스마트카드와 지문을 이용한 강화된 ID기반의 인증 기법

전 일 수[†] · 김 현 성[††]

요 약

최근에 KIM03[9]은 지문과 스마트카드를 이용한 ID기반의 인증 기법을 제안하였다. 하지만 Scott[10]은 KIM03의 인증 기법이 소극적 공격(Passive attack)에 취약함을 보였다. 본 논문에서는 KIM03의 인증 기법에 존재하는 문제점을 해결할 수 있는 강화된 ID기반의 인증 기법을 제안한다. 특히, 본 논문에서 제안한 기법은 기존의 ID기반의 암호화 시스템이 공유하는 문제점인 ID 복구문제(Repairability)를 해결한다. 본 논문에서 제안한 ID기반의 인증 프로토콜은 ID기반의 암호화 시스템의 장점을 유지하면서 이 방식의 문제점들을 효율적으로 해결한다.

키워드 : 인증기법, 스마트카드, 지문, ID 복구문제

Enhanced ID-based Authentication Scheme using Smartcards and Fingerprints

Il-Soo Jeon[†] · Hyun-Sung Kim[††]

ABSTRACT

Recently, Kim et al. proposed ID-based authentication schemes using smartcards and fingerprints. However, Scott showed that they were vulnerable to the passive eavesdropping attack. Thereby, this paper proposes an enhanced ID-based authentication scheme to solve the problems in Kim et al. scheme. Especially, the proposed scheme solves the ID repairability problem commonly shared in the previous ID-based cryptosystems. The proposed ID-based authentication scheme supports the advantages in the previous ID-based cryptosystems and solves the problems in them effectively.

Key Words : Authentication Scheme, Smartcard, Fingerprint, ID Repairability

1. 서 론

Diffie와 Hellman[1]이 1976년 공개키 분배 프로토콜을 제안한 이래로 많은 공개키 암호시스템들이 제안되었다. 이 프로토콜은 유한 필드 상에서 이산대수 문제의 어려움을 이용하여 참여자들 간에 세션키를 공유한다. 하지만 이 프로토콜은 참여자들을 인증하는 방법을 제공하지 못하기 때문에 중간 침입자 공격(man-in-the-middle attack)에 대하여 안전하지 못하였다. 이러한 인증에 관한 문제는 다양한 방법으로 해결이 가능하며 그 중 한 가지 방법이 ID기반의 인증 프로토콜이다.

1984년 Shamir[2]에 의해 ID(Identification)정보에 기반한 서명기술이 제안된 이후 ID정보에 기반한 많은 연구가 진행되었다. Shamir의 방식에서는 가입자의 ID정보를 공개키로 이용하고 비밀키 자체가 공개키에 대한 증명으로 이용된다. 그러므로 ID기반의 암호화시스템은 식별자와 비밀키의 쌍(식별자, 비밀키)으로 구성된다. 이 암호화 시스템은 저장하거나, 검증할 공개키 증명이 별도로 필요 없기 때문에 다른 공개키 암호화 시스템에 비해서 매우 효율적인 시스템이다. Okamoto[3]는 Diffie-Hellman의 키 분배 프로토콜에 ID정보를 이용한 인증을 첨가한 기법을 제안하였다. 이 기법은 키 교환을 위한 낮은 통신의 복잡도를 제시하였으나 높은 대역폭 사용과 많은 계산량으로 인한 부하, 그리고 위장공격에 취약한 문제점을 안고 있다. Shieh 등[4]은 적은 계산량과 Okamoto 방식에서 나타나는 안전성 문제를 해결한 인증 프로토콜을 제안하였다. 그러나 Yen[5]에 의해서 이 기법이 메시지 재전송 공격과 알려지지 않은 키 공유 공격(Unknown key share attack)에 취약하다는 분석이 제시되었다. 이들 프로토콜은 RSA 공개키 암호 시스템과 같이 두 개의 큰 소수의 곱인 합성수의 인수분해 문제에 기반한다.

