해 낼 수 있다. 따라서 공격자는 스마트카드에 저장된 H(IDi(+)K)과 N, H() 값을 획득할 수 있다.
  이에 따라 공격자가 사용자의 과거 로그인 메시지 중 하나를 가로채기하여 소유하고 있다고 가정하자. 즉 메시지 1의 IDi, r (+) H(IDi(+)K), Auth에서 H(IDi(+)K)를 XOR 연산하여 r 값을 도출할 수 있게 된다. 이를 통해 메시지 2의 s (+) H(IDi(+)K) 또한 s 값을 생성할 수 있으며 이 두 값 r, s를 이용하여 서버에 대한 재생공격이 가능하게 된다.
- Offline Guessing attack(오프라인 추측 공격) : 공격자는 H(IDi(+)K)과 N, H() 정보를 가지고 있으므로 메시지 1의 값을 통해 오프라인 추측공격이 가능하다. 즉, 메시지 1의 Auth 값은 다음과 같은 값으로 구성되어 있다. H(H(HPW(+)H(IDi(+)K)),r) = H(H(*H(IDi, PW, N)* (+)H(IDi(+)K)),r). 따라서 공격자는 Auth'= H(H(H(IDi, *PW'*, N) (+)H(IDi(+)K)),r)을 연산하고 이를 통해 Auth? = Auth'을 비교하여 패스워드 값

PW를 추측할 수 있다.

- Impersonation attack(가장 공격) : 공격자가 정당한 로그인 정보를 위조하기 위해서 암호화된 메시지 값 안에 포함된 공격자 생성값 IDx을 메시지 1과 2에서 이미 H(IDi(+)K)을 통해 획득한 s, r 값을 이용해 메시지 3에서 IDx, H(s,r)을 전송하여 서버로부터 정상적인 사용자가 IDx인 것으로 인식하게 한다.

5. 개선된 제안프로토콜

이러한 Chen-Lee 프로토콜의 문제점으로 분석되었던 부분은 스마트카드 내에 저장된 정보가 DPA(차별화 전력 분석: Differential Power Analysis)를 통해 노출되고, 이 정보를 통해 상호 인증을 위한 난수값이 노출됨으로써 발생되었으며 이는 사용자의 OTP(일회성 패드 : One Time Pad)를 이용한 난수값을 추가적으로, 인증시 입력함으로써 인증시에 사용되는 난수값과 함께 XOR 연산을 함으로써 안전성을 보장받게 되었다. 즉 제안프로토콜은 다음 그림 3과 같은 절차로 인증이 이루어지며 앞서 언급된 취약성은 인증과정에서 도입된 One-Time-Pad 기술에 의해 극복할 수 있다. OTP 기법에서 많이 사용하는 Challenge-Response 방식은 사용자의 토큰 카드에 고유 랜덤값과 시스템에서 가지고 있는 사용자의 랜덤값을 일치시켜 이 값을 키값으로 랜덤하게 숫자를 만들어 시스템에서 Challenge하고 사용자가Response하여 인증하는 방식이다. 여기에서 사용되는 암호 기법이 DES(Data Encryption Standard)이며, 이를 DES Challenge-Response이라 한다. 기존의 Chen-Lee 프로토콜에서 Challenge-Response 형태로 서버와 사용자가 자신의 소유정보를 주고 받으며 인증하는 방식을 이용하여 세션마다 OTP에 사용되는 하나의 추가적인 랜덤값만 입력하여 비용을 최소화한다. 즉 시스템 개발시의 밴더입장에서의 개발비용의 추가는 필수불가결하지만, 사용자는 스마트카드를 발급 받음과 동시에 OTP용 난수 집합 T={T1, T2, T3, … Tn}을 이용한 값들을 함께 가지게 된다.

그림 3의 절차는 다음과 같이 설명될 수 있다.

[등록 단계]

Step 1. 사용자 U는 자신의 패스워드 PW와 임의의 난수값 N을 선택하여 $HPW = H(IDi, PW, N)$를 계산하고, 자신의 아이디 IDi와 함께 메시지 {IDi, HPW}를 서버 S에게 전송한다.

