情報保護學會論文誌
第18卷 第5號, 2008. 10

스마트카드를 이용한 속성기반 사용자 인증 스킴

유 혜 정[1†], 이 현 숙[2‡]
[1]세종사이버대학교, [2]고려대학교, 울릉공대학교

An Attribute-Based Authentication Scheme Using Smart Cards

Hye Joung Yoo[1†], Hyun Sook Rhee[2‡]
[1]Sejong Cyber University, [2]Korea University, University of Wollongong

요 약

컴퓨터 네트워크 환경에서 사용자가 서버에서 제공되는 서비스를 요청할 때, 사용자는 인증 과정을 거쳐야만 한다. 이런 사용자 인증 과정을 통하여 서버는 사용자가 서버에서 제공하는 서비스를 이용할 수 있는지 그리고 이 서비스에 대한 정확한 접근 권한을 결정하게 된다. 이러한 사용자 인증 시스템에서 개인정보보호에 대한 중요성이 증대되고 있다. 이러한 프라이버시 보호 요구에 발맞추어 사용자 익명성을 제공하는 여러 인증기술이 제안되었으며, 최근에는 스마트카드를 이용한 사용자 익명성을 제공하는 인증 스킴이 제안되고 있다. 스마트카드를 이용한 사용자 인증 스킴은 사용자의 적격성을 입증하고 안전한 통신을 제공하는 매우 실용적인 기술이다. 그러나 아직까지 스마트카드를 이용한 사용자 익명성 제공 속성기반 인증에 대한 연구는 존재하지 않는다. 본 논문에서는 사용자를 인증하는 기술 중에서 스마트카드를 이용한 속성기반 인증 스킴을 제안하고자 한다. 스마트카드를 이용하여 계산량 측면에서 효율성을 취하고, 사용자는 한 번의 등록으로 속성에 따라 다양한 서비스를 안전하게 제공받을 수 있도록 하였으며, 사용자의 프라이버시 보호를 위해 원격 서버에게도 안전한 익명성을 제공받으면서 서버와의 상호 인증을 수행하도록 하였다.

ABSTRACT

In a network environment, when a user requests a server's service, he/she must pass an examination of user authentication. Through this process, the server can determine if the user can use the provided services and the exact access rights of this user in these services. In these authentication schemes, the security of private information became an important issue. For this reason, many suggestions have been made in order to protect the privacy of users and smart cards have been widely used for authentication systems providing anonymity of users recently. An remote user authentication system using smart cards is a very practical solution to validate the eligibility of a user and provide secure communication. However, there are no studies in attribute-based authentication schemes using smart cards so far. In this paper, we propose a novel user authentication scheme using smart cards based on attributes. The major merits include : (1) the proposed scheme achieves the low-computation requirement for smart cards; (2) user only needs to register once and can use permitted various services according to attributes; (3) the proposed scheme guarantees perfect anonymity to remote server.

Keywords : User Authentication, Smart Cards

Ⅰ. 서 론

사용자가 정보 자산에 접근을 요청할 때 시스템과 관리자는 사용자의 실재(實在), 사용자의 확인 그리고 권한의 부여와 같은 인증 허가의 일련의 과정을 거치게 되며, 이러한 일련의 과정에서 사용자 인증은 서버에서 제공하는 서비스의 접근 여부를 결정하게 된다.

사용자 인증 기술로 가장 널리 사용되는 방식으로는 사용자만이 알고 있는 정보 즉, 패스워드를 입력함으로써 사용자 인증을 수행하는 것이다. 전통적인 패스워드 기반 인증 스킴에서 서버 또는 시스템은 시스템에 등록된 사용자들의 패스워드 전부를 저장하기 위한 패스워드 테이블을 유지해야만 한다. 이러한 패스워드 테이블은 일반적으로 그 크기가 크고 다른 사람에게 드러나지 않아야 하기 때문에 이 같은 테이블을 유지한다는 것은 비효율적일 뿐 아니라 어려운 일이다. 이러한 패스워드 테이블에 대한 모든 가능한 공격을 피하고, 계산량과 통신량 측면에서 효율성을 취하고자 패스워드 테이블이 없는 스마트카드에 기반 한 많은 인증 시스템이 제안되었다[1,2]. C.I. Fan et al.[2]에서는 스마트카드를 이용한 안전한 원격 인증 스킴을 위한 조건 중 하나를 이용자의 패스워드를 포함한 테이블을 사용하지 않는 것이라 하였으며, 이를 포함한 안전성과 관련된 조건을 다음과 같이 요약하고 있다 :