한편 Tsujii[6]는 이산대수문제의 안전성에 기반한 ElGamal 공개키 암호시스템을 이용하여 ID기반의 암호 시스템을 제안하였으나 이 시스템은 많은 계산량이 요구될 뿐만 아니라 공모 문제와 같은 보안의 취약성을 갖고 있었다. Wang등[7]과

※ 본 연구는 금오공과대학교 학술연구비에 의하여 연구된 논문
† 정 회 원 : 금오공과대학교 전자공학부
†† 정 회 원 : 경일대학교 컴퓨터공학부
논문접수 : 2005년 8월 26일, 심사완료 : 2005년 10월 11일

Yang등[8]은 스마트카드를 이용한 ID기반의 인증 프로토콜을 제안하였다. 이들 프로토콜에서는 재전송 공격에 대응하기 위하여 시스템의 타임스탬프를 사용하였지만 여전히 재전송공격에 취약했고, 사용자의 ID정보 또한 위조될 수 있었다. 최근에 KIM03[9]은 스마트카드와 지문을 이용한 ID기반의 두 가지 프로토콜(KLY 인증기법)을 제안하였다. 하지만 Scott [10]은 KIM03의 인증 기법이 소극적 공격(Passive attack)에 취약함을 보였다.

본 논문에서는 ID방식에 기반한 암호화 시스템의 장점을 유지하면서 이 방식의 문제점들을 해결할 수 있는 스마트카드와 지문을 이용한 강화된 ID기반의 인증 기법을 제안한다. 본 논문에서 제안한 기법은 기존의 ID기반의 암호화 시스템이 공유하는 문제점인 ID 복구문제(Repairability)를 해결한다. 인증을 위한 처리에 필요한 모든 정보는 외부로부터 보호하기 위해서 스마트카드에 저장하고 모든 연산은 스마트카드 내부에서 이루어진다. 또한, 스마트카드의 소유자 인증과 난수 생성을 위하여 지문을 이용한다. 제안한 인증기법은 관련된 프로토콜에 비해 보다 높은 안전성과 효율성을 제공할 수 있을 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 KIM03이 제안한 ID기반의 인증기법과 Scott의 공격에 대해서 기술한다. 3장에서는 기존의 ID기반의 인증기법에서 공유하는 문제점을 해결할 수 있는 스마트카드와 지문을 이용한 강화된 ID기반의 인증기법을 제안하고 4장에서는 제안된 프로토콜들에 대한 암호학적 안전성 분석을 제시한다. 마지막으로 5장에서는 결론을 맺는다.

2. 관련 연구

본 장에서는 최근에 KIM03[9]이 제안한 스마트카드와 지문을 이용한 ID기반의 인증기법(KLY 인증기법)과 이 기법에 대한 Scott[10]의 공격기법에 대해서 살펴본다.

2.1 KLY 인증기법

Kim03은 타임스탬프(Timestamp-based)와 랜덤값(Nounce-based)을 이용한 ID기반의 인증 기법(KLY 인증기법)을 각각 제안하였다. 본 논문에서는 랜덤값을 이용한 ID기반의 인증기법에 대해서 자세히 살펴본다. KLY 인증기법은 등록단계와 로그인단계, 그리고 검증단계의 3단계로 구성된다. KLY 인증기법의 각 단계는 다음과 같다.

[등록단계] 원격서버가 클라이언트에게 스마트카드를 발급하고, 스마트카드를 발급받은 사용자는 자신의 지문정보를 스마트카드에 등록한다.

Step 1. 클라이언트 A는 자신의 아이디 ID_i와 패스워드 PW_i를 원격서버 B에게 안전한 방법으로 전송한다.

Step 2. 원격서버 B는 클라이언트 A의 스마트카드 아이디인 CID_i를 생성하고 S_i와 h_i를 다음과 같이 계산한다. 여기서 CID_i는 사용자의 ID_i를 기반으로 유도한다.

$$S_i = ID_i^{SK}$$

$$h_i = g^{PW_i \cdot SK}$$

여기서 SK는 서버의 비밀키이고, CID_i는 검증 단계에서 스마트카드의 유효성 검증을 위해서 사용될 스마트카드의 아이디이다.

Step 3. 원격서버 B는 스마트카드의 메모리에 n, g, $f()$, ID_i, CID_i, S_i, 그리고 h_i를 저장하고 그 카드를 클라이언트 A에게 발급한다.

Step 4. 클라이언트 A는 발급받은 스마트카드에 자신의 지문 정보를 등록한다. 지문을 등록할 때는 입력된 지문정보로부터 특징점을 추출하여 추출된 특징점 정보를 저장하며, 이러한 정보는 스마트카드의 소유자 인증에 사용된다.

등록단계는 원격 서버에 새로운 가입자가 생기거나 가입자가 자신의 패스워드를 바꾸고자 하는 경우에만 수행된다.

