# 개인정보보호를 위한 스마트카드 기반의 보안솔루션 설계

박정효, 김재우, 전문석
숭실대학교 일반대학원 컴퓨터학과
e-mail : {helios914, saypeace, mjun}@ssu.ac.kr

# A Design of Security Solution Based on Smart Cards for Privacy Protection

Jeong-Hyo Park, Jae-Woo Kim, Moon-Seog Jun
Dept of Computer Science, Soongsil University

요 약

유비쿼터스 시대의 도래로 인하여 웹 환경에서 원격서버로 사용자들의 통신이 급증함에 따라 최근에는 사용자의 개인 프라이버시 보호에 대한 관심이 증가하면서 사용자 익명성을 제공하는 스마트카드 기반 인증 프로토콜에 대한 연구가 활발하게 진행되고 있다. 하지만 기존에 제시된 익명성 기법들은 안전성 및 효율성에 대한 문제가 지속적으로 지적되어 왔다. 또한 그 중에서 가장 큰 문제점이 익명성과 역상성을 갖고 있는 추적 기술 이었다. 이에 본 논문은 이러한 사용자 인증에서의 부분 익명성 그리고 문제 발생 시 익명의 사용자를 추적할 수 있는 기법을 제안한다.

## 1. 서론

인터넷은 우리 생활에 없어서는 안 될 필수 요소가 되어가고 있다. 그러나 인터넷 서비스 및 전자상거래 이용 시 서비스 제공자들은 불필요하거나 지나치게 과도한 사용자의 개인정보를 요구하여 개인의 프라이버시를 침해하고 있으며, 또한 정보관리의 부주의로 인하여 대형 개인정보 유출사고가 빈번하게 발생하고 있다. 또한 인터넷 이용자들의 의식 변화로 개인정보 보호에 대한 인식이 커지고 있는 실정이다. 이러한 상황에서 중요한 개인 정보들은 제3의 믿을만한 기관에 안전하게 저장하고, 서비스 제공자에게는 꼭 필요한 정보만을 제공하는 방안을 생각할 수 있다. 그러나, 실명을 사용하는 현 인터넷 체계에서 이런 방법을 이용한 개인정보보호에는 한계가 있으며 이를 해결하기 위한 방안으로 익명 인증 방법이 논의되고 있다.

이에 따라 본 논문은 스마트카드를 이용하여 개인정보보호를 부분적으로 익명 인증하고 필요시에는 불법 사용자를 추적할 수 있는 보안하는 솔루션을 제안한다.

### 1.1. 익명성 정의

최근 개인 프라이버시 보호에 대한 관심 및 요구가 증가됨에 따라 사용자가 자신의 신원을 드러내지 않고 서비스나 리소스를 사용하는 것을 제공하는 방향으로 연구가 활발히 진행되고 있다. 익명성이란 어떤 행위를 한 사람의 신원이 드러나지 않는 특성으로서 통신채널 상에서 도청자로부터 정당한 사용자의 신원이 드러나지 않아야하는 익명 통신과 제3자뿐만 아니라 원격 서버에 대해서도 사용자의 신원이 보장되는 사용자 익명성으로 정의된다.

### 1.2. 추적성 정의

원격서버는 사용자의 신원을 신뢰기관을 통해 얻을 수 있다. 이때 악의적인 서버일 경우에도 정당한 사용자임을 알 수 없어야 한다.

서비스 제공자에 의한 개인정보유출사고 등이 증가하면서 제 3자뿐만 아니라 원격 서버에 대해서도 익명성이 보장되는 기법이 요구되고 있다. 하지만 이러한 익명 인증 기법은 원격서버가 사용자의 악의적인 행동을 감지했을 때 신뢰기관의 협조를 얻어 악의적인 사용자를 찾아낼 수 있어야 한다. 이 때, 시스템 내의 각 사용자는 유일하게 식별되어야 하며 각 사용자는 자신의 행위에 대해서 책임을 지어야 한다.

### 1.3. 환경

초기의 인증 기법들을 살펴보면, 등록단계에서 사용자가 원격 서버에 자신의 아이디와 비밀번호를 제출하고 서버는 사용자의 아이디와 비밀번호를 데이터베이스에 저장함으로써 등록이 이루어졌다. 하지만 이러한 기법은 정당한 사용자의 개인 프라이버시를 만족하지 않는다. 예를 들어, 사용자는 제 3자뿐만 아니라 서버관리자에게 자신이 다운받는 콘텐츠에 대한 사용자가 자신임을 알리기 원하지 않을 것이다. 하지만 미디어 콘텐츠를 다운 받는 사용자가 등록되지 않는 다수의 사용자에게 콘텐츠를 불법으로 배포할 때 신뢰기관의 협조를 얻어 악의적인 사용자를 추적하는 것이 가능해야 한다. 이러한 환경에서처럼 제3자뿐만 아니라 서버에 대해서도 사용자 익명성이 제공됨과 더불어, 신뢰기관의 협조를 얻어 악의적인 사용자를 추적할 수 있는 기법이 절실히 필요하다.