Step 2. S는 자신의 비밀키 K를 이용하여 $v = H(HPW(+)H(IDi(+)K))$를 계산하고, 이를 검증테이블에 IDi와 함께 저장한 후 스마트카드에 $H(IDi(+)K)$과 $H()$ 두 값을 저장하고 사용자에게 스마트카드를 발급한다. 이때 OTP용 난수값의 집합인 T를 사용자에게 별도

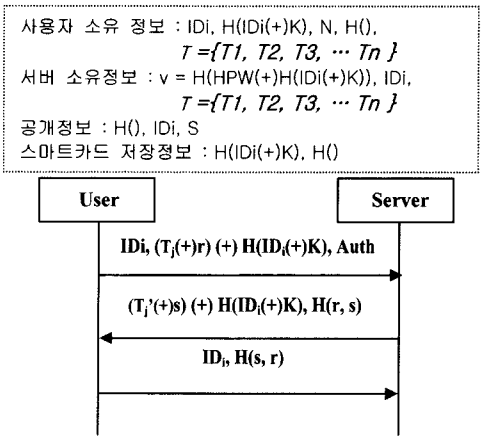

그림 3 개선된 Chen-Lee 프로토콜

발급한다.

Step 3. 스마트카드를 발급 받은 사용자 U는 스마트카드에 임의의 난수값 N을 입력하고 등록을 마친다.

[로그인 및 인증 단계]

Step 1. U가 자신의 아이디 IDi와 패스워드 PW를 입력하면 스마트카드는 난수값 r을 선택하고 OTP 난수값 집합 T에서 Tj 선택하여 (Tj(+) r) (+) H(IDi (+)K)과 Auth = H(H(HPW(+)H(IDi(+)K)),r)을 연산 및 생성한 후 IDi값과 함께 S에게 메시지 {IDi, (Tj(+) r) (+) H(IDi (+)K), Auth}를 보낸다.

Step 2. S는 받은 메시지에서 아이디 IDi와 자신의 K를 이용하여 H(IDi(+)K)를 계산하고 (Tj(+) r) (+) H(IDi(+)K)를 XOR연산하여 (Tj(+) r) 값을 도출한다. S는 도출된 (Tj(+) r) 값과 서버의 T에서 Tj값을 검색 후 r값을 도출한다. 또한 S는 도출된 r값과 자신의 검증자 v = H(HPW(+) H(IDi(+)K))를 이용하여 받은 Auth' = H(v, r)값을 생성한다. 생성된 Auth'을 U로부터 받은 Auth 값과 비교하여 일치할 경우, S는 난수값 s를 선택하고 OTP 난수값 집합 T에서 Tj'선택하여 (Tj'(+) s) (+) H(IDi(+)K)를 생성하고 그렇지 않으면, 로그인 요청을 거절한다.

Step 3. 메시지를 받은 스마트카드는 (Tj'(+) s) (+) H(IDi(+)K) 메시지를 H(IDi(+)K)와 XOR 연산하여 (Tj'(+) s) 값을 도출한다. U는 도출된 (Tj'(+) s) 값과 사용자의 T에서 Tj'값을 검색 후 s값을 도출한다. 이 값을 자신의 r값과 H(r,s) 연산하여 받은 H(r,s) 값과 비교하여 타당성을 검증한 후 서버를 인증한다. 마지막으로 검증된 s값을 이용하여 IDi와 H(s,r)을 서버에게 보내어 스마트카드를 인증 받고자 한다. 서버는 받은 H(s,r)을 연산하여 자신이 받은 값과 비교 후 일치하면 인증한다.

```
#Free variables

U, S : Agent
r, s, n, t: Nonce
key : Secretkey
pw : Agent x Agent -> Password
InverseKeys = (key, key), (pw, pw)
H : HashFunction

#Protocol description

0.      -> U  : S
1.   U -> S  : U, H(U (+) key) (+) (r(+) t),
                H(H( H(U, n, pw(U, S)) (+)
                H(U, key)), r)
2.   S  -> U  : (s(+) t) (+) H(U (+) key), H(r, s)
3.   U  -> S  : U, H(s, r)

#Intruder Information

Intruder = Mallory
IntruderKnowledge = {User, Server, M, N,
pw(Mallory, User), pw(Mallory, Server), H(User,
Key)}
```

그림 4 개선된 Chen-Lee 프로토콜 명세

위의 프로토콜을 Casper로 명세하면 다음과 같다(지면관계상 3가지 항목만 표현).

