http://dx.doi.org/10.3745/KTCCS.2013.2.11.503

A Study on Secure Remote User Authentication Scheme using Smart Card

Sung Jong Go† · Im Yeong Lee††

ABSTRACT

Recently, the rapid development of network technology has enabled people to use various services on the internet. However, the existing password-based user authentication system used in the internet environment requires a password table, which is a potential security threat as it could be leaked by an insider. To solve this issue, remote user authentication methods that do not require a user password table have been proposed. Regarding remote user authentication using a smart card in particular, various methods have been suggested to reduce expenses and to improve stability and efficiency, but the possibility of impersonation attacks and password-guessing attacks using information saved in a user's smart card still exist. Therefore, this study proposes a remote user authentication method that can safeguard against impersonation attacks and password guessing attacks, by analyzing weak points of conventional methods and creating a smart card's ID and password that are based on the user's ID and password.

Keywords : Remote User Authentication, Smart Card, Password Guessing Attack, Impersonation Attack

스마트카드를 이용한 안전한 원격 사용자 인증기법에 관한 연구

고 성 종† · 이 임 영††

요 약

최근 네트워크 기술의 급속한 발전과 함께 사람들은 인터넷을 통해 다양한 서비스를 이용할 수 있게 되었다. 하지만 인터넷 환경에서 많이 사용되는 패스워드 기반의 사용자 인증 방식은 패스워드 테이블이 요구되기 때문에 내부자에 의한 패스워드 테이블 노출 등과 같은 보안 위협들이 존재한다. 이러한 문제를 해결하기 위해 사용자의 패스워드 테이블이 요구되지 않는 인증 방법으로 원격 사용자 인증 방식이 제안되었다. 그 중 스마트카드를 이용한 원격 사용자 인증 방식은 계산 비용이나 효율성, 안전성을 개선하기 위한 다양한 방법들이 제안되었지만 위장 공격 위협과 스마트카드에 저장된 정보를 이용한 패스워드 추측 공격 위협이 존재한다. 본 논문은 기존 방식들의 취약점을 분석하고 기존 사용자 아이디/패스워드기반의 스마트카드 아이디와 패스워드를 생성하여 위장 공격과 패스워드 추측 공격에 대해 안전한 원격 사용자 인증 방식을 제안하였다.

키워드 : 원격 사용자 인증, 스마트카드, 위장 공격, 패스워드 추측 공격

1. 서 론

최근 네트워크 기술의 급속한 발전과 함께 사람들은 시간이나 장소에서 구애받지 않고 인터넷 서비스를 이용할 수 있게 되었다. 인터넷 서비스에 접근하는 과정에서 사용되는 사용자 인증 방식은 서비스를 이용하기 위한 사용자를 확인하는 매우 중요한 과정으로 패스워드 기반의 인증 방식이 많이 사용되고 있다. 패스워드 기반의 인증 방식은 사용자가 알고 있는 정보를 바탕으로 선택된 패스워드를 이용하여 간편하게 서비스를 이용 가능하지만 서버는 서비스를 이용하는 사용자의 인증 정보로 모든 사용자에 대한 패스워드들을 저장하기 위해 패스워드 테이블이 요구된다. 이러한 패스워드 테이블의 구성은 내부 유출에 대한 문제가 이슈화됨에 따라 내부자에 의한 패스워드 테이블의 노출로 인해 아이디 도용 문제가 발생할 수 있다. 이러한 문제를 해결하기 위해 Lamport에 의해 패스워드 테이블의 구성없이 사용자의 신원을 증명할 수 있는 원격 사용자 인증 방식이 제안되었다[1].

그 중, Hwang과 Li가 최초로 스마트카드를 이용한 원격 사용자 인증 방식을 제안하였다. 스마트카드는 보안 모듈, 메모리 관리 모듈, 입출력 모듈 등이 탑재하고, 집적회로(IC:Integrated Circuit) 칩을 내장하고 있기 때문에 자체 연산 가능한 보안 매체로써 하나의 원격지 서버로 이용 가능하다. 하지만, 제안된 방식은 ElGamal 공개키 암호를 이용

※ 본 연구는 순천향대학교 학술연구비 지원으로 수행하였음.
† 준 회 원 : 순천향대학교 컴퓨터공학과 석사과정
†† 종신회원 : 순천향대학교 소프트웨어학과 교수
논문접수 : 2013년 10월 14일
심사완료 : 2013년 10월 30일
* Corresponding Author : Im Yeong Lee(imylee@sch.ac.kr)

하여 이산대수의 어려움에 기반한 안정성을 제공하지만 높은 연산 비용을 요구한다는 문제점을 가지고 있다[2].

이러한 연산 비용 문제를 해결하기 위해 Sun등은 보다 효율적인 해시기반의 원격 사용자 인증 방식을 제안하였다[3]. 이 후에도 연산비용 문제를 해결하기 위해 해시기반의 다양한 연구들이 진행되었다.

연산비용 문제 뿐 아니라 다양한 기능을 제공하기 위해서 많은 연구들이 진행되었다. 그 중, Chien등은 상호인증을 제공할 수 있는 방식을 제안하였으며[4], Ku등은 사용자의 패스워드를 자유롭게 변경할 수 있는 방식을 제안하였다[5].