[로그인단계] 로그인을 위해서 클라이언트 A는 카드리더기에 자신의 스마트카드를 입력하고 스마트카드 소유자 인증을 위해서 자신의 지문을 지문입력기에 입력하고, 원격서버의 로그인에 필요한 정보인 ID_i와 패스워드 PW_i를 입력한다. 지문을 통한 사용자 인증이 성공할 경우에만 스마트카드는 다음과 같은 로그인 절차를 수행한다.

Step 1. 스마트카드가 초기 로그인 메시지 $M_1 = \{ID_i, CID_i\}$을 원격서버 B에게 보낸다.

Step 2. 원격서버는 ID_i와 CID_i의 유효성을 검사한다. 만약 유효성 검사가 성공하면 원격서버는 난수 r_s를 생성하고 다음 수식을 이용하여 N을 계산한 후 클라이언트에게 보낸다.

$$N = f(CID_i, r_s)$$

Step 3. 스마트카드는 받은 N이 재사용된 랜덤 값이 아니라면, 입력된 지문 좌표계의 해쉬된 정보를 이용하여 난수 r_i를 생성하고 다음을 계산하여 $M_2 = \{X_i, Y_i\}$ 을 원격서버에 보낸다.

$$X_i = g^{r_i \cdot PW_i} \bmod n$$

$$Y_i = S_i \cdot h_i^{r_i \cdot N} \bmod n$$

[검증단계] 서버는 클라이언트 A로부터 받은 메시지의 검증을 통하여 A가 정당한 사용자인지를 결정한다. 이러한 검증을 위하여 서버는 다음의 절차를 수행한다.

Step 1. 원격서버는 다음 수식이 맞는지 체크한다.

$$Y_i^{SK^{-1}} \equiv ID_i \cdot X_i^N \bmod n$$

이 수식은 클라이언트에 의해 입력된 패스워드 PW_i가 서버에 의해 발급된 스마트카드에 등록된

패스워드와 일치하고 클라이언트가 정확한 S_i를 알고 있을 때만 성립한다. 이 수식이 성립할 때만 서버가 클라이언트의 접근을 허락한다.

2.2 Scott의 공격기법

Scott[10]은 KLY 인증기법이 패스워드나 지문정보와 스마트카드에 대한 접근 없이도 소극적공격(Passive attack)이 가능함을 보였다. 이 공격방법은 KLY 인증기법의 검증단계에 초점을 맞췄다. 검증단계 Step1에서 $Y_i^{SK^{-1}} \equiv ID_i \cdot X_i^N \bmod n$을 다음과 같이 유도할 수 있다.

$$Y_i = (ID_i \cdot X_i^N)^{SK} \bmod n$$

위의 식에서 공격자는 SK를 모르지만 적법한 사용자 U_j를 가장하기 위하여 다음 식을 계산 할 수 있다.

$$G = ID_j \cdot X_j^N \bmod n$$

위의 식으로부터 공격자는 다음 식을 만족하는 SK를 찾을 수 있다.

$$G^{SK} = Y_j \bmod n$$

즉, KLY 인증기법에서 $\{G, G^{SK}\}$를 아는 것은 SK를 아는 것만큼 공격자에게 좋은 정보가 된다. 사용자 U_i를 가장한 로그인을 위해서 공격자는 $\{ID_i, CID_i\}$에 관련된 도청된 값을 전송함으로서 로그인단계를 시작한다. 서버가 랜덤 값 N을 전송할 때 공격자는 다음 값을 전송한다.

$$X_i = G/ID_i^{N^{-1}} \bmod n$$
$$Y_i = (G^{SK})^N \bmod n$$

위의 수식에서 생성된 $\{X_i, Y_i\}$ 쌍은 KLY 인증기법의 검증단계를 성공적으로 통과한다.

3. 강화된 ID기반의 인증기법

본 장에서는 KLY 인증기법의 문제를 해결하고 기존의 ID기반의 인증기법에서 공유하는 문제점을 해결할 수 있는 스마트카드와 지문을 이용한 강화된 ID기반의 인증기법을 제안한다.

3.1 표기 및 초기설정

본 절에서는 제안된 인증기법에서 사용될 용어와 표기법, 그리고 가정들을 정의한다.

인증기법을 위한 가정은 다음과 같다. 클라이언트(A)와 서버(B)는 합법적인 참여자들이다. A와 B는 안전하게 Z_n^* 상의 생성자인 g와 큰 소수인 n를 미리 공유하고 있다. 또한 A는 패스워드 PW_i를 소유하고 있다. $f()$는 일방향 해쉬 함수(one-way hash function)이다. 표현의 간편함을 위해 프로토콜 수행에 있어서 'mod n' 연산은 생략한다. 스마트카드의 소유자 인증을 위한 지문 알고리즘은 KLY 인증기법에서와 같은 알고리즘을 사용한다.