1. 스마트카드의 계산량은 작아야만 한다.
2. 사용자의 패스워드를 포함한 테이블을 사용하지 않는다.
3. 사용자들은 자신의 패스워드를 자유롭게 선택할 수 있다.
4. 시간 동기화와 지체시간 제한을 요구하지 않는다.
5. 재연공격에 강하다.
6. 상호인증 기능을 제공한다.
7. 스마트카드 오프라인 사전공격에 강하다.
8. 분실된 카드는 취소가 가능하다.

일반적인 인증 시스템에서는 등록과 로그인 과정에서 사용자의 개인적인 정보를 전달하게 되는데, 이는 매우 주의를 요한다. 사용자의 구매 패턴이나 사적인 선호도 등과 같은 민감한 정보가 유출되어 마케팅 목적으로 남용되는 경우, 사용자의 프라이버시를 위배하는 결과를 낳아 법적인 대응까지 초래할 수 있기 때문이다. 이와 같이 사용자의 익명성은 서비스를 요청하고 서비스에 접근하는 동안 제공되어야 할 바람직한 안전성 요소라고 할 수 있으며, 최근 스마트카드를 이용한 인증 시스템에서도 사용자의 익명성을 제공하는 인증기술에 대한 연구가 진행되고 있다.

스마트카드를 이용한 인증 시스템에서 사용자 익명성에 대한 연구는 2004년 Das et al.[3]가 동적 아이디(Dynamic identity)를 이용하여 사용자 익명성을 제공하는 방법으로 처음 제안하였다.

지금까지 제안된 익명성을 제공하는 스마트카드를 이용한 인증 스킴들은 인증 단계에서 사용자의 익명성을 제공하지만 사용자에 따라서 인증의 권한을 다르게 주는 인증의 다양성은 제공하지 못한다. 서비스 접근에 대한 허가나 불가가 아닌 개인이 가진 다양한 속성 즉, 사용자의 직업, 거주 지역, 취미 등 관심분야 그리고 직위나 부서 등과 같은 특성 값들에 따라, 제공되는 서비스의 폭과 깊이를 달리 하지는 못하는 것이다. 예를 들어, 기존 스킴들은 기업의 인증 시스템과 같은 인증의 다양성을 요구하는 서비스에 활용되는데 다음의 두 가지 어려움이 존재한다. (1) 기업 내 특정 부서의 기밀문서가 다른 부서의 직원들에게 공개되는 것을 막기 위해 부서를 출입하는 직원들에게 사무실을 이동할 때마다 사용자 인증 시스템을 이용하도록 한다면 사용자의 위치정보 등 필요이상의 정보가 노출되어 개인의 프라이버시를 침해할 수 있을 것이다. (2) 그래서 이러한 피해를 줄이기 위해 사용자의 익명성을 제공하는 '스마트카드를 이용한 익명 인증 시스템'을 이용하고자 한다면 지금까지의 연구에서는 사용자 속성에 따라 사용자를 분류하여 다양하게 인증할 수 있는 방법이 존재하지 않는다.

인증의 다양성은 사용자의 프라이버시 보호를 위한 익명성을 제공하면서 사용자에게 제공되는 정보나 서비스가 사용자의 직업이나 직위, 소속에 따라 범위나 내용이 달라지는 환경에서 요구된다.