## 2. 관련연구

### 2.1. Das 인증 프로토콜 표기법

이번 장에서는 앞으로 프로토콜에서 사용될 용어에 대한 정의이다.

- $U_i$ : I번째 사용자
- S : 원격 서버
- $C_{ID_i}$ : I번째 사용자의 동적 ID
- r,e : 매 세션 마다 스마트카드에 의해 생성된 랜덤 값
- $x_s$ : 서버의 개인 키
- h() : 일방향 해쉬함수

### 2.1.1 Das 인증 프로토콜

Das[1] 등은 고정된 아이디를 사용함으로써 원격 인증 시 사용자의 부분 개인정보가 유출되는 것을 막기 위해 동적 아이디를 사용하여 사용자와 원격 서버를 제외한 제3자에게 대해 익명성을 보장하는 기법을 제안하였다. 이번 절에서는 Das 등의 기법에서 사용자의 익명성이 만족되지 않는 것을 중점으로 살펴볼 것이다. 이 기법은 등록 단계, 로그인 단계, 검증 단계로 구성되어 있다.

[등록 단계]

1. 등록단계에서 새로운 사용자 $U_i$는 자신의 $PW_i$를 안전한 채널을 통해 서버 S에게 제출한다.
2. S는 $N_i$를 계산하고 Ui의 스마트카드에 h(), Ni, y를 저장한다.
   $N_i = h(PW_i) \oplus h(x_s)$

[로그인 단계]

로그인 단계에서 $U_i$가 원격 서버에 로그인을 원할 때, 자신의 스마트카드를 리더기에 삽입한다. 스마트카드는 다음 과정을 수행한다.

1. $C_{ID_i} = h(PW_i) \oplus h(N_i \oplus y \oplus T)$를 계산한다.
2. $B_i = h(C_{ID_i} \oplus h(PW_i))$를 계산한다.
3. $C_i = h(N_i \oplus B_i \oplus y \oplus T)$를 계산한다.
4. 스마트카드는 $\{C_{ID_i}, N_i, C_i, T\}$를 S에게 보낸다.

[검증 단계]

S는 데이터 $\{C_{ID_i}, N_i, C_i, T\}$를 T′ 시간에 받고 다음과 같은 수행을 한다.

1. T와 T′ 사이의 시간 간격을 확인한다.
2. $h(PW_i) = C_{ID_i} \oplus h(N_i \oplus y \oplus T)$를 계산한다.
3. $B_i = h(C_{ID_i} \oplus h(PW_i))$를 계산한다.
4. 다음 식이 성립하는지 확인한다. 만약 식이 일치하면 요청을 받아들인다.
   $C_i = h(N_i \oplus B_i \oplus y \oplus T)$

### 2.1.2 Das 인증 프로토콜 분석

Das와 Saxena, Gulati는 동적 아이디를 사용함으로써 처음으로 사용자의 익명성을 제공한 인증 프로토콜을 제안하였다. 그러나 사용자 $U_i$가 데이터 $\{C_{ID_i}, N_i, C_i, T\}$를 서버에게 보낼 때, $N_i = h(PW_i) \oplus h(x_s)$는 고정된 값으로 등록단계에서의 정보를 이용하여 사용자를 추적하는 것이 가능하다는 것이 밝혀졌다. 즉, 로그인 단계에서 서버에게 보내는 데이터를 통해 사용자를 구분할 수 있게 됨으로써 사용자 익명성을 제공하지 못한다. 또한 이 프로토콜은 사용자 인증만을 제공한다[2,3,4,5].

## 3. 제안 시스템

제안 시스템은 웹서버로 안전한 인증을 하기 위한 시스템으로 설계되었으며, 사용자 단방향 인증을 사용자와 이용 시스템의 상호 인증으로 보완하였고, 사용자의 제3자에 의한 익명성뿐만 아니라 이용 시스템에서도 부분익명성이 가능하도록 제안되었으며, 기존의 내부자에 의한 개인정보 유출을 방지할 수 있도록 구성되어 있다.