A, B	각각 클라이언트와 서버의 식별자
ID_i	클라이언트 i의 아이디
EID_i	클라이언트 i의 확장된 아이디
CID_i	스마트카드의 식별자
g	곱셈군(multiplicative group) Z_n^*의 생성자(generator)
n	큰 소수
PW_i	클라이언트에 의해 선택된 패스워드
SK	서버의 비밀키
SK^{-1}	Z_n^*상에서 SK의 역수
e	클라이언트의 아이디 확장을 위한 Z_n^*의 임의의 원소
r_s	B에 의하여 생성된 Z_n^*의 임의의 원소
r_i	A에 의하여 생성된 Z_n^*의 임의의 원소 (지문 입력정보를 통하여 생성)
$f()$	일방향 해쉬 함수 (one-way hash function)

(그림 1) 인증기법을 위한 표기

3.2 인증기법의 수행

제안된 인증기법도 KLY 인증기법과 마찬가지로 등록단계와 로그인단계, 그리고 검증단계의 3단계로 구성된다. 인증기법의 각 단계는 다음과 같다.

[등록단계] 원격서버가 클라이언트에게 스마트카드를 발급하고, 스마트카드를 발급받은 사용자는 자신의 지문정보를 스마트카드에 등록한다.

Step 1. 클라이언트 A는 랜덤 값 e를 선택한 후 자신의 아이디 ID_i와 패스워드 PW_i와 함께 e를 원격서버 B에게 안전한 방법으로 전송한다.

Step 2. 원격서버 B는 클라이언트 A의 확장된 아이디인 $EID_i = (ID_i||e)$와 스마트카드 식별자인 $CID_i = f(ID_i||e)$를 생성하고 S_i와 h_i를 다음과 같이 계산한다. 서버는 사용자 U_i를 위하여 e를 저장한다.

$$S_i = EID_i^{SK}$$

$$h_i = g^{PW_i \cdot SK}$$

Step 3. 원격서버 B는 스마트카드의 메모리에 n, g, e, $f()$, ID_i, CID_i, S_i, 그리고 h_i를 저장하고 그 카드를 클라이언트 A에게 발급한다.

Step 4. 클라이언트 A는 발급받은 스마트카드에 자신의

지문 정보를 등록한다. 지문을 등록할 때는 입력된 지문정보로부터 특징점을 추출하여 추출된 특징점 정보를 저장하며, 이러한 정보는 스마트카드의 소유자 인증에 사용된다.

등록단계는 원격 서버에 새로운 가입자가 생기거나, 가입자가 패스워드 변경을 요구할 때, 그리고 가입자가 자신의 비밀정보가 누출되었을 경우 재등록을 위해서만 수행된다.

[로그인단계] 로그인을 위해서 클라이언트 A는 카드리더기에 자신의 스마트카드를 입력하고 스마트카드 소유자 인증을 위해서 자신의 지문을 지문입력기에 입력하고, 원격서버의 로그인에 필요한 정보인 ID_i와 패스워드 PW_i를 입력한다. 지문을 통한 사용자 인증이 성공할 경우에만 스마트카드는 다음과 같은 로그인 절차를 수행한다.

Step 1. 스마트카드가 초기 로그인 메시지 $M_1 = \{ID_i, CID_i\}$을 원격서버 B에게 보낸다.

Step 2. 원격서버는 ID_i와 $CIDi$의 유효성을 검사한다. 만약 유효성 검사가 성공하면 원격서버는 난수 r_s를 생성하고 다음 수식을 이용하여 N을 계산한 후 클라이언트에게 보낸다.

$S_i = (ID_i \| e)^{SK}$

$N = f(CID_i, r_s) \oplus S_i$

Step 3. 스마트카드는 받은 N이 재사용된 랜덤 값이 아니라면 N'을 계산한 후, 입력된 지문 좌표계의 해쉬된 정보를 이용하여 난수 r_i를 생성하고 다음을 계산하여 $M_2 = \{X_i, Y_i\}$ 을 원격서버에 보낸다.