또한, 다양한 보안 취약점을 보완한 많은 연구들도 이루어졌다. Yoon등은 인가되지 않은 사용자에 의해 쉽게 패스워드가 변경될 수 있다는 문제점을 해결하기 위한 방식을 제안하였고[6], Lee등은 위조 공격을 해결하기 위한 방식을 제안하였다[7]. 이 외에도 Wang등은 서비스 거부 공격을 해결하기 위한 방식을 제안하였다[8].

하지만 이러한 기존 연구들은 공격자가 사용자와 서버의 통신 과정에서 도청한 정보를 이용하여 정당한 사용자로 위장하거나 분실 또는 도난당한 스마트카드로부터의 저장된 정보들을 추출하여 사용자의 패스워드가 추측될 수 있다.

따라서 본 논문은 기존 방식들을 분석하고 사용자 위장 공격과 스마트카드에 저장된 정보 발생할 수 있는 패스워드 추측 공격으로부터 안전한 사용자 인증 방식을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 스마트카드를 이용한 원격 사용자 인증 방식을 분석하고, 3장에서는 기존 방식의 취약점 분석을 기반으로 보안요구사항을 도출한다. 4장에서는 위장 공격으로부터 안전한 방식과 오프라인 패스워드 추측 공격으로부터 안전한 방식을 제안하고, 5장에서는 기존 요구 사항을 기반으로 제안방식을 분석한다. 마지막으로 6장에서 결론을 맺는다.

2. 관련 연구

본 장에서는 기존 스마트카드를 이용한 원격 사용자 인증 방식의 구조를 알아보고 발생할 수 있는 공격 위협에 대한 취약점을 분석한다.

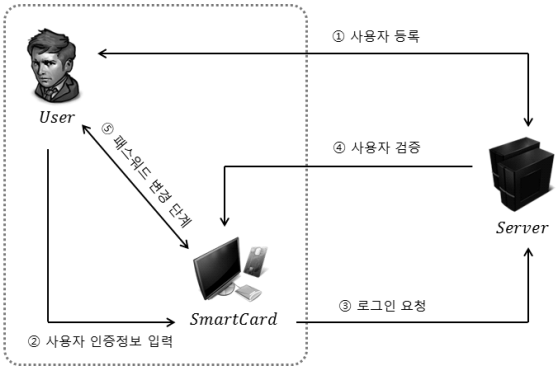

Fig. 1. Remote User Authentication Scheme

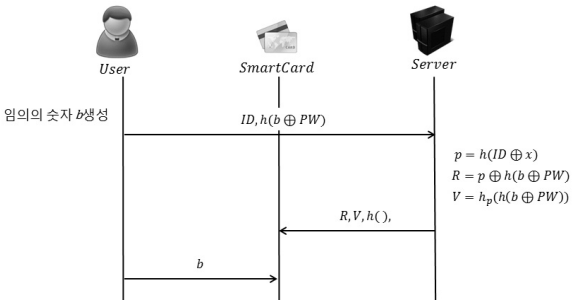

Fig. 2. Registration Phase

2.1 시스템 계수

기존 방식들은 다음과 같은 시스템 계수를 사용한다.

$*$: 각각의 객체
(U : 사용자, S : 서버, C : 스마트카드)
ID : 사용자의 식별자
PW : 사용자의 비밀 번호
V : 스마트카드 소유자를 검증하기 위한 값
$h()$: 해시 함수
$h_*()$: 비밀 키 $*$를 포함한 해시 함수
T_* : 객체 $*$의 타임스탬프

2.2 기존 방식

Chen 등이 제안한 방식은 기존 방식의 위장 공격으로부터의 위협을 해결하기 위하여 제안된 방식이다[9]. 해당 방식은 등록 단계, 로그인 단계, 검증 단계, 패스워드 변경 단계로 구성되어 있으며 각 단계는 다음과 같다(Fig. 1).

1) 등록 단계

이 단계는 사용자가 서버에 자신을 등록하고 스마트카드를 발급받는 과정으로 안전하게 수행된다고 가정한다(Fig. 2).

Step 1. 사용자는 임의의 숫자 b를 선택하고 사용자의 등록 정보를 서버에 전송한다.

Step 2. 서버는 p, R, V를 계산하고 R, V, h()를 스마트카드에 입력한다.