속성의 의미를 사용자의 직위나 소속으로 한정시키면, 사용자 인증에서 역할의 개념을 사용함으로써 스킴 내에서의 권한은 역할과 관련되어 사용자들은 역할의 한 멤버가 되고, 역할에 따라 부여받은 접근권한을 통하여 역할의 수행에 필요한 최소한의 자원만을 접근할 수 있도록 하여 권한의 이해와 관리를 간편하게 해주며, 이

접수일 : 2008년 5월 2일; 수정일 : 2008년 6월 30일;
채택일 : 2008년 7월 4일
† 주저자, 교신저자 hjyoo@sjcu.ac.kr

러한 점에서 속성기반 사용자 인증 스킴은 어느 정도 역할기반 접근제어 스킴과 유사한 점을 담고 있다고 할 수 있다. 그러나 역할기반 접근제어 스킴에서는 권한 관리를 단순화하고 특정한 보안정책을 구현하는데 있어서 유연성을 제공하는 것에 중요한 의미를 두고 있는 반면, 속성기반 인증 스킴에서는 각 개인이 소유한 역할을 포함한 다양한 속성에 따라 서비스 접근에 대한 폭과 깊이를 달리한다는 것에 중요한 의미를 둔다는 점에서 근본적인 차이가 있다. 즉, 역할기반 접근제어 스킴에서의 역할은 접근을 그룹화하지만 제안된 스킴에서의 속성은 접근을 다양화하고 세분화한다.

본 논문에서 제안한 스마트카드를 이용한 속성기반 인증 스킴은 인증의 다양성을 제공하기 위해 기존의 속성기반 암호화 기법의 특성을 인증 프로토콜에 도입한 기술이다. 사용자가 인증 시스템에서 이용할 자신의 스마트카드를 발급받을 때 자신의 속성에 대한 비밀 값을 포함한 스마트카드를 발급받게 되며, 실제로 아이디 기반 인증 시스템에서도 자신의 비밀 값을 제 3의 신뢰기관으로부터 발급받게 된다. 그러나 이렇게 발급받은 비밀 값들은 안전성을 보장받기 위해서 사용자가 기억하기에는 어려운 형태의 정보가 될 것이고, 결국 사용자가 안전하게 이 비밀 값을 저장하는 것이 요구된다. 더욱이 사용자의 속성 값이 여러 개인 환경을 생각한다면 그 속성 값들에 대한 비밀 값들을 안전하게 저장하기위해서는 스마트카드에 안전하게 저장하여 발급하는 형태를 생각하는 것은 자연스러운 결과이다.

스마트카드를 이용한 사용자의 익명성을 제공하는 속성기반 인증기법은 사내 및 국가적 차원의 기밀서류 열람통제 시스템과 직업이나 관심분야에 따라 특화된 다양한 서비스를 제공받을 수 있는 분산 환경에서의 인증 시스템과 같은 익명성을 필요로 하는 많은 환경에서 활용할 수 있을 것으로 기대된다. 또, 본 논문에서 제안한 인증 기술에서는 스마트카드를 이용하여 기존의 속성기반 암호화 기법에서 요구했던 페어링(pairing) 연산을 없애고 지수연산까지만 요구하고 있다. 이러한 연산량은 기존에 제안된 안전성이 증명된 익명 인증 스킴 중 키 교환을 요구하는 스킴과 동일하다는 점에서 계산량 측면의 효율성과 안전성 측면에서의 사용자 익명성을 제공하는 새로운 시스템에 대한 연구 측면에서도 의미가 있다고 할 수 있다.

본 논문의 구성은 다음과 같다. 제 2장에서는 제안된 시스템 구조와 관련된 연구들에 대해 간략하게 서술하고, 제 3장에서는 새로운 프로토콜을 제안한다. 다음으로 4장에서는 제안된 프로토콜의 안전성과 효율성을 분석하고 마지막으로 제 5장에서 결론을 끝으로 본 논문을 마무리 짓고자 한다.

Ⅱ. 용어 및 관련 연구

이번 장에서는 제안된 시스템 구조와 관련된 용어 및 연구들에 대해 간략하게 알아본다.