자유변수 영역의 난수값 t가 추가되고, 프로토콜 기술 영역은 메시지 1과 2에서 r과 s 값에 각각 t값을 XOR 연산하였고 나머지 영역은 모두 동일하게 명세 되었다.

명세된 위 프로토콜은 FDR을 통해 검증한 결과, 2.2의 3가지 속성을 다음과 같이 만족하였다.

- Replay attack(재생공격) : [15-18]에 의한 사실로 공격자가 전력소모를 모니터링하여 스마트카드에 저장된 정보 H(IDi(+)K)를 추출해 낼 수 있지만 스마트카드와 함께 발급된 OTP정보를 알 수 없기 때문에 메시지 1의 IDi, (Tj (+) r) (+) H(IDi(+)K), Auth에서 H(IDi(+)K)를 XOR 연산하여 r 값을 도출할 수 없으며 이에 따라 서버에 대한 재생공격이 불가능하게 된다.
- Offline Guessing attack(오프라인 추측 공격) : 공격자는 H(IDi(+)K)과 N, H() 정보를 가지고 있지만, 메시지 1의 Auth 값은 위의 재생공격에서 본 바와 같이 r 값을 도출할 수 없으므로 Auth 값을 비교하기 위한 공격자의 H(*H(H(IDi, PW, N)* (+)H(IDi(+)K)),r) 값을 생성할 수 없다. 따라서 공격자는 패스워드 값 PW를 추측할 수 없다.
- Impersonation attack(가장 공격) : 공격자가 정당한 로그인 정보를 위조하기 위해서 암호화된 메시지 값 안에 포함된 공격자 생성값 IDx을 메시지 1과 2에서 H(IDi(+)K)을 통해 s, r 값을 획득해야 가장공격에 이용 가능하지만 OTP 값을 알 수 없으므로 s, r 값을 도출할 수 없고, 따라서 메시지 3에서 IDx, H(s,r)을 생성 및 전송할 수 없기 때문에 서버에의 가장공격이 불가능하다.

6. 결 론

본 논문에서는 사용자에게 안전한 통신 서비스를 제공하기 위해 스마트카드를 사용한 패스워드 기반의 인증 프로토콜을 제안하였다. 기존의 Chen-Lee 프로토콜은 계산비용이 큰 지수연산 및 공개키 연산을 사용하지 않고 XOR 및 해쉬 연산을 주 연산으로 사용하고, 메시지 전송회수가 적기 때문에 이전의 프로토콜들에 비해 계산비용이 훨씬 적고 통신비용도 적으므로 매우 효율적으로 인증을 할 수 있는 장점을 가지고 있다. 하지만 스마트카드의 저장된 정보의 노출로 인해 취약성을 가지고 있고 이를 개선한 프로토콜을 통해 패스워드 추측공격과 재생공격, 그리고 가장공격에 안전성을 가질 수 있었다.

참 고 문 헌

[1] Chien, H.Y. and Chen, C.H., "A Remote Authentication Scheme Preserving User Anonymity," IEEE AINA'05, Vol.2, pp. 245-248, 2005.

[2] Das, M.L., Saxena, A., and Gulati, V.P., "A dynamic ID-based remote user authentication Scheme," IEEE Transactions on Consumer Electronics, Vol. 50, No.2, pp. 629-631, 2004.

[3] MacKenzie, P., Shrimpton, T., and Jakobsson, M., "Threshold Password Authenticated Key Exchange (extended abstract)," Advances in Cryptology Proc. of CRYPTO 2002, pp. 385-400, 2002.

[4] MacKenzie, P., "More Efficient Password Authenticated Key Exchange," RSA Conference, Cryptographer's Track, pp. 361-377, 2001.