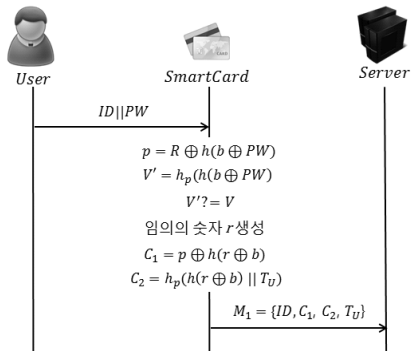

Fig. 3. Login Phase

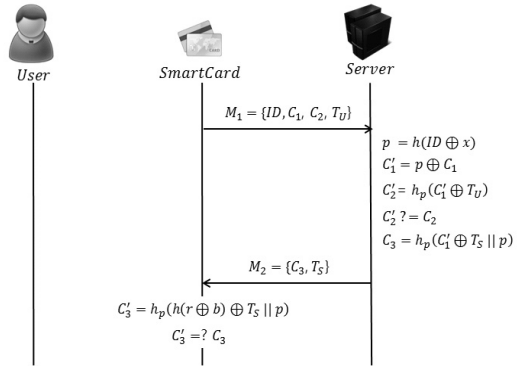

Fig. 4. Verification Phase

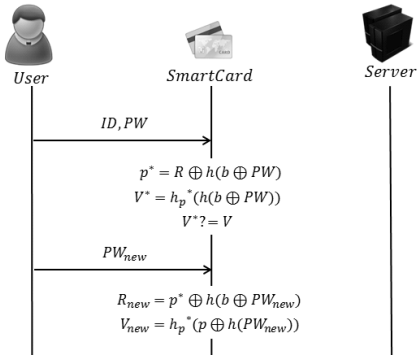

Fig. 5. Password Change Phase

Step 3. 서버은 V와 R, h()를 포함한 스마트카드를 사용자에게 발급한다.

Step 4. 사용자는 임의로 생성한 숫자 b를 스마트카드에 입력한다. 등록 과정을 통해 사용자가 소유한 스마트카드는 V, R, b와 h() 포함하고 있으며 사용자는 다음 과정에서 더 이상 b를 기억할 필요가 없다.

2) 로그인 단계

이 단계는 사용자가 서버에 로그인할 때의 과정으로 다음과 같은 작업을 수행한다(Fig. 3).

Step 1. 사용자는 스마트카드 리더에 스마트카드를 삽입하고 ID와 PW를 입력한다.

Step 2. 스마트카드는 스마트카드의 소유자를 확인하기 위해 p, V′을 계산하고 V와 V′을 비교한다. V와 V′가 다르면 스마트카드는 세션을 종료한다.

Step 3. 스마트카드는 임의의 숫자 r을 생성하고 인증 정보로 C1, C2를 계산한다.

Step 4. 스마트카드는 서버에 로그인 요청 메시지 M1을 전송한다.

3) 검증 단계

이 단계는 로그인 요청 메시지 M1을 받은 후에 수행하는 과정으로 서버와 스마트카드는 다음과 같은 작업을 수행한다(Fig. 4).

Step 1. 서버는 ID 또는 타임스탬프가 유효한지 확인한다. △T는 전송 지연에 대한 유효 시간 간격으로 (TU-TS)>△T를 검사하여 타임스탬프의 유효성을 확인한다.

Step 2. 서버는 로그인 요청 메시지를 확인하기 위해 p, C_1', C_2'을 계산하고 C_2'과 C_2를 비교한다. C_2'와 C_2가 다르면 로그인 요청을 거절한다.

Step 3. 서버는 상호 인증을 위한 검증 정보로 C_3를 계산하고 검증 메시지 M_2를 사용자의 스마트카드에 전송한다.

Step 4. 사용자의 스마트카드는 T_S가 유효한지 확인하고 검증 메시지를 확인하기 위해 C_3'을 계산하고 C_3'과 C_3를 비교한다. C_3'과 C_3 다르면 사용자 인증에 실패한다.

4) 패스워드 변경 단계

이 단계는 사용자가 기존의 패스워드 PW를 새로운 패스워드 PW_{new}로 변경하는 과정으로 다음과 같은 작업을 수행한다(Fig. 5).

Step 1. 사용자는 스마트카드 리더에 스마트카드를 삽입하고 ID와 PW를 입력하고 패스워드 변경을 요청한다.

Step 2. 스마트카드는 스마트카드의 소유자를 확인하기 위해 p^*, V^*을 계산하고 V^*와 V를 비교한다.

Step 3. V^*과 V가 같다면 사용자는 새로운 패스워드 PW_{new}를 선택하고 다르면 스마트카드는 패스워드 변경 요청을 거절한다.

Step 4. 사용자의 스마트카드는 새로운 R_{new}와 V_{new}를 계산하여 R과 V를 대체함으로써 새로운 패스워드로 변경을 완료한다.

2.3 취약점 분석

1) 위장 공격 위협

스마트카드를 이용한 원격 사용자 인증 방식은 서버로부터 스마트카드를 발급받은 정당한 사용자만이 스마트카드를 이용하여 서버에 사용자의 신분을 증명하는 방법이다. 하지만 Wang et al. Scheme은 공격자가 로그인 요청 메시지와 검증 메시지를 도청하여 습득한 정보를 이용하여 새로운 로그인 요청 메시지를 생성함으로써 정당한 사용자로 위장할 수 있다[9].

2) 스마트카드에서의 패스워드 추측 공격 위협

스마트카드는 사용자가 인증에 필요한 정보를 포함한 물리적 보안 매체이다. 하지만 스마트카드를 분실 및 도난당했을 경우, 공격자는 스마트카드에 저장된 정보들이 추출할 수 있다. 추출된 정보들은 별도의 암호 기술 없이 해시 기반의 정보로써 공격자는 적은 노력만으로도 사용자의 패스워드의 추측이 가능하다[10].