2.1 용어

- ID, pw : 사용자의 아이디, 사용자의 패스워드
- C_{ID} : 사용자의 동적 ID
- r, e : 스마트카드가 생성한 랜덤 값
- x_s , y : 서버의 비밀 키
- G : 서버가 정의한 모든 속성 값들의 집합
- A, A^* : G의 부분 집합
- $a_{i,j}$: 사용자 U_i에 해당하는 속성 값
- G^* : 위수가 소수p인 군
- $h()$: $\{0,1\}^* \rightarrow \{0,1\}^l$: 일방향 해쉬 함수
- $h()$: $\{0,1\}^* \rightarrow G^*$: full-domain 해쉬 함수
- T, ΔT: 타임스탬프, 타임스탬프 허용제한시간

2.2 Das et al. 스킴

Das et al.[3]의 스킴 구성을 알아본다. 이 스킴은 등록 단계, 로그인 단계, 검증 단계로 구성되어 있다.

〈등록 단계〉

1. 새로운 사용자 U는 자신의 패스워드 PW을 안전한 채널을 통해 서버 S에게 제출한다.
2. S는 N을 계산하고 U의 스마트카드에 해쉬함수 $h()$, N, S의 비밀 키 y을 저장한다: $N=h(PW)\oplus h(x_S)$, 여기에서 x_S는 S의 비밀 키이다.

〈로그인 단계〉

U가 원격 서버에 로그인을 원할 때, 자신의 스마트카드를 리더기에 삽입한다. 스마트카드는 다음 과정을 수행한다.

1. $C_{ID}=h(PW)\oplus h(N\oplus y\oplus T)$, 여기에서 C_{ID}는 사용자의 동적 ID이며, T는 타임스탬프이다.

2. $B=h(C_{ID}\oplus h(PW))$
3. $C=h(N\oplus B\oplus y\oplus T)$
4. 스마트카드는 $\{C_{ID}, N, C, T\}$을 S에게 보낸다.

〈검증 단계〉
S는 데이터 $\{C_{ID}, N, C, T\}$을 T' 시간에 받고 다음을 수행한다.
1. T와 T' 사이의 시간 간격을 확인한다.
2. $h(PW)=C_{ID}\oplus h(N\oplus y\oplus T)$을 계산한다.
3. $B=h(C_{ID}\oplus h(PW))$을 계산한다.
4. C와 $h(N\oplus B\oplus y\oplus T)$의 값이 같은지 확인한다. 만약 값이 일치하면 요청을 받아들인다.

로그인 단계에서 사용자가 $\{C_{ID}, N, C, T\}$을 서버에게 보내면, 서버는 자신이 등록 단계에서 사용자마다 유일하게 할당하는 고정 값 N을 이용하여 사용자를 추적하는 것이 가능하게 된다. 따라서 위 스킴은 사용자의 서버에 대한 익명성이 제공되지 않는다.

2.3 속성기반 암호(ABE) 시스템

Sahai와 Waters[4]에 의해 처음 제안된 속성기반 암호(ABE) 시스템은 기존의 신원(identity)기반 암호 시스템을 일반화한 것으로 속성 값을 암호 인자로 사용하여 속성에 대한 비밀 키를 가지고 있는 사용자만이 암호화된 데이터를 복호할 수 있도록 제안된 암호화 기법이다. 이러한 속성기반 시스템은 분산 환경에서 데이터의 안전성을 위한 잠재력에 대해 높이 평가받고 있다. Sahai와 Waters의 ABE 시스템은 다음 네 개의 알고리즘으로 구성되어 있다.

$<Set-up(k)>$
임계 값 k을 입력 값으로 하여 마스터 키 MK와 일련의 공개 파라미터 PK을 출력한다.
$k\rightarrow Set-up(k)\rightarrow(MK, PK)$

$<Key-Gen(S, MK)>$
사용자의 속성 값들의 집합 S와 MK을 입력 값으로 하여 S의 비밀 키 SK을 출력한다.
$(S, MK)\rightarrow Key-Gen(S, MK)\rightarrow SK$

$<Encrypt(M, S', PK)>$
사용자는 타깃 집합 S'와 공개 파라미터를 가지고 메시지 M을 암호화한다.
$(M, S', PK)\rightarrow Encrypt(M, S', PK)\rightarrow C$

