논문 2010-05-21

속성기반 재 암호화를 이용한 스마트카드 인증권한 분배스킴

(Smart Card Certification-Authority Distribution Scheme using Attributes-Based Re-Encryption)

서 화 정, 김 호 원*
(Hwa-Jeong Seo, Ho-Won Kim)

Abstract : User authentication is an important requirement to provide secure network service. Therefore, many authentication schemes have been proposed to provide secure authentication, such as key agreement and anonymity. However, authority of scheme is limited to one's self. It is inefficient when authenticated users grant a certification to other users who are in an organization which has a hierarchical structure, such as a company or school. In this paper, we propose the first authentication scheme to use Attributes-Based Re-encryption that creates a certification to other users with specified attributes. The scheme, which has expanded from Rhee et al. scheme, has optimized computation performance on a smart card, ensuring the user's anonymity and key agreement between users and server.

Keywords : Attribute-based encryption, Attribute based proxy re-encryption, Smart card, User authentication

1. 서 론

네트워크 서비스를 안전하게 제공하는데 있어 사용자 인증은 중요한 과정이다. 따라서 사용자는 서비스 요청 시 인증 서버와 상호인증 후 서비스를 제공받게 된다. 하지만 인증과정에 사용되는 개인정보는 공격자에게 노출 시 악의적인 목적으로 사용되어 사용자에게 피해를 줄 수 있다. 따라서 사용자의 정보를 안전하게 보호하기 위해 익명성을 제공하며 상호간의 안전한 인증 및 키교환이 가능한 기법들이 제안되고 있다.

2008년, 스마트카드에 속성기반암호화[3]를 적용한 인증 스킴인 Rhee et al.[4]이 제안되었다. 해당 스킴은 인증에 대한 권한을 속성에 따라 설정가능하다. 하지만 자신의 인증권한을 이용하여 다른 사용자에게 인증을 부여하는 것은 불가능하다. 예를 들어 회사와 같은 계층구조를 가진 조직에서 서버에 대한 접근권한을 가진 과장이 출장 중인 경우 같은 부서의 대리에게 특정 서버에 대한 접근권한 부여가 불가능하다.

하지만 본 논문에서 제안하는 속성기반 재암호화를 통한 인증권한 재분배 스킴은 다른 사용자에게 인증권한을 부여하는 것이 가능하다. 해당 스킴은 과장이 대리의 특정한 속성(직위, 부서)정보를 이용하여 재암호화를 한 후 Proxy서버를 통해 재암호문을 대리에게 제공된다. 재암호문을 전달받은 대리는 과장의 인증권한과 자신의 속성값을 이용하여 인증 서버로부터 인증을 받을 수 있다. 또한 대리의 익명성이 보장되며 서버와 대리 상호 간의 키교환도 안전하게 수행된다.

본 논문은 제 2장에서 논문과 관련된 연구들에 대해 소개하고 제 3장에서는 속성기반 재암호화기법을 이용한 인증권한 재분배 스킴을 제안한다. 제 4장에서는 제안한 기법의 성능 및 안전성을 분석하며 마지막으로 제 5장에서는 제안된 스킴에 대한

* 교신저자(Corresponding Author)
논문접수 : 2010. 08. 04., 수정일 : 2010. 08. 31.,
채택확정 : 2010. 09. 15.
서화정, 김호원 : 부산대학교 컴퓨터 공학과
※ 이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2008-0061842).

결론을 내린다.

II. 관련연구

본 논문에서 사용되는 용어와 제안된 스킴과 관련된 연구결과에 대해 설명한다.

1. 용어

[표 1]는 Rhee et al.과 제안된 스킴에 사용된 용어에 대한 설명이다.

표 1. Rhee et al.과 제안된 스킴에 사용되는 용어
Table 1. Terms used in Rhee et al. and proposed scheme.