3. 보안요구사항

본 장에서는 스마트카드를 이용한 원격 사용자 인증에서의 보안 위협에 따른 보안요구사항을 도출한다.

3.1 보안요구사항

- 기밀성 : 사용자 인증은 서비스에 접근하는 사용자의 신분을 증명하는 방법으로써 정당한 사용자만이 자신이 소유한 스마트카드를 이용하여 인증 정보를 생성하고 검증할 수 있어야하며 통신에서 사용되는 데이터들은 사용자의 신분을 증명하기 위한 민감한 정보를 포함하고 있어 데이터가 노출되더라도 그 데이터의 값을 유추하거나 생성할 수 없어야 한다.
- 무결성 : 스마트카드에서 생성된 로그인 메시지와 서버에서 생성된 검증 메시지는 사용자의 신원을 증명하는 근거가 되므로 통신 중간에 위·변조되지 않아야 한다.
- 상호인증 : 상호간에 정단한 객체임을 증명하기 위하여 스마트카드와 서버는 신뢰할 수 있는 정보를 바탕으로 서로간의 인증이 제공되어야 한다.

4. 제안방식

본 장에서는 스마트카드를 이용한 해시기반의 원격 사용자 인증 방식으로 스마트카드의 아이디와 패스워드를 생성하여 사용자 인증을 수행하며 제안방식 1에서 위장 공격 위협을 해결할 수 있는 방식과 제안방식 2에서 패스워드 추측 공격 위협을 해결할 수 있는 방식을 제안한다. 제안 방식의 구성은 기존 방식과 동일하게 등록 단계, 로그인 단계, 검증 단계, 패스워드 변경 단계로 구성되어 있다.

4.1 시스템 계수

$*$: 각각의 객체
(U : 사용자, S : 서버, C : 스마트카드)
ID : 사용자의 식별자
PW : 사용자의 비밀 번호
CID : 사용자의 ID기반의 스마트카드 식별자
CPW : 사용자의 PW기반의 스마트카드 비밀번호
V : 사용자를 검증하기 위한 정보
N : 등록 횟수
$h()$: 해시 함수
$*_x$: 객체 $*$의 비밀 키
T_* : 객체 $*$의 타임스탬프

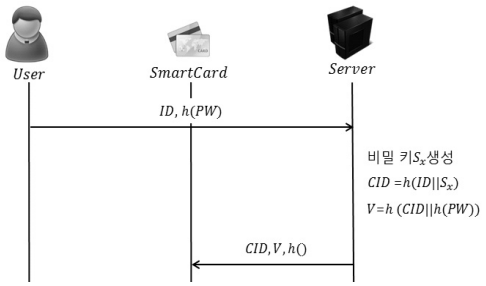

Fig. 6. Registration Phase

4.2 제안방식 1

본 제안방식 1은 불필요한 XOR연산을 제거하여 연산량을 줄이고 사용자의 스마트카드와 서버 사이에 발생할 수 있는 위장 공격으로부터 안전한 방식이다.

1) 등록 단계

이 단계는 사용자가 서버에 자신을 등록하고 스마트카드를 발급받는 과정으로 안전하게 수행된다고 가정한다(Fig. 6).

Step 1. 사용자는 서버에 사용자의 정보를 전송한다.

Step 2. 서버는 비밀 키 SX를 생성하고 CID와 V를 계산하여 스마트카드에 입력한다.

Step 3. 서버는 CID와 V를 포함한 스마트카드를 사용자에게 발급한다. 등록 과정을 통해 사용자가 발급받은 스마트카드는 CID와 V, h() 포함하고, 서버는 더 이상 사용자로부터 입력받은 h(PW)정보를 저장할 필요가 없다.

2) 로그인 단계

이 단계는 사용자가 서버에 로그인할 때의 과정으로 다음과 같은 과정을 수행한다(Fig. 7).

Step 1. 사용자는 스마트카드 리더에 스마트카드를 삽입하고 ID와 PW를 입력한다.

Step 2. 스마트카드는 스마트카드의 소유자를 확인하기 위해 V′을 계산하고 V와 V′을 비교한다. V와 V′가 다르면 스마트카드는 세션을 종료한다.

Step 3. 스마트카드는 임의의 숫자 r을 생성하고 로그인 요청 정보로 C_1, C_2를 계산한다.

Step 4. 스마트카드는 서버에 로그인 요청 메시지 M1을 전송한다.

3) 검증 단계

이 단계는 서버가 로그인 요청 메시지 M1을 받은 후 수행되는 과정으로 서버와 스마트카드는 다음과 같은 작업을 수행한다(Fig. 8).

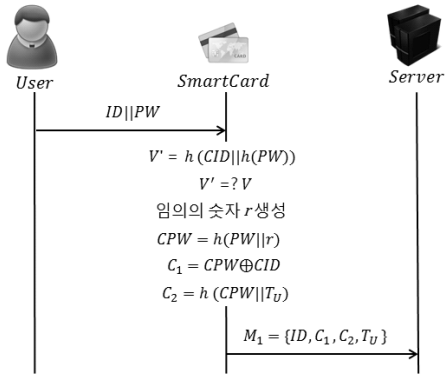

Fig. 7. Login Phase

Step 1. 서버는 ID 또는 타임스탬프가 유효한지 확인한다. △T는 전송 지연에 대한 유효 시간 간격으로 (TU-TS)>△T를 검사하여 타임스탬프의 유효성을 확인한다.