$<Decrypt(C, S', S, SK)>$
S와 SK을 가지고 있는 사용자는 복호 알고리즘을 통해 암호문 C을 복호한다. 이때, $|S\cap S'|\geq k$인 경우에만, 평문 M으로 복호가 가능하게 된다.
$(C, S', S, SK)\rightarrow Decrypt(C, S', S, SK)\rightarrow M$

Ⅲ. 제안된 스킴

Das et al.의 스킴을 처음으로 스마트카드를 이용한 익명 인증 스킴들이 제안되고 있다. 하지만 익명성을 제공하면서 시스템 접근 권한을 증명하기 위한 기술은 사용자의 접근의 다양성을 제공하기에는 무리가 있다. 본 논문에서는 수신자가 어떠한 특정 속성을 만족한다는 것을 송신자는 알지만 수신자의 신원을 알 수 없는 속성기반 암호 시스템의 특성을 인증 시스템에 적용하여 인증의 다양성을 제공하고자 하였다. 우리의 스마트카드를 이용한 속성기반 인증 스킴의 특성은 다음과 같다.

1. 사용자 인증: 사용자는 자신의 아이디, 패스워드와 서버로부터 발급된 스마트카드를 이용하여 인증 메시지를 생성하게 된다. 이때, 사용자는 자신에게 부여된 속성에 대한 비밀 값을 포함하는 인증 메시지를 발생하여 서버로부터 사용자 인증을 수행한다.

2. 사용자 익명성: 서버는 로그인 메시지로부터 정당한 속성에 대한 비밀 값을 검증하여 특정 속성에 대한 정당성을 검증하게 된다. 이때, 서버는 로그인 메시지로부터 사용자의 아이디나 패스워드와 같은 개인정보를 얻을 수는 없다.

3. 인증의 다양성: 익명성을 제공하는 기존의 인증 시스템의 경우 사용자 익명성 제공이라는 목적에 부합하기 위하여 사용자 정보를 전혀 얻을 수 없도록 엄격하게 제한하거나 인증 시스템 사용에 대한 필요성이 확보된 경우 사용자 정보의 과다한 노출이 문제가 되고 있다. 이 경우 사용자의 신원이 아닌 직위나 부서 혹은 직업과 같은 속성에 따라서 접근 권한을 줄 수 있는 인증방법이 있다면 응용에 맞는 유연한 익명성을 제공하면서

다양한 분야에 활용 가능하게 될 것이다.

본 논문에서 제안한 속성기반 인증 스킴은 등록, 로그인 그리고 검증 단계로 구성된다. 등록 단계는 사용자가 카드를 잃어버리거나 패스워드를 잊지 않는다면 각각의 사용자에 대해 단 한번만 수행하게 된다.

먼저 서버는 각 속성 값별로 제공받을 수 있는 서비스를 정의를 내리는 것이 필요하다. 사용자는 서버가 제공할 수 있는 서비스를 확인한 후 자신의 개인정보를 이용하여 서버에 등록하게 되고, 이때 서버는 사용자가 가지고 있는 자격(직업, 직위 등)을 인증하고 사용자에게 제공할 수 있는 서비스에 해당하는 특성 값을 제공하게 된다. 사용자는 발급받은 특성 값들을 이용하여 그때그때 필요한 서비스를 요청하게 되는 것이다.

〈등록 단계〉

등록 단계를 통하여 사용자 U_i는 자신의 아이디와 패스워드를 인증 서버 S에 등록한다. S는 다음과 같은 인증 정보를 U_i의 스마트카드에 안전하게 저장한다. 등록 단계에서 발급받은 속성 값들의 부분 집합을 이용해 단 한 번의 발급으로 다양한 속성 값들의 조합을 통하여 다양하고 특성화된 서비스를 제공받을 수 있게 된다.