기호	설명
ID	사용자의 아이디
pw	사용자의 패스워드
r, r_p, e	스마트카드와 서버에서 생성되는 랜덤 값
x_s	서버의 비밀 키
C	인증에 필요한 로그인 메시지
G	서버가 정의한 속성 값들의 집합
A, A^*	G의 부분 집합
U_i	사용자 i를 나타내는 기호
U_a	사용자 a를 나타내는 기호
S	인증 서버를 나타내는 기호
S_{U_i}	사용자 i의 Proxy server를 나타내는 기호
$a_{i,j}$	사용자 U_i에 해당하는 속성 값
G^*	위수가 소수 p인 군
$h()$	$\{0,1\}^* \rightarrow \{0,1\}^l$ 일방향 해쉬 함수
$T, \triangle T$	타임스탬프, 타임스탬프 허용제한시간
g	Diffie-Hellman 키교환 프로토콜의 파라미터
$\oplus$	bitwise exclusive-or 연산
$=>$	안전한 회선을 통한 전송
$\rightarrow$	일반 회선을 통한 전송

2. 선행연구

Rhee et al. scheme은 속성기반 암호화를 이용하여 새로운 인증 기법을 제안하였다. 해당 스킴은 속성에 따라 사용자에게 다양한 조건에 따른 인증이 가능하게 한다. 하지만 인증권한에 대한 분배 기능은 제공하지 않는다. 따라서 본 논문에서는 속성기반 프록시 재암호화 기법을 이용하여 특정한 속성을 가진 사용자에게 인증권한 분배를 제안한다.

2.1. 속성기반 암호화(ABE : Attribute-Based Encryption)

Sahai와 Waters에 의해 제안된 퍼지 아이디 기반 암호화(Fuzzy Identity-Based Encryption) 기법[3]은 신원(Identity)기반 암호화 기법[2]을 확장한 것으로 송신자가 선택한 속성 값을 암호 인자로 암호화하여 해당 속성값을 가지고 있는 수신자가 복호화할 수 있도록 제안된 시스템이다. 해당 기법은 암호화 과정이 기존의 신원 기반 암호화 기법에서와 같이 1대1관계가 아닌 1대N관계이므로 분산 환경 시스템에서의 다양한 응용에 적용가능하다.

2.2. Rhee et al. scheme[4]

Rhee et al.의 scheme은 속성기반 암호화를 스마트카드인증에 최초로 적용하였다. 속성값을 사용하여 상호간의 인증을 익명으로 수행이 가능하며 서버와 사용자간의 세션키분배도 Diffie-Hellman Protocol을 통해 안전하게 수행된다. 또한 Chien et al.[1]와 달리 대칭키 암호를 사용하지 않으므로 성능이 개선된다. 스킴은 [표 2]의 등록 단계, [표 3]의 로그인 단계, 그리고 [표 4]의 검증단계로 구성된다. 등록단계는 스마트카드를 부여받을 때 [Step 1]에서 자신의 ID와 password에 대한 정보를 서버쪽으로 전송한다. [Step 2~3]에서는 서버의 비밀키, 스마트카드의 비밀키 값 그리고 스마트카드의 아이디에 해쉬와 XOR연산을 수행하여 암호문을 생성한다. [Step 4]에서는 속성값과 서버의 비밀키값을 XOR연산을 한 후 해시를 하며 서버의 비밀키 값에 대한 해시값을 다시 XOR연산한다. [Step 5]에서는 생성된 메시지를 스마트카드로 안전한 회선을 통해 전송한다.

표 2. 등록 단계
Table 2. Registration phase

1 $U_i => S$: ID, pw를 전송한다.
2 S : $V = h(x_s) \oplus h(pw)$를 계산한다.
3 S : $I = h(x_s) \oplus h(ID \oplus pw)$를 계산한다.
4 S : $y_i = h(a_{i,j} \oplus x_s) \oplus h(x_s)$를 계산한다. 속성값은 $a_{i,j} \in A_i, 1 \leq j \leq n$ $(A_i \subseteq G)$조건을 만족한다.
5 $S => U_i$: $(A_i, h(), Y_i, V, I)$를 전송한다.