Step 2. 서버는 로그인 요청 메시지를 확인하기 위해 CID, CPW′, C_2'을 계산하고 C_2'과 C_2를 비교한다.

Step 3. 서버는 상호 인증을 위한 검증 정보로 C_3를 계산하고 검증 메시지 M_2를 사용자의 스마트카드에 전송한다.

Step 4. 사용자의 스마트카드는 T_S가 유효한지 확인하고 검증 정보를 확인하기 위해 C_3'을 계산하고 C_3'과 C_3를 비교한다.

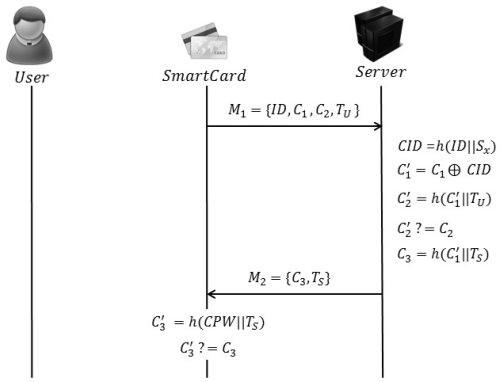

Fig. 8. Verification Phase

4) 패스워드 변경 단계

이 단계는 사용자가 기존의 패스워드 PW를 새로운 패스워드 PW_{new}로 변경하는 과정으로 다음과 같은 작업을 수행한다(Fig. 9).

Step 1. 사용자는 스마트카드 리더에 스마트카드를 삽입하고 ID와 PW를 입력하고 패스워드 변경을 요청한다.

Step 2. 스마트카드는 스마트카드의 소유자를 확인하기 위해 V′을 계산하고 V′와 V를 비교한다.

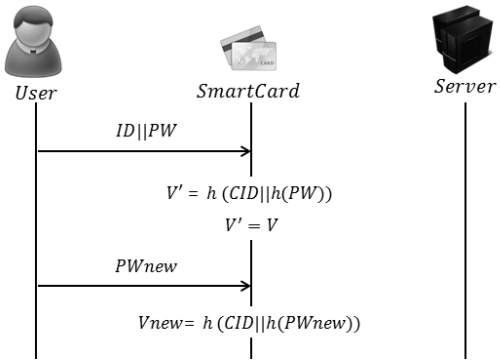

Fig. 9. Password Change Phase

Step 3. V′과 V가 같다면 사용자는 새로운 패스워드 PW_{new}를 선택하고 다르면 스마트카드는 패스워드 변경 요청을 거절한다.

Step 4. 사용자의 스마트카드는 V_{new}를 계산하여 V를 대체함으로써 새로운 패스워드로 변경된다.

4.3 제안방식 2

본 제안방식 2는 스마트카드의 소유자를 서버의 정보를 포함한 검증 정보를 이용하여 확인함으로써 공격자가 스마트카드에서 추출한 정보로부터 패스워드를 추측하거나 스마트카드의 소유자를 서버 없이 검증할 수 없도록 한다.

1) 등록 단계

이 단계는 사용자가 서버에 자신을 등록하고 스마트카드를 발급받는 과정으로 안전하게 수행된다고 가정한다(Fig. 10).

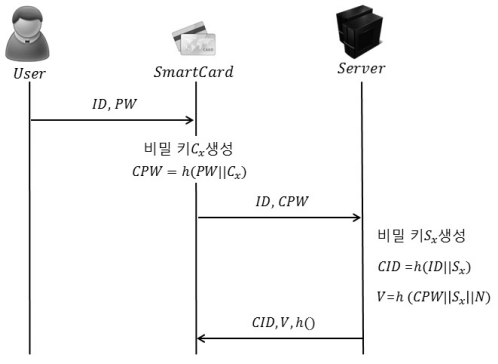

Fig. 10. Registration Phase

Step 1. 사용자는 스마트카드 리더에 스마트카드를 삽입하고 ID와 PW를 입력한다.

Step 2. 스마트카드는 비밀 키 C_X를 생성하고 사용자의 PW를 이용하여 CPW를 생성한 후, 사용자 등록을 요청한다.

Step 3. 서버는 비밀 키 S_X를 생성하고 CID와 V를 계산하여 스마트카드에 전송한다. 사용자의 등록 횟수를 나타내

는 속성으로 N=0으로 생성하고 재등록 과정일 경우 N = N + 1로 설정하여 V의 입력 값으로 사용한다.

Step 4. 사용자는 등록 과정을 통해 서버로부터 전송받은 CID와 V, h()를 소유한 스마트카드에 저장한다. 또한, 재등록 과정을 통해 사용자의 PW와 관계없이 새로운 검증 정보 V_{new}를 재발급 받을 수 있다.

$$V_{new} = h(CPW \| S_x \| N+1)$$

2) 로그인 단계

이 단계는 사용자가 서버에 로그인할 때의 과정으로 다음과 같은 작업을 수행한다(Fig. 11).