1. U_i는 자신의 아이디 ID와 패스워드 pw을 선택한 후 안전한 채널을 통하여 S에게 (ID, pw)을 보낸다.
2. (ID, pw)을 전송받은 S는 U_i에 해당하는 n개의 속성 값 $a_{i,j} \in A_i, 1 \le j \le n$ $(A_i \subseteq G)$와 자신의 비밀키 x_S을 이용하여 V, I, Y_i을 다음과 같이 계산한다. 여기서 G는 S가 정의한 모든 속성 값들의 집합이다.
   (1) $V = h(x_S) \oplus h(pw)$ 이고 $I = h(x_S) \oplus h(ID \oplus pw)$
   (2) $y_i = h(a_{i,j} \oplus x_S) \oplus h(x_S)$, $1 \le j \le n$ 그리고 $Y_i = y_1, \ldots, y_n$
3. S는 안전한 채널을 통하여 U_i의 스마트카드에 $(A_i, h(\cdot), Y_i, V, I)$을 저장하여 발급한다.

〈로그인 단계〉

U_i는 자신이 가진 다양한 속성 중에서 원하는 서비스를 제공받기 위해 필요한 k개의 특정 속성 값 집합 $A^* = \{a_{i,j_t} | a_{i,j_t} \in A_i, 1 \le t \le k \le n\}$에 대해 서버와의 인증을 위해서 다음의 과정을 수행한다. 이때, 사용자의 익명성을 위해서 서버는 사용자의 ID와 pw에 대한 정보를 인증 메시지로부터 알 수 없어야 한다.

1. U_i는 자신의 스마트카드를 리더기에 삽입하고 자신의 pw와 선택한 k개의 속성 값 $a_{i,j_t}, 1 \le t \le k$을 입력한다.
2. 스마트카드는 다음을 수행한다.
   (1) $V \oplus h(pw) \oplus h(ID \oplus pw) = I$인지를 체크하여 만족한다면 다음 단계를 수행하고 만족하지 않는다면 멈춘다.
   (2) W, X_t, X 값을 계산한다: $W = V \oplus h(pw)$, $X_t = y_t \oplus W (1 \le t \le k)$, $X = \prod_{t}^{k} X_t$
   (3) 임의의 수 $r, r' \in G^*$을 선택하고 스마트카드의 타임스탬프 T을 이용하여, $C_1 = (X \| T)^r$, $C_2 = W \oplus r$ 그리고 $C_3 = g^{r'}$을 계산한다. 이때, g는 G의 생성원이다.
   (4) 인증을 위해 S에게 로그인 메시지 $C = [(a_{i,j_1}, a_{i,j_2}, \cdots, a_{i,j_k}), C_1, C_2, C_3, T]$ 을 전송한다.

〈검증 단계〉

S는 U_i의 스마트카드로부터 로그인 메시지 C을 T' 시간에 받은 후 다음과 같은 연산을 수행한다.

1. 전송 시 고려된 유예 시간 ΔT을 이용하여 현재시간 T'와의 시간차를 확인하여 $|T - T'| < \Delta T$이면 다음 단계를 수행한다.
2. $a_{i,j_t} \in A, 1 \le t \le k$의 형태가 맞는지를 체크한다. 만약 형태가 옳지 않다면, S는 로그인 요청을 거절한다.
3. $r'' = C_2 \oplus h(x_s)$와 $Z = \prod_{j_t}^{k} h(a_{i,j_t} \oplus x_s)$을 계산한다.
4. $(Z \| T)^{r''} = C_1$인지를 체크하고, 만약 성립한다면, S는 로그인 요청 수락 후 다음 단계로 간다.
5. S는 임의의 수 $e \in G^*$을 선택하고 상호 인증 메시지 $C_3 = Z^{r''+1}$와 $C_4 = g^e$을 계산한 후 U_i의 스마트카드로 전송한다.
6. C_3을 받자마자, U_i의 스마트카드는 이 값이 $W^{r+1} = C_3$ 인지를 체크한다. 만약 등호가 성립하면 U_i는 S가 정당한 서버임을 확신하게 되어 U_i와 S 사이의 상호인증이 성립하게 되고 세션 키 $K = g^{r'e}$값을 공유하게 된다.