로그인과정은 스마트카드를 통한 인증이 필요한 시점에 수행되어 서버와의 인증에 필요한 메시지를 생성한다. [Step 1]에서는 스마트 카드의 아이디와 비밀번호 그리고 속성값을 입력한다. [Step 2~3]에서는 비밀키값을 통해 V, W 값을 생성한다. [Step 4]에서는 속성값과 W값을 XOR연산을 하며 [Step 5]에서는 타임 스탬프와 키교환에 사용되는 인자를

생성하여 해쉬 및 XOR연산을 수행한다. [Step 6]에서는 생성된 결과값을 인증 서버에게 보내게 된다.

표 3. 로그인 단계
Table 3. Login phase

1 스마트카드를 terminal에 넣고 ID, pw 그리고 선택한 k개의 속성 값 $a_{i,j_t}, 1 \leq t \leq k$를 입력한다.
2 U_i : $V \oplus h(pw) \oplus h(ID \oplus pw)$를 계산하여 I값과 비교하여 동일한 경우 다음 단계를 진행한다.
3 U_i : $W = V \oplus h(pw)$를 계산한다.
4 U_i : $X_t = y_t \oplus W(1 \leq t \leq k), X = \prod_t^k X_t$를 계산한다.
5 U_i : $C_1 = (X \| T)^r, C_2 = W \oplus r, C_3 = g^{r'}$을 계산한다. $r, r' \in G^*$는 임의의 수, T는 타임스탬프 그리고 g는 G의 생성원이다.
6 $U_i \rightarrow S$: $C = [(a_{i,j_1}, a_{i,j_2}, \ldots, a_{i,j_k}), C_1, C_2, C_3, T]$을 전송한다.

검증과정의 [Step 1]에서는 스마트 카드로부터 받은 메시지의 타임스탬프를 확인하여 재전송 공격을 판단한다. [Step 2]에서는 전송된 속성값이 특정 속성을 만족하는지 확인한다. [Step 3~4]에서는 전달되어온 메시지로부터 인증에 필요한 값을 계산하기 위해 지수 인자와 밑수를 계산한다. [Step 5]에서는 상대방과 키교환 및 상호인증에 필요한 메시지를 생성한다. [Step 6~7]에서는 스마트카드로 전송된 메시지를 확인하여 서버임을 확인하고 Diffie-Hellman기법을 사용하여 서버와 스마트카드 간의 키교환을 하게 된다.

표 4. 검증 단계
Table 4. Verification phase

1 S : T를 계산하여 $\triangle T$를 만족하는지 확인한다.
2 S : 전송된 속성값 $a_{i,j_t} \in A, 1 \leq t \leq k$이 조건을 만족하는 경우 다음 단계를 진행한다.
3 S : $r'' = C_2 \oplus h(x_s)$와 $Z = \prod_{j_t}^k h(a_{i,j_t} \oplus x_s)$를 계산한다.
4 S : $(Z \| T)^{r''}$를 계산하여 C_1와 동일한 경우 다음 단계를 진행한다.
5 S : $C_4 = Z^{r''+1}$와 $C_5 = g^e$를 계산한다. 임의의 수 $e \in G^*$를 만족한다.
6 $S \rightarrow U_i$: $B = [C_4, C_5]$를 전송한다.
7 U_i : X^{r+1}를 계산하여 C_4와 동일한 경우 서버에 대한 인증이 되며 세션키 $C_5^r = g^{re}$를 공유하게 된다.