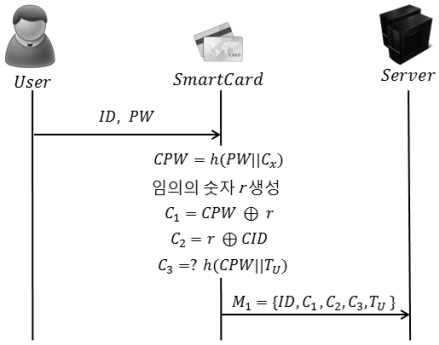

Fig. 11. Login Phase

Step 1. 사용자는 스마트카드 리더에 스마트카드를 삽입하고 ID와 PW를 입력한다.

Step 2. 스마트카드는 임의의 숫자 r을 생성하고 로그인 요청 정보로 C_1, C_2, C_3를 계산한다.

Step 3. 스마트카드는 서버에 로그인 요청 메시지 M_1을 전송한다.

3) 검증 단계

이 과정은 인증 요청 메시지 M1을 받은 후에 서버와 스마트카드는 다음과 같은 과정을 수행한다(Fig. 12).

Step 1. 서버는 ID 또는 타임스탬프가 유효한지 확인한다. △T는 전송 지연에 대한 유효 시간 간격으로 (TU-TS)>△T를 검사하여 타임스탬프의 유효성을 확인한다.

Step 2. 서버는 로그인 요청 메시지를 확인하기 위해 CID, C_2', C_3'을 계산하고 C_3'과 C_3를 비교한다. C_3'과 C_3가 다르면 로그인 요청을 거절한다.

Step 3. 서버는 상호 인증을 위한 검증 정보로 V, C_2', C_4를 계산하고 검증 메시지 M_2를 사용자의 스마트카드에 전송한다.

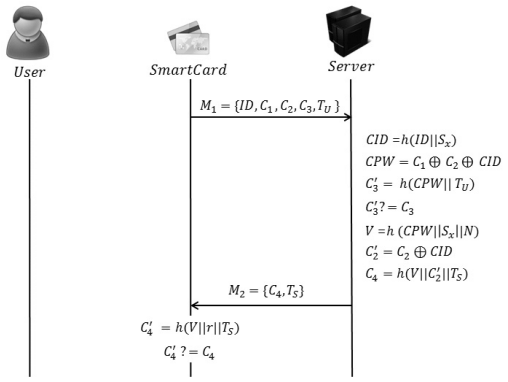

Fig. 12. Verification Phase

Step 4. 사용자의 스마트카드는 T_S가 유효한지 확인하고 검증 정보를 확인하기 위해 C_4'을 계산하고 C_4'과 C_4를 비교한다.

4) 패스워드 변경 단계

이 단계는 사용자가 기존의 패스워드 PW를 새로운 패스워드 PW_{new}로 변경하는 과정으로 다음과 같은 작업을 수행한다. 이 과정은 사용자 인증 후 진행된다(Fig. 13).

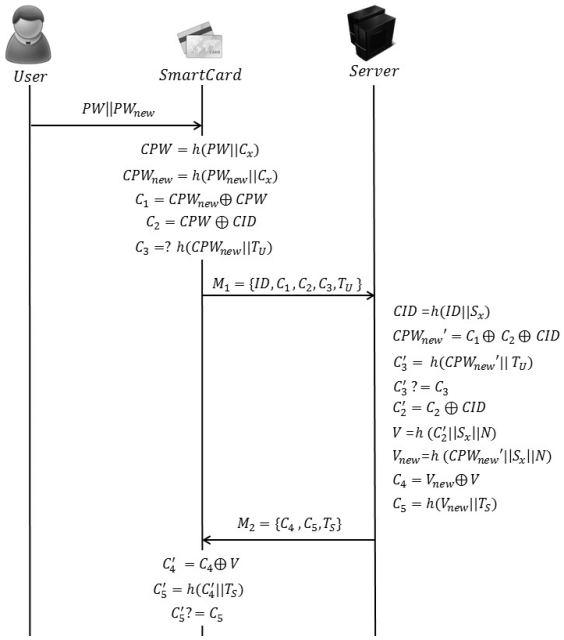

Fig. 13. Password Change Phase

Step 1. 기존 패스워드 PW와 새로운 패스워드 PW_{new}를 입력하고 패스워드 변경을 요청한다.

Step 2. 스마트카드는 임의의 숫자 r을 생성하고 패스워드 변경 요청 정보로 C_1, C_2, C_3를 계산한다.

Step 3. 스마트카드는 서버에 패스워드 변경 요청 메시지 M_1을 전송한다.

Step 4. 서버는 패스워드 변경 요청 메시지를 받은 후, ID 또는 타임스탬프가 유효한지 확인한다. △T는 전송 지연에 대한 유효 시간 간격으로 (TU-TS)>△T를 검사하여 타임스탬프의 유효성을 확인한다.