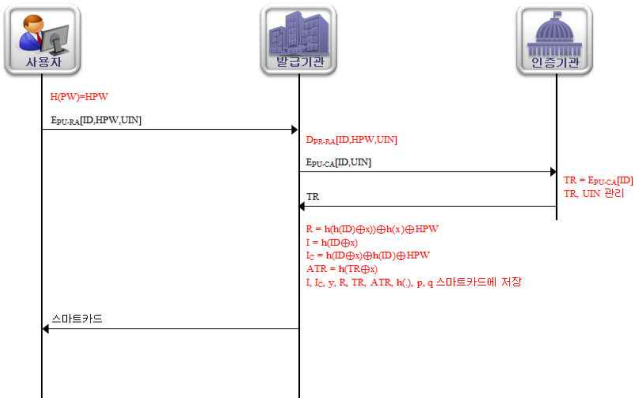
### 3.1. 시스템 파라미터

- ID : 사용자의 아이디
- PW : 사용자의 패스워드
- UIN : 사용자의 개인정보
- TR : 추적 정보
- x : 발급기관의 비밀키
- SK : 세션키
- CS : 불법적인 행동에 대한 리포트
- h(.) : 일방향 해쉬함수

### 3.2. 제안 프로토콜

제안된 프로토콜은 등록, 인증, 추적 총 3단계로 구성된다. 패스워드 변경은 아이디와 패스워드 인증을 통해 변경을 할 수 있으므로 본 논문에서는 제외하였다.

#### 3.2.1 등록 프로토콜




[그림 1] 등록 프로토콜

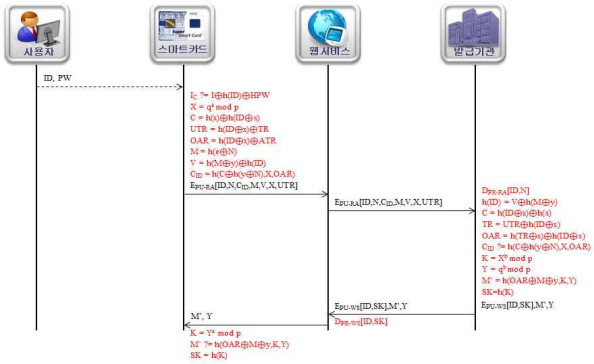
① $E_{PU-RA}$[ID,HPW,UIN]
사용자는 h(PW)를 하여 HPW를 생성하여 발급기관에 전송한다.

② $E_{PU-CA}$[ID,UIN]
발급기관은 사용자에게 받은 정보를 복호화하여 아이디와 개인정보를 인증기관으로 전송한다.

③ TR
인증기관은 추후 사용자의 추적을 위해 ID를 자신의 공개키로 암호화한 TR 값을 발급기관에 전송한다.

④ 스마트카드
발급기관은 사용자 인증과 세션키 생성을 위한 값들을 생성한 후 스마트카드 안에 저장하여 사용자에게 발급한다.

#### 3.2.2 인증 프로토콜




[그림 2] 인증 프로토콜

① ID,PW
사용자 인증을 위해 스마트카드를 리더기에 삽입 후 아이디, 패스워드를 입력하여 인증한다.

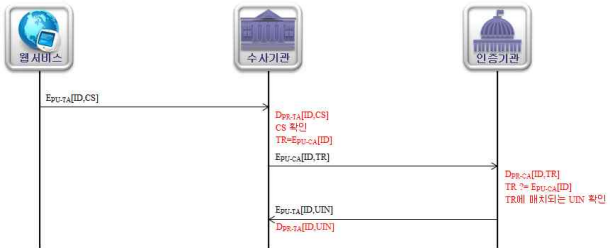
② $E_{PU-RA}$[ID,N,CID,M,V,X,UTR]
세션키 생성을 위해 사용자 아이디, 임의 값, 동적 아이디, 동적 아이디를 인증하기 위해 필요한 UTR, X, M, V를 웹서비스에게 전송한다.

③ $E_{PR-WS}$[$E_{PU-RA}$[ID,N,CID,M,V,X,UTR]]
웹 서비스는 전송받은 정보들에 자신의 개인키로 서명 후 발급기관에 전송한다.

④ $E_{PU-WS}$[ID,SK],$E_{PR-RA}$[M′,Y]
발급기관은 전송받은 정보들을 바탕으로 동적아이디를 확인 후 세션키를 생성한다.

⑤ $E_{PR-RA}$[M′,Y]
발급기관에서 서명된 값인 M′,Y를 가지고 발급기관의 인증을 하고 세션키를 생성한다.

#### 3.2.3 추적 프로토콜




[그림 3] 추적 프로토콜

① $E_{PU-TA}$[ID,CS]
웹서비스는 사용자의 불법적인 행위를 발견하였을 경우 사용자의 ID와 불법적인 행동은 CS를 수사기관에 전송한다.

② $E_{PU-CA}$[ID,TR]
수사기관은 CS를 판별 후, 사용자의 정보를 얻기

위해 인증기관에 사용자의 아이디와 추적 정보를 전송한다.