2.3. 속성기반 프록시 재암호화 기법(ABPRE : Attribute Based Proxy Re-encryption with Delegating Capabilities)[5]

ABPRE 방식은 ABE를 통해 사용자(U_1)의 속성값으로 암호화된 암호문 C를 다른 사용자($U_2, \ldots U_n$)의 속성값으로 재암호화하여 재암호문 C'를 Proxy Server로 제공한다. 예를 들어 회사의 부서정보시스템에 대한 접근정보가 과장(U_1)의 속성값((나이 >40) $\wedge$ (접근권한))으로 암호화되어 있는 경우 과장이 출장 중 일때 부서정보를 복호할 수 있는 다른 사용자($U_2, \ldots U_n$)가 필요한 경우가 있다. 이 경우 ABPRE방식을 이용하면 다른 사용자에게 인증권한 부여가 가능하다. 과장은 암호문 C를 다른 사용자의 속성값($U_2, \ldots U_n$)를 이용하여 변환한 후 프록시를 지정하여 암호문 C'를 제공한다. 따라서 과장이 없어도 다른 사용자가 과장의 대리인으로써 암호화된 정보에 접근 할 수 있다. ABPRE 암호는 6개의 단계로 구성된다.

-Setup$(1^k) \rightarrow (pp, mk)$: 비밀 값 1^k를 입력하여 공개 값 pp와 마스터 키 mk를 생성한다.

-KeyGen$(S, mk) \rightarrow (usk)$: 속성값의 집합 S와 mk를 입력하여 사용자의 비밀키 usk를 생성한다.

-Encrypt$(AS, m) \rightarrow (C)$: 접근권한을 나타내는 속성값의 구조인 AS와 메시지 m을 입력하여 암호문 C를 생성한다.

-Rekey generation$(usk, AS) \rightarrow (rk)$: 사용자의 비밀키 usk와 새로운 사용자의 속성값의 구조 AS를 입력하여 재암호화 키값인 rk를 생성한다.

-Re-encryption$(rk, C) \rightarrow (C')$: 재암호화 키 rk와 암호문 C를 입력하여 재암호화과정을 거쳐 재암호문 C'를 생성한다.

-Decrypt$(usk, AS) \rightarrow (m)$: 속성값의 구조인 AS가 암호문 C를 만족하는지 확인한 뒤 사용자의 비밀키 usk와 C를 입력하여 암호문을 복호화 한다.

Ⅲ. 제안된 스킴

시스템 접근권한에 대한 다양성 제공을 위해 속성기반 암호화를 이용한 Rhee et al.[4]이 제안되었다. 이는 수신자가 특정 속성을 만족하는 경우 송신자는 인증이 가능하다. 그러나 서버로부터 생성되어 전달받은 메시지를 통해 자신만 서버와 인증이 가능하다. 만약 자신의 권한을 이용해서 다른 속성

을 가진 사용자가 서버와의 인증이 가능하도록 허용해주어야 하는 경우 다른 사용자 역시 [표 2], [표 3]의 등록과 로그인 단계를 수행하여야 한다. 하지만 제안된 스킴은 [그림 1]과 같이 Rhee et al. 스킴의 등록, 로그인, 검증단계에 [표 5]의 재암호화 과정과 [표 6]의 복호화 과정을 추가하여 등록과 로그인 단계를 거치지 않고 재암호화 과정을 통해 인증권한 분배가 가능하다.

그림 1. Rhee et al.과 제안된 알고리즘의 관계
Fig. 1. Relation between Rhee et al. and proposed algorithm

재암호화과정에서는 등록단계이후 서버로부터 전달받은 메시지를 재암호화하여 자신의 Proxy server를 통해 배포한다. 재암호문은 특정한 속성을 만족하는 사용자가 서버와 상호인증 시 사용된다. [그림 2]와 [그림 3]는 Rhee et al. 스킴과 제안된 스킴의 인증권한 분배의 차이점을 나타내고 있다. 제안된 스킴에서는 인증서버에 등록되지 않은 사용자 2가 인증서버에 등록된 사용자 1의 Proxy 서버에 저장된 재암호문을 이용하여 인증서버와 상호인증이 가능하다. 하지만 [그림 2]의 Rhee et al.에서는 사용자2는 인증서버에 등록 및 로그인 단계를 수행해서 권한을 얻을 뒤에 가능하다.