$N' = N \oplus S_i$

$X_i = g^{r_i \cdot PW_i} \oplus S_i$

$Y_i = S_i \cdot h_i^{r_i \cdot N}$

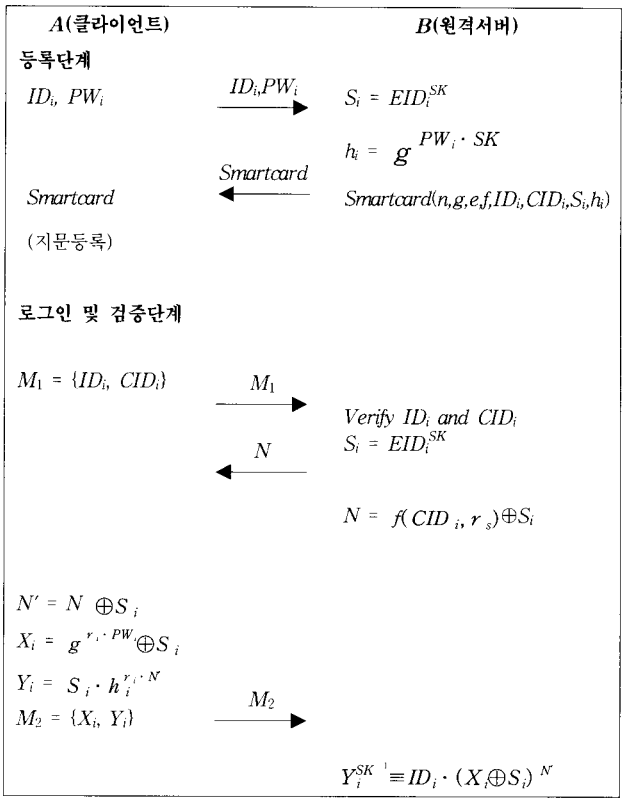
[검증단계] 서버는 클라이언트 A로부터 받은 메시지의 검증을 통하여 A가 정당한 사용자인지를 결정한다. 이러한 검증을 위하여 서버는 다음의 절차를 수행한다.

Step1. 원격서버는 다음 수식이 맞는지 체크한다.

$Y_i^{SK \cdot 1} \equiv ID_i \cdot (X_i \oplus S_i)^N$

이 수식은 클라이언트에 의해 입력된 패스워드 PW_i가 서버에 의해 발급된 스마트카드에 등록된 패스워드와 일치하고 클라이언트가 정확한 S_i를 알고 있을 때만 성립한다. 이 수식이 성립할 때만 서버가 클라이언트의 접근을 허락한다.

본 논문에서 제안한 스마트카드와 지문을 이용한 강화된 ID기반의 인증기법의 전체적인 처리과정은 그림2와 같다. 본 논문에서 제안한 인증기법은 ID 복구문제를 해결하기 위해서 등록단계에서 확장된 아이디인 EID를 사용한다.



(그림 2) 제안한 인증기법

4. 안전성 분석

본 장에서는 본 논문에서 제안한 강화된 ID기반의 인증기법의 암호학적 안전성 분석을 제시한다. 제안한 인증기법은 패스워드 추측공격(Password guessing attack), 메시지 재전송 공격(Message replay attack), 위장공격(Impersonation attack), 그리고 Scott의 소극적공격의 측면에서 안전성을 분석한다.

패스워드 추측공격은 사람이 기억 가능한 작은 크기의 패스워드를 사용하기 때문에 발생한다. 패스워드 추측공격은 크게 온라인과 오프라인 패스워드 추측공격으로 나눌 수 있다. 온라인 패스워드 추측공격은 패스워드 인증 실패 횟수를 계산함으로써 쉽게 탐지되고 조치될 수 있으므로, 본 논문에서는 오프라인 패스워드 추측 공격에 대해서만 고려한다. 공격자는 인증을 위해서 전송되었던 메시지를 가로채어 저장해 두고, 오프라인으로 패스워드를 추측하기 위한 공격을 수행할 수 있다. 본 논문에서 제안한 인증기법에서 패스워드를 획득할 수 있는 유일한 방법은 스마트카드에 저장된 값 $h_i = g^{PW_i \cdot SK}$를 이용하는 방법이다. 그러나 이 방법은 h_i가 안전한 스마트카드에 저장되어 있어서 지문을 통한 소유자 인증 없이는 직접적인 접근이 불가능 하므로 이 공격은 불가능하다. 또한, 공격자가 h_i를 안다고 할지라도 패스워드를 알기 위해서는 유한필드상의 이산대수 문제를 풀어야 하므로 이 공격 역시 불가능하다.