③ $E_{PU-TA}$[ID,UIN]
인증기관은 추적기관의 ID값이 TR과 매칭되는지 확인 후 아이디와 개인정보를 수사기관에 전송한다.

## 4. 성능분석

이번 장에서는 제안된 기법의 안전성과 기능에 대해 논하고, 기존 기법과 비교를 통해 효율성을 살펴본다.

### 4.1. 안전성 비교

[표 1] 안전성 비교 표

| 안전성 비교 | Das et al. | 제안 프로토콜 |
|---|---|---|
| 익명성 | △ | ○ |
| 추적 가능성 | × | ○ |
| 상호인증 | × | ○ |
| 가장 공격 | × | ○ |
| 키교환 | × | × |

1. 웹서비스는 사용자의 아이디와 패스워드를 알지 못하고 발급기관에서 인증을 해준 정보를 가지고 인증을 대행하기 때문에 사용자의 익명성을 보장한다.
2. 웹서비스는 사용자의 불법적인 행위를 발견하였을 경우 $C_{ID}$값과 TR값을 수사기관에 전송함으로서 불법 사용자를 추적할 수 있다.
3. 제안된 기법은 웹서비스와 사용자 간의 상호 인증이 발급기관을 통해 이루어지며 또한 주고받는 값을 통해 다시 한번 인증을 하게 된다.
4. 제안된 기법은 외부, 내부 공격자에 의한 가장 공격에 안전하다. 외부 공격자가 정당한 사용자의 아이디와 패스워드를 얻었다고 가정하였을 때, 정당한 로그인 정보를 위조하기 위해서는 V 값 안에 포함된 비밀 값 y를 알아야 $h(M \oplus y)$를 만들 수 있다. 하지만 공격자는 서버의 비밀 값을 알지 못하기 때문에 정당한 사용자 인척 가장할 수 없다. 내부 공격자일 경우 $h(x)$를 얻어도 TR 값과 서버의 비밀 키로 이루어진 OAR값을 생성 할 수 없기 때문에 $C_{ID}$를 구성할 수 없다.
5. 사용자는 스마트카드에서 M′와 Y를 전송받아 $K = Y^a \bmod p$, K 값을 구하고 위변조되었는지 OAR을 통해 확인하며 $SK = h(K)$를 통해 세션키를 생성하기 때문에 별도의 키교환이 필요하지 않다.

## 5. 결론

스마트카드를 이용한 원격 사용자 인증 기법은 사용자들의 프라이버시에 대한 관심이 증가하면서 점차 발전해왔다. 본 논문에서 제시한 기법은 스마트카드 특유의 이동성과 보안성을 살리면서 사용자의 익명성을 제공하는 프로토콜로서 인터넷 환경에서 인증을 필요로 하는 다양한 분야에서 활용 가능하다.

기존의 인터넷을 통한 사용자 인증으로는 ID/PWD 방식, OTP 방식, 인증서 방식, I-PIN 방식 등이 사용되고 있다. 하지만 별도로 서버측에 검증테이블을 관리하거나, 보안토큰을 요구하고 있다. 이러한 불가피한 문제들은 내부자 공격 또는 외부자 공격에 의한 개인정보 유출 사고를 지능화하고 있다.

본 논문에서는 이러한 보안문제를 해결하기 위해 별도의 토큰이 필요하지 않은 스마트카드를 사용하여 원격지 통신을 가능하게 하기 위한 프로토콜을 제안하였다.

## 참고문헌

[1] M. L. Das, A. Saxena and V. P. Gulati, "A dynamic ID-based remote user authentication scheme", IEEE Trans. Consumer Electron., vol. 50, No. 2, pp. 629-631, May 2004.

[2] Md. Misbahuddin, Md Aijz Ahmed, A. Ananda Rao, C. Shoba Bindu, and M.A. Muqsit Khan. "A Novel Dynamic ID-Based Remote User Authentication Scheme". Annual India Conference, pp:1-5, Sept. 2006.

[3] I-EN Liao, C.C.Lee,and M.S.Hwang, "Security enhancement for a dynamic ID-based remote user authentication scheme", in IEEE CS Press, International Conference on Next Generation WebServicesPractices(NWeSP'05),pp.437-440,Seoul,Korea,August 2005.

[4] W.C.KU and S.T.C, "Impersonation attack on a dynamic ID based remote user authentication using smartcards", IEICE Transaction on Communication, vol.e88-b,no.5,May 2005.

[5] 이영숙, 원동호, "스마트카드를 이용한 사용자 인증 스킴의 안전성 분석 및 개선," 한국컴퓨터정보학회 논문지, 제15권, 제 1호, 139-147쪽, 2010년 1월.