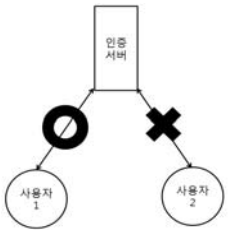

그림 2. Rhee et al.스킴
Fig. 2. Rhee et al. scheme

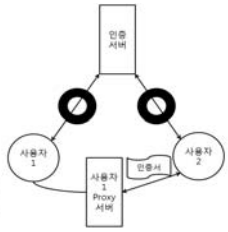

그림 3. 제안된 스킴
Fig. 3. Proposed scheme

1. 속성기반 재암호화 인증 스킴의 특성 제안된 스킴에서 제공하는 특성은 다음과 같다.

-등록된 사용자와 서버간의 상호인증 : 사용자는 자신의 ID와 password값을 이용하여 인증 메시지를 생성하며 서버쪽에서는 서버의 비밀키를 이용한 인증을 수행한다. 따라서 상호간의 안전한 인증이 가능하다.

-사용자 익명성 : 서버는 사용자로부터 전달받은 메시지를 속성값을 이용하여 검증하게 된다. 따라서 송신자의 ID, password에 대한 정보 없이 메시지 인증이 가능하다.

-인증의 다양성 : 속성기반 암호화를 통한 인증을 통해 사용자의 신원에 대한 정보 외에도 직위나 부서와 같은 속성에 따라 차별화된 접근권한을 줄 수 있다. 이처럼 속성을 통한 인증 시스템은 분산시스템 환경에 응용 가능하다.

-인증권한 부여기능 : 서버로부터 인증을 받은 사용자 1은 서버에 등록되지 않은 사용자 2에게 자신이 서버로부터 전달받은 인증 메시지를 재암호화하여 제공함으로써 서버에 대한 인증을 사용자 2가 가능하도록 인증권한을 부여할 수 있다.

2. 제안된 스킴의 구성

속성기반 재암호화 인증 스킴은 Rhee et al.스킴의 장점에 재암호화 과정을 추가하여 새로운 기능이 가능하도록 설계되었다. 스킴은 등록, 로그인, 검증 그리고 재암호화, 재암호화 검증 단계로 구성된다. 등록 단계는 사용자가 스마트카드를 서버에 등록하는 과정으로써 자신의 ID와 password를 서버에 전송하며 최초에 한번만 수행된다. 로그인단계에서는 사용자가 가진 속성 중 원하는 서비스에 맞추어 속성을 정의하여 서버에 알려준다. 검증 단계는 사용자의 메시지 복호화 과정을 통해 사용자가 보내온 속성값에 따른 인증을 해주게 된다. 재암호화 과정은 로그인 단계 이후에 수행된다. 로그인과정을 수행한 사용자1은 등록되지 않은 사용자2에게 서버에 대한 접근 권한을 부여하기 위해 자신의 Proxy 서버에 암호문을 재암호화하여 제공한다. 재암호문은 사용자2의 특정한 속성값에 따라 암호화된다. 검증단계에서는 재암호화된 값을 복호화하여 사용자1의 권한을 확인함과 동시에 사용자2의 특정한 속성값에 의해 수정된 재암호문을 검증하여 만족하는 경우 사용자 인증이 이루어진다.

2.1 재암호화 단계

[Step 1]에서는 인증서버와 로그인과정을 거친 사용자1이 등록되지 않은 사용자2에게 인증권한을 부여하기 위해 자신의 Proxy 서버에 암호문 C'를 전송한다. [Step 2]에서는 사용자2의 특정한 속성값 a_{a,j_f}을 사용하여 재암호화 키값 P를 생성한다. P