Step 5. 서버는 패스워드 변경 요청 메시지를 확인하기 위해 CID, C_2', C_3'을 계산하고 C_3'과 C_3를 비교한다. C_3'과 C_3가 다르면 패스워드 변경 요청을 거절한다.

Step 6. 서버는 패스워드 변경에 대한 확인 정보로 V, V_{new}, C_4, C_5를 계산하고 검증 메시지 M_2를 사용자의 스마트카드에 전송한다.

Step 7. 스마트카드는 검증 메시지를 확인하기 위해 C_4', C_5'을 계산하고 C_5'과 C_5를 비교한다.

Step 8. 스마트카드는 C_5'과 C_5 같다면 검증 정보 V를 C_4'로 대체하고 다르면 패스워드 변경에 거절한다.

5. 제안방식 분석

Wang Scheme은 사용자 인증을 위해 스마트카드를 이용하여 생성되는 로그인 정보와 서버에서 생성되는 검증 정보가 유사한 형태를 이루고 있기 때문에 공격자는 로그인 과정과 검증 과정에서 도청한 정보를 이용하여 유효한사용자의 패스워드는 추측할 수 없지만 정당한 사용자로 위장하여 로그인 요청 메시지를 생성할 수 있다.

또한 Wang Scheme과 Chen Scheme은 등록 과정을 통해 스마트카드에 사용자 인증에 필요한 정보를 저장하게 된다. 스마트카드는 저장된 정보를 이용하여 로그인 요청과 사용자 검증을 수행된다. 하지만 스마트카드에 저장된 정보들은 해시 기반의 데이터이기 때문에 스마트카드를 분실 및 도난당했을 경우 공격자는 스마트카드에 저장된 정보를 추출하여 적은 노력만으로도 사용자의 패스워드의 추측이 가능하다.

이러한 기존 방식들의 취약점으로부터 도출된 보안 요구사항에 대한 제안 방식의 분석은 다음과 같다.

- 기밀성 : 통신에서 사용되는 데이터들은 등록 과정을 통해 스마트카드를 발급받은 사용자만이 CID와 CPW를 이용하여 로그인 및 검증 과정을 수행할 수 있다. 또한 임의의 숫자 r을 이용하여 매번 다른 요청 메시지를 생성하기 때문에 공격자는 메시지를 유추하거나 추측할 수 없다.
- 무결성 : 사용자 인증하는 과정에서 생성되는 로그인 요청 메시지와 검증 메시지는 XOR 연산된 정보와 XOR 연산된 정보로부터 추출될 인증 정보의 해시 값으로 구성되기 때문에 XOR 연산으로부터 추출된 결과의 해시 결과를 비교함으로써 위·변조가 여부를 확인 가능하다.
- 상호인증 : 등록 과정에서 입력된 정보를 바탕으로 스마트카드에서 생성된 로그인 요청 메시지와 서버에서 생성된 검증 메시지를 확인함으로써 스마트카드와 서버의 사이에 상호 인증을 제공한다.

따라서 제안방식 1의 경우는 사용자의 아이디와 패스워드 기반으로 생성된 스마트카드의 아이디와 패스워드를 이용하여 다른 형태의 로그인 요청 메시지와 검증 메시지를 구성함으로써 위장 공격으로부터 안전하다. 또한 불필요한 XOR 연산을 제거하여 연산량이 감소되는 효과를 얻을 수 있다.

Table 1. Analysis of the Proposed Schemes

		Wang Scheme	Chen Scheme	제안 방식 1	제안 방식 2
위장 공격		X	O	O	O
		타임스탬프 변조를 통한 위장 공격에 취약	타임스탬프를 연접함으로써 위장 공격 불가능	타임스탬프를 연접함으로써 위장 공격 불가능	타임스탬프를 연접함으로써 위장 공격 불가능
병렬 세션 공격		X	O	O	O
		동일한 형태의 로그인 및 검증 과정이 구성되어 병렬 세션 공격에 취약	p를 이용하여 다른 형태의 로그인 및 검증 과정을 이용하여 위/변조 불가능	CID/CPW기반의 다른 형태의 로그인 및 검증 메시지 위/변조 불가능	CPW와 검증 정보를 이용하여 로그인 및 검증 메시지 위/변조 불가능
오프라인 패스워드 추측 공격		X	X	X	O
		스마트카드에 저장된 Hash 기반 정보를 통해 적은 노력으로 추측 가능	스마트카드에 저장된 Hash 기반 정보를 통해 적은 노력으로 추측 가능	스마트카드에 저장된 Hash 기반 정보를 통해 적은 노력으로 추측 가능	검증 정보가 서버의 정보를 요구하기 때문에 패스워드 추측이 어려움
연산량	등록	3 H + 2 X	3 H + 3 X	3 H	3 H
	로그인	5 H + 4 X	5 H + 3 X	4 H + 1 X	2 H + 2 X
	검증	4 H + 5 X	4 H + 5 X	4 H + 1 X	5 H + 3 X
	PW 변경	6 H + 6 X	6 H + 6 X	4 H	9 H + 7 X