〔표 1〕 효율성 분석

프로토콜	계산 량			사용자 익명성	세션 키 교환	속성기반 인증
	로그인	인증	총계			
Our Scheme	2H+1E	2H+3E	4H+4E	**Yes**	**Yes**	**Yes**
Das et al. scheme[3]	5H	3H	8H	No	No	No
Yoon et al. scheme[5]	5H+1E	4H+3E	9H+4E	**Yes**	No	No
Chien et al. scheme[6]	1H+1E+1S	3H+2E+2S	4H+3E+3S	No	**Yes**	No

H : 해쉬 함수의 계산량, E : 지수계산, S : 대칭키 암호/복호

Ⅳ. 분 석

이 장에서는 제안된 스킴의 안전성과 효율성을 분석한다. 안전성의 기본요소는 C.I. Fan et al.[2]에서 분류된 조건 중 제안된 인증 스킴에서 요구되는 것과 그 외 중요하다고 여겨지는 안전성 요소를 모두 고려하였다. 제안된 스킴은 가장 공격, 오프라인 패스워드 공격 그리고 재사용 공격에 대해서 안전하고 forward-secure 성질을 만족하며, 외부 공격자와 악의적인 서버에 대한 사용자의 익명성을 제공한다. 이때 스마트카드의 temper-resistant 성질을 기반으로 공격자가 사용자의 스마트카드를 오염시키거나 스마트카드로부터 정보를 얻는 공격은 고려하지 않으며, 공격자는 네트워크의 정보를 모두 얻을 수 있는 것으로 가정한다. 다음은 안전성에 대한 자세한 설명이다.

1. 은밀한 검증자 공격(stolen-verifier attack)
   제안된 프로토콜은 검증 테이블을 필요로 하지 않는다. 따라서 어느 누구도 서버로부터 검증할 수 있는 정보를 얻을 수는 없다. 그러므로 제안된 스킴은 은밀한 검증자 공격에 대해서 안전하다.

2. 사용자 가장 공격(user-impersonation attack)
   공격자가 사용자가 선택한 속성들에 대한 정당한 인증 메시지를 생성하기 위해서는 C_1과 C_2에 사용된 임의의 값 r 또는 서버의 비밀 키에 대한 해쉬 값 $h(x_S)$ 그리고 서버의 비밀 키 x_S 값을 알 수 있어야한다. 따라서 x_S 값이 서버의 비밀 키라는 가정에 기반을 두고 사용자 가장 공격에 대해서 안전하다.

3. 서버 가장 공격(server-impersonation attack)
   인증 메시지에 대한 정당한 답신 메시지를 생성하기 위해서 공격자는 서버의 비밀 키 x_S을 알거나 C_2로부터 r 값을 알 수 있어야 한다. 따라서 제안된 스킴은 서버 가장 공격에 대해서 안전하다.

4. 오프라인 패스워드 공격(offline password attack)
   정당한 사용자의 로그인 메시지는 사용자의 패스워드 정보를 포함하지 않는다. 단지, 로그인 메시지 생성단계에서 자신의 아이디와 패스워드 정보 그리고 스마트카드를 이용하여 정당한 로그인 메시지를 생성하게 된다. 따라서 공격자는 로그인 메시지로부터 사용자의 패스워드 정보를 얻을 수 없다.

5. 사용자의 익명성(user anonymity)
   정당한 사용자의 로그인 메시지는 사용자의 패스워드 정보를 포함하지 않고 등록 단계에서 서버로부터 부여받은 속성 값에 대한 인증을 수행하고 서버도 속성 값들에 대한 검증만을 수행한다. 따라서 로그인 메시지는 사용자의 아이디나 패스워드 정보를 포함하지 않기 때문에 서버와 외부 공격자 모두에게 사용자의 익명성을 제공하게 된다.

6. 재사용 공격(replay attack)
   정당한 사용자에 의해서 생성된 로그인 메시지를 그대로 이용할 경우 타임스탬프 체크 방법에 의해서 본 논문에서 제안된 스킴은 재사용 공격에 대한 안전성을 제공하게 된다.