값은 서버의 비밀키값과 XOR연산을 통해 생성한다. [Step 3]에서는 생성된 재암호화 메시지를 사용자2에게 안전한 회선을 통해 전송하게 된다. 이때 재암호화 키값과 속성값의 집합을 C'과 합쳐서 보내준다. [Step 4]에서는 사용자2가 가진 속성값을 통해 Q값을 계산한다. [Step 5]에서는 Q값을 통해 W를 계산한다. W값을 통해 [Step 6]에서는 $C_2' = (rr_p) \oplus W$ 를 계산한다. [Step 7]에서는 새로운 타임 스탬프값 T'과 임의의 값 r_p를 생성하고 두 개의 값을 곱한 결과값을 C_1에 승수 연산을 하여 재암호화 메시지를 생성한 후 인증 서버에게 전송한다. 재암호문을 전송받은 인증서버는 사용자 2에 대한 검증과정 없이도 사용자2가 올바른 속성값을 가지고 있음을 확인할 수 있다. 그 이유는 사용자 2가 올바른 속성값을 가지고 있지 않으면 [Step 5]에서 W 값을 계산할 수 없으므로 재암호문 C_2'를 생성할 수 없기 때문이다.

표 5. 재암호화 단계
Table 5. Re-encryption phase

1 $U_i => S_{U_i}$: $C' = [(a_{i,j_1}, a_{i,j_2}, \dots, a_{i,j_k}), C_1, C_2, C_3, T, W]$을 전송한다.
2 S_{U_i} : $P = \prod_{f}^{d} h(a_{a,j_f}) \oplus W$ 를 계산한다. a_{a,j_f}는 특정한 재암호화에 사용되는 속성값으로써 범위는 $1 \leq f \leq d \leq n$이며 $a_{a,j_f} \in A_a, (A_a \subseteq G)$조건을 만족한다. n은 속성값의 전체개수이다.
3 $S_{U_i} => U_a$: $C'' = [A_a, P, (a_{i,j_1}, \dots, a_{i,j_k}), C_1, C_2, C_3, T]$를 전송한다.
4 U_a : 자신의 속성값을 이용하여 $Q = \prod_{f}^{d} h(a_{a,j_f})$을 계산한다.
5 U_a : $W = Q \oplus P$를 계산한다.
6 U_a : $C_2' = ((C_2 \oplus W) r_p) \oplus W$를 계산한다. $r_p \in G^*$는 임의의 수이다.
7 U_a : 암호문을 재암호화 하여 $C_1' = (C_1)^{r_p T'}$를 계산한다. 타임스탬프 T'는 현재 시간을 저장한다. $r_p T'$ 승수연산은 T'와 r_p를 곱한 다음 승수연산을 한다.
8 $U_a \rightarrow S$: 재암호화된 재암호문 $C''' = [(a_{i,j_1}, \dots, a_{i,j_k}), , C_1', C_2', C_3, T, T']$를 인증서버로 전송한다.

2.2 검증 단계(재암호화)

검증 단계에서는 먼저 암호문의 구성요소를 확인하여 재암호화가 안된 기존 암호문인 경우 Rhee et al.의 검증 단계를 수행한다. 만약 재암호화 과정이 수행된 재암호문인 경우 [표 6]의 검증단계를 따라 인증을 수행하게 된다. [Step 1]에서는 전송된 메시지의 타임스탬프를 확인하여 허용시간 안에 도착했는지 확인한다. [Step 2]에서는 등록된 사용자의 속성값과 서버의 비밀키값을 통해 Z값과 r''를 생성한다. 이는 등록된 사용자의 인증권한을 증명한다. [Step 3]에서는 C_1'을 계산하여 전송되어온 메시지와 동일한지 확인한다. [Step 4]에서는 사용자에게 서버인증과 세션키 교환을 수행하기 위해 Z''와 g^e값을 전송한다. 이를 전송받은 등록되지 않은 사용자는 Z''값에 T'값을 승수 연산을 하여 C_1'과 동일한지 확인한다. 해당 단계의 인증이 안전한 이유는 Integer factorization문제로써 Z''값을 계산하는 것이 불가능하기 때문이다. g^e값은 상호간의 인증이 끝난 후 r승수연산을 수행하면 Diffie-Hellman기법을 통해 서버와 사용자간에는 동일한 세션키를 가지게 된다.