(O : 공격으로부터 안전 , X : 공격 가능)
(H : Hash 연산량, X : XOR 연산량)

제안방식 2의 경우는 등록 과정에서 생성된 V값을 스마트카드에 저장하고 서버에서 생성된 V값 기반의 검증 메시지를 확인함으로써 스마트카드의 소유자를 검증한다. V값은 사용자의 PW기반으로 생성된 CPW와 함께 서버의 Sx, N를 입력으로 생성되기 때문에 서버의 정보 없이 생성될 수 없으며, 재등록 과정에서 생성되는 새로운 검증 정보는 N값 변화에 따른 임의의 해시 결과 값으로 다음에 사용될 Vnew 값을 추측하는 것은 어렵다. 따라서 스마트카드에 저장된 정보만으로 검증 정보 V를 생성하거나 추측할 수 없기 때문에 스마트카드를 분실 및 도난당했을 경우 공격자는 스마트카드에 저장된 정보를 추출하여 사용자의 패스워드를 추측하거나 스마트카드의 소유자를 검증할 수 없다. 기존 방식 및 제안 방식에 대한 분석은 Table 1과 같다.

6. 결 론

기존 아이디/패스워드기반의 인증 기술은 서버에서 사용자에 대한 검증을 위해 사용자의 패스워드 테이블을 구성해야 된다. 이러한 패스워드 테이블은 공격자에 의해 취득되거나 서버 내부자에 의해 노출됨에 따라 사용자의 ID 도용 문제가 발생할 수 있기 때문에 패스워드 테이블의 구성없이 사용자 인증 가능한 원격 사용자 인증 방식이 등장하였고 기존의 인증 매체를 대체한 보안 매체로써 스마트카드가 발달함에 따라 스마트카드를 이용한 다양한 원격 사용자 인증 방식들이 제안되었다.

본 논문은 사용자의 아이디/패스워드를 이용하여 스마트카드의 아이디와 패스워드를 생성하여 로그인 요청 메시지와 검증 메시지를 다르게 구성함으로써 위장 공격의 위협으로부터 안정한 방식과 서버에서 생성된 검증 정보를 이용하여 스마트카드의 소유자를 확인함으로써 스마트카드를 도난 및 분실 당했을 경우 발생할 수 있는 패스워드를 추측 공격 위협으로부터 안전한 방식을 제안하였다. 따라서 스마트카드를 이용한 안전한 원격 사용자 인증 방식을 제공할 수 있을 것이라 사료된다.

참 고 문 헌

[1] L. Lamport, “Password authentication with insecure communication” Communications of ACM. Vol 24, Issue 12, pp.770-772, 1981.

[2] M.S. Hwang, L.H. Li, “A new remote user authentication scheme using smart cards” IEEE Transactions on consumer Electronics, Vol.46, No.1, pp.28-30, 2000.

[3] H.M. Sun, “An efficient remote use authentication scheme using smart cards”, IEEE Transactions on consumer Electronics, Vol 46, No.4, pp.958-961, 2000.

[4] H.Y. Chien, J.K. Jan, Y.M. Tseng, “An efficient and practical solution to remote authentication: smart card”, Computers & Security, Vol.21, No.4, pp.372-375, 2002.

[5] W.C. Ku, S.M. Chen, “Weaknesses and Improvements of an Efficient Password Based Remote User Authentication Scheme Using Smart Card”, IEEE, Transaction on consumer Electronics, Vol.50, No.1, pp.201-207, 2004.

[6] E.J. Yoon, E.K.. Rye, K.Y. Yoo. “Further Improvement of an Efficient Password Based Remote User Authentication Scheme Using Smart Card”, IEEE Transaction on Consumer Electronics, Vol.50, No.2, pp.612-614, 2004.

[7] N.Y. Lee, Y.C. Chiu, “Improved remote authentication scheme with smart card”, Computer Standards & Interfaces 27, pp.177-180, 2005.

[8] X.M Wang, W.F. Zhang, J.S. Zhang. M.K. Khan, “Cryptanalysis and improvement on two efficient remote”, computer Standards & Interface 29, pp.507-512, 2007.

[9] T.H Chen, H.C. Hsiang, W.K. Shih, “Security enhancement on an improvement on two remote user authentication schemes using smart cards”, Future Generation computer Systems 27, pp.377-380, 2011.

[10] T.L. Chun, C.L. Cheng, “A ROBUST REMOTE USER AUTHENTICATION SCHEME USING SMART CARD”, Information Technology and Control, Vol.40, No.3, pp.236-245, 2011.

고 성 종

e-mail : sjgo@sch.ac.kr

2012년 순천향대학교 소프트웨어공학부 (학사)

2012년～현 재 순천향대학교 컴퓨터공학과 석사과정

관심분야 : 컴퓨터 보안, OTP, 스마트 카드, 인증

이 임 영

e-mail : imylee@sch.ac.kr

1981년 2월 홍익대학교 전자공학과

1986년 2월 오사카대학 통신공학전공(석사)

1989년 2월 오사카대학 통신공학전공(박사)

1985년～1994년 한국전자통신연구원 선임연구원

1994년～현 재 순천향대학교 소프트웨어학과 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안