본 논문에서 제안된 스킴은 스마트카드를 기반으로 구성되었기 때문에 계산상의 효율성 또한 중요하다고 할 수 있다. 이전에 제안된 스마트카드를 이용한 익명 인증 스킴 중 최근 결과인 Das et al.[3], Yoon et al.[5] 그리고 Chien et al.[6]의 스킴과의 비교를 통해서 효율성을 분석하고자 한다. 계산량의 비교를 위해서 우리가 제안한 스킴에서 하나의 속성에 대한 검증을 위한 계산

량을 비교·분석하였다. 표 2의 결과를 통해서도 알 수 있듯이 제안된 스킴은 세션 키를 교환하는 Chien et al. 스킴보다 대칭키 암호 계산을 이용하지 않는다는 측면에서 효율적이며, 익명성을 제공하는 Yoon et al.의 스킴보다 좀 더 효율적이다. 만약 Yoon et al.의 스킴에서 세션 키 교환의 기능을 추가한다면 더 많은 계산량을 요구하게 될 것이다.

V. 결 론

본 논문에서 제안된 스킴은 스마트카드를 이용한 속성기반의 사용자 익명성을 제공하는 최초의 프로토콜로 인증방법의 다양성을 제공한다는 측면에서 그 의미가 크다고 할 수 있다. 사용자가 자신의 아이디, 패스워드와 서버로부터 발급된 스마트카드를 이용하여 인증 메시지를 생성할 때, 자신에게 부여된 속성에 대한 비밀값을 포함하는 인증 메시지를 발생하여 서버로부터 사용자 인증을 수행함으로써 사용자는 한 번의 등록으로 속성에 따라 다양한 서비스를 제공받을 수 있으며, 이때 서버는 로그인 메시지로부터 사용자의 아이디나 패스워드와 같은 개인정보를 얻을 수 없게 되어 사용자는 외부 공격자뿐만 아니라 서버에 대해서도 타당한 익명성을 제공받게 된다. 본 스킴은 다중 서버 환경으로의 확장이 가능하며, 각 서비스 별 속성 값 구성에 대한 속성 정책 연구가 요구된다.

참고문헌

[1] M.S. Hwang and L.H. Li, "A new remote user authentication scheme using smart cards", *IEEE Transactions On Consumer Elctronics*, Vol. 46, No1, pp. 28-30, 2000.

[2] C.I. Fan, Y.C. Chan, Z.K. Zhang, "Robust remote authentication scheme with smart cards", *Computers and Security 2005*, Vol. 24, No.8, pp. 619-628, 2005.

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

[4] A. Sahai and B. Waters, "Fuzzy identity based encryption", In Eurocrypt 2005, 2005.

[5] E.J. Yoon, E.K. Ryu, K.Y. Yoo, "Efficient remote user authentication scheme based on generalized ElGamal signature scheme," *IEEE Transactions on Consumer Electronics*, Vol. 50, No.2, pp. 568-570, 2004

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

〈著者紹介〉

유 혜 정 (Hye Joung Yoo) 정회원

1997년 2월 : 고려대학교 수학과 졸업
1999년 2월 : 고려대학교 수학과 석사
2002년 8월 : 고려대학교 수학과 박사 정보보호전공
2003년 3월~2004년 12월 : 고려대학교 정보보호대학원 계약조교수
2004년 1월~현재 : 세종사이버대학교 정보보호시스템학과 조교수
<관심분야> 암호프로토콜, 컨텐츠 보안

이 현 숙 (Hyun Sook Rhee) 정회원

1998년 2월 : 단국대학교 수학과 졸업
2000년 2월 : 단국학교 수학과 석사
2008년 2월 : 고려대학교 정보경영공학전문대학원 박사 정보보호전공
2008년 3월~2008년 8월 : 고려대학교 정보경영공학전문대학원 박사후과정
2008년 9월 ~ 현재 : 호주 울릉공대학교 박사후과정
<관심분야> 암호프로토콜, 사용자 익명성, 데이터 프라이버시 보호기술