표 6. 검증 단계(재암호화)
Table 6. Verification phase(Re-encryption)

1 S : T'가 $\triangle T$ 를 만족하는지 확인한다.
2 S : $r'' = C_2' \oplus h(x_s)$와 $Z = \prod_{j_t}^{k} h(a_{i,j_t} \oplus x_s)$를 계산한다.
3 S : $(Z \| T)^{r'' T'}$를 계산하여 C_1'와 동일한 경우 다음 단계를 진행한다.
4 S : $C_4 = (Z \| T)^{r''}$와 $C_5 = g^e$를 계산한다. 임의의 수 $e \in G^*$를 만족한다.
5: $S \rightarrow U_a$: $B = [C_4, C_5]$를 전송한다.
6: U_a : $C_4^{T'}$를 계산하여 C_1'와 동일한 경우 서버에 대한 인증이 되며 세션키 $C_5'' = g^{re}$를 공유하게 된다.

Ⅳ. 분 석

1. 안전성 분석

로그인과 인증단계는 Rhee et al.스킴의 안전성과 동일하다. 따라서 안전성에 대한 분석은 추가된 재암호화단계와 재암호화검증단계에 대해서만 다룬다. 스킴의 재암호화 단계는 가장 공격, 재사용공격, 오프라인 패스워드 공격, 그리고 재사용 공격에 안

전하다. 단 스마트카드의 temper resistant한 성질을 이용한 안전성은 고려하지 않는다.

-은밀한 검증자 공격 : 전송되어지는 메시지는 연산을 통해 암호화된 값이므로 공격자는 메시지와 서버로부터 인증정보를 얻는 것이 불가능하다.

-사용자 가장 공격 : 공격자는 정당한 인증메시지에 사용된 C_1', C_2'를 생성하는 것이 불가능하다. 그 이유는 서버의 비밀키값 x_s와 임의의 값 r, r_p 그리고 사용자의 속성값을 알 수 없기 때문이다.

-서버 가장 공격 : 공격자는 자신이 서버임을 증명하기 위해 C_4를 생성할 수 있어야 한다. 하지만 서버의 비밀키값 x_s와 임의의 값 r, r_p를 알 수 없으므로 불가능하다.

-재사용 공격 : 타임 스탬프를 이용하여 제한된 시간 안에 도착하지 못한 메시지는 유효하지 않으므로 재사용 공격으로부터 안전하다.

-오프라인 패스워드 공격 : 재암호화 단계에서는 새로운 사용자의 password정보가 사용되지 않는다. 또한 등록단계에서는 안전한 회선으로 ID와 password가 전달되므로 공격자는 재암호화 메시지로부터 사용자의 패스워드 정보를 얻는 것이 불가능하다.

-사용자의 익명성 : 재암호화 단계에 사용되는 값들은 전부 사용자의 속성값에 기반하였기 때문에 속성값을 통해 사용자가 누구인지 확인하는 것은 불가능하다.

2. 연산량 및 정보보호 기능 분석

제안된 스킴은 Rhee et al.스킴을 기반으로 하였기 때문에 기존의 연산량에 재암호화 과정에 따른 연산량만 추가되었다. 재암호화 과정에는 해쉬연산 두번, 지수연산을 한번 수행하여 암호문을 재암호문으로 변환하며 인증과정에서는 기존의 인증과정과 동일한 연산량으로 재암호문을 인증한다. 이는 인증과정에서 사용되는 승수연산 수행시 두 번의 승수연산 되신 곱셈후 승수연산을 수행함으로써 보다 효율적인 연산이 가능하게 한다. 또한 제안된 스킴은 Chien et al.스킴에서 사용되는 대칭키 암 · 복호화를 수행하지 않으므로 연산속도가 빠르다. 또한 Yoon et al.의 스킴보다 적은 해시연산을 통해 구현되므로 효율적이다.