[5] Boyko, V., MacKenzie, P. and Patel, S., "Provably Secure Password Authentication and key Exchange Using Diffie-Hellman(extended abstract)," EuroCrypt 2000, pp. 156-171, 2000.

[6] Munilla, J. and Peinado, A., "Off-line password guessing attack to Peyravian-Jeffries's remote user authentication protocol," A Computer Communications 30, pp. 52-54, 2006.

[7] Bellovin, S. M. and Merritt. M., "Encrypted Key Exchange: Password-based Protocols Secure against Dictionary Attacks," In Proc. of IEEE Security and Privacy, pp. 72-84, 1992.

[8] Bellovin, S.M. and Merritt, M., "Augmented encrypted key exchange : a password-based protocol secure against dictionary attacks and password file compromise," Technical report, AT&T Bell Laboratories, 1994.

[9] Kwon, T. and Song, J., "Secure agreement scheme for gxy via password authen-tication," Electronics Letters Vol.35, No.11, pp. 892-893, 1999.
[10] Chen, T.H. and Lee, W.B., "A new method for using hash functions to solve remote user authentication," Computers and Electrical Engineering 34, pp. 53-62, 2008.
[11] Lowe, G., "Casper: A compiler for the analysis of Security Protocols," In Proc. of the 1997 IEEE Computer Security Foundations Workshop X, IEEE Computer Society, Silver Spring, MD, pp. 18-30, 1997.
[12] Hoare, C.A.R., Communicating Sequential Processes, Prentice-Hall, 1985.
[13] Formal Systems Ltd. FDR2 User Manual, Aug. 1999.
[14] Lin, C.L., Wen, H.A., Hwang, T. and Sun, H.M. "Provably secure three-party password-authenticated key exchange," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E87-A (11), pp. 2990-3000, 2004.
[15] Ku, W.C. and Chen, S.M., "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics 50 (1), pp. 204-207, 2004.
[16] Hwang, T. and Ku, W.C., "Reparable key distribution protocols for Internet environ- ments," IEEE Trans.Commun., Vol.43, No.5, pp. 1947-1949, May, 1995.
[17] Kocher, P., Jaffe, J. and Jun, B., "Differential power analysis," In Proc.of Advances in Cryptology (CRYPTO'99), pp. 388-397, 1999.
[18] Messerges, T.S., Dabbish, E.A. and Sloan, R.H., "Examining smart card security under the threat of power analysis attacks," IEEE Transactions on Computers 51(5), pp. 541-552, 2002.

김 현 석

육군사관학교 경제·경영학과 학사. 고려대학교 컴퓨터학과 석사. 고려대학교 컴퓨터학과 박사. 2007년~현재 육군사관학교 전자·정보학과 전임강사. 관심분야는 정형기법, 네트워크 보안, 전자상거래 보안, RFID 보안프로토콜 설계, 스마트카드 보안 설계

김 주 배

공군사관학교 외국어학과 학사. 현재 고려대학교 컴퓨터학과 석사과정. 관심분야는 정형기법, RFID 프로토콜, 스마트카드 보안, 보안 프로토콜 검증

정 연 오

고려대학교 전산학과 학사. 현재 고려대학교 컴퓨터·전파통신공학과 석사과정. 관심분야는 정형기법, 정보보호, 보안프로토콜

한 근 희

서울산업대학교 컴퓨터학과 학사. 한양대학교공과대학원 컴퓨터학과 석사. 고려대학교 컴퓨터학과 박사. 2006년~현재 행정안전부 정보보호정책과 근무. 2004년~현재 건국대학교 정보통신대학원 겸임교수. 관심분야는 통합보안관리와 인터넷 보안, 모바일 보안, 차세대 인터넷

최 진 영

서울대학교 컴퓨터 공학과 학사. Dept. of Mathematics and Computer Science, Drexel Univ. 석사. Dept. of Computer and Information Science, University of Pennsylvania 박사. 1996년~현재 고려대학교 컴퓨터·전파통신공학부 교수. 관심분야는 정형기법, 임베디드 실시간 시스템, 프로그래밍 언어, 프로세스 대수, 소프트웨어 공학