표 7. 스킴의 계산량 비교
Table 7. Comparison of complexity of scheme

프로토콜	계산량			
	로그인	인증	재암호화	총계
Our scheme	2H+1E	2H+3E	· 2H+1E	4H+4E 6H+5E
Rhee et al. scheme[4]	2H+1E	2H+3E	·	4H+4E
Das et al. scheme[6]	5H	3H	·	8H
Yoon et al. scheme[7]	5H+1E	4H+3E	·	9H+4E
Chien et al. scheme[1]	1H+1E+1S	3H+2E+2S	·	4H+3E+3S
H : 해시함수, E : 지수 연산, S : 대칭키 연산				

표 8. 스킴의 정보보호 기능비교
Table 8. Comparison of security feature of scheme

프로토콜	사용자 익명성	세션키 교환	속성기반인증	인증권한부여
Our scheme	Yes	Yes	Yes	Yes
Rhee et al. scheme[4]	Yes	Yes	Yes	No
Das et al. scheme[6]	No	No	No	No
Yoon et al. scheme[7]	Yes	No	No	No
Chien et al. scheme[1]	No	Yes	No	No

Ⅴ. 결 론

본 논문에서 제안된 스킴은 인증서버에 ID와 password를 등록한 사용자가 자신의 속성값를 사용하여 서버에 로그인한다. 만약 인증권한 분배가 필요한 경우 로그인메시지는 다른 사용자의 속성으로 재암호화되어 Proxy서버에 저장된다. 이때 서버와의 인증이 필요하지만 서버에 등록되지 않은 사용자는 특정한 속성을 만족하는 경우 등록된 사용자의 권한을 이용하여 익명성을 보장받으며 인증을 받는 것이 가능하다. 또한 기존의 속성기반 재암호화기법은 타원곡선 기반으로 구현되어 스마트카드 상에서 부적합했던 기법을 지수, 해시 연산을 통해 제안함으로써 해당 연산이 가능한 스마트카드의 적

용에 적합하다. 본 스킴은 속성값에 따른 다양한 서비스 제공이 가능하며, 인증권한부여가 가능하다. 따라서, 회사나 학교와 같이 사용자 상호간에 계층 구조를 가진 단체에서 사용하는 인증시스템에서 활용도가 높다.

참 고 문 헌

[1] H. Y. Chien, C. H. Chen, "A remote authentication scheme preserving user anonymity", IEEE AINA'05, Vol.2, pp. 245-248, 2005.

[2] D. Boneh, M. Franklin, "Identity-based encryption from the weil pairing", CRYPTO, pp. 213-229, 2001.

[3] A. Sahai, B. Waters, "Fuzzy identity-based encryption", Proc. of EUROCRYPT'05, LNCS3494, pp. 457-473, 2005.

[4] 이현숙, 유혜정, "스마트카드를 이용한 속성기반 사용자 인증 스킴", 정보보호학회논문지, 제18권, 제5호, pp. 41-47, 2008.

[5] X. Liang, Z. Cao, H. Lin, Jun Shao, "Attribute based proxy re-encryption with delegating capabilities", ASIACCS 2009, Sydney, Australia, 10-12 March 2009. ACM, pp. 276-286, 2009.

[6] 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.

[7] 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.

저 자 소 개

서 화 정

2010년 : 부산대학교 정보컴퓨터공학과 학사.
현재, 부산대학교 컴퓨터공학부 석사.
관심분야 : 임베디드 하드웨어, Real-time OS.
Email : hwajeong@pusan.ac.kr

김 호 원

1993년 : 경북대학교 전자공학과 학사.
1995년 : 포항공과대학교 전자전기공학과 공학석사.
1999년 : 포항공과대학교 전자전기공학과 공학박사.
1998~2008년 : 한국전자통신연구원(ETRI) 정보보호연구단 선임연구원/팀장.
현재, 부산대학교 정보컴퓨터공학부 조교수.
관심분야 : 스마트그리드 보안, VLSI 설계, RFID/USN 정보보호기술, PKC 암호, Embedded system 보안.
Email : howonkim@pusan.ac.kr