메시지 재전송 공격은 이전 세션의 메시지를 저장하고 다

음 세션들에서 재전송(Replay)하는 방법으로 참여자들이 알지 못한 상태에서 불법적인 사용자가 인증을 시도하기 위한 공격이다. 본 논문에서는 메시지 재전송 공격을 방지하기 위하여 매 세션마다 새로운 랜덤 값과 S_i의 조합 정보를 사용한다. 공격자가 메시지 재전송 공격을 하기 위해서는 이전 세션에서 획득한 N, X_i, Y_i와 현재 세션에서 얻은 N으로부터 검증단계의 식을 만족할 수 있는 새로운 Y_i로 변경할 수 있어야 한다. 그러기 위해서는 정확한 r_i와 S_i를 유추할 수 있어야 하지만 공격자가 이전 세션과 현재 세션에서 얻은 정보로부터 정확한 r_i와 S_i를 유추할 수 있는 방법이 없다.

적법한 사용자나 공격자가 타인을 위장하기 위해서는 위장하고자 하는 사용자의 아이디와 패스워드를 알아야 한다. 사용자의 아이디는 공개된 정보이기 때문에 쉽게 알 수 있지만, 본 논문에서 제안한 인증기법은 사용자의 확장된 아이디인 EID_i를 사용하기 때문에 e값을 모르는 공격자는 확장된 아이디를 확인할 수 있는 방법이 없다. 그리고 사용자의 패스워드는 스마트카드에 저장되어 있고 $h_i = g^{PW_i \cdot SK}$를 안다고 하더라도 원격 서버의 비밀키 SK를 찾는 것 역시 이산대수의 어려움에 근거하고 있다.

마지막으로 Scott의 소극적 공격을 살펴본다. Scott의 공격이 이루어지기 위해서 공격자는 이전 세션의 메시지를 저장하고 다음 세션들을 위해서 이전 세션의 메시지 ID_i, CID_i, N, X_i, Y_i로부터 $\{G, G^{SK}\}$쌍을 유도할 수 있어야 한다. 그러나 공격자가 수식 $Y_i = ID_i \cdot (X_i \oplus S_i)^N$에서 G를 계산하기 위해서는 S_i를 알아야 하지만 S_i를 유추하기 위해서는 e를 알아야 하고, e를 안다고 하더라도 SK를 알기 위해서는 h_i로부터 이산대수의 문제를 풀 수 있어야 한다.

추가적으로, 본 논문에서 제안한 인증기법은 기존의 ID기반의 암호화 시스템에서 공유하고 있는 문제점인 ID 복구문제를 확장된 아이디 EID_i를 사용함으로서 해결하였다. 대부분의 ID기반의 암호화 시스템에서는 ID와 연계된 중요한 정보가 노출되었을 경우, 그 ID를 사용하는 이용자는 자신의 ID를 다른 ID로 바꾸거나 서버의 비밀 값을 바꾸어 전체시스템을 수정 해야만 한다. 그러나 본 논문에서 제안한 인증기법에서는 아이디 확장을 위한 Z_n^*의 랜덤 값 e를 사용함으로서 등록단계 Step 2에 제시된 것처럼 $EID_i = (ID_i \| e)$를 이용하여 효율적으로 ID 복구문제를 해결하였다. <표 1>은 ID기반의 프로토콜들의 특징을 보여준다.

〈표 1〉 ID기반의 프로토콜간의 특성 비교

특성 \ 프로토콜	KIM03[9]	제안한 프로토콜
패스워드 추측공격	S	S
메시지 재전송공격	S	S
위장공격	S	S
Scott의 소극적공격	NS	S
ID복구가능성	NP	P

S : 안전　NS : 안전하지 않음　P : 제공　NP : 제공하지 않음

5. 결 론

본 논문에서는 KLY 인증기법의 문제점을 해결하기 위하여 스마트카드와 지문을 이용한 강화된 ID기반의 인증기법을 제안하였다. 본 논문에서 제안한 인증기법은 기존의 ID기반의 암호화 시스템이 공유하는 문제점인 ID 복구문제(Repairability)를 효율적으로 해결하였다. 프로토콜 수행에 필요한 모든 정보는 외부로부터 보호하기 위해서 스마트카드에 저장하고 모든 연산은 스마트카드 내부에서 이루어진다. 제안한 인증기법은 ID방식에 기반한 암호화 시스템의 장점을 유지하면서 이 방식의 문제점들을 효율적으로 해결할 수 있었다. 제안된 인증기법은 유한필드상의 이산대수 문제의 어려움, 그리고 해쉬함수의 암호학적 강도에 기반하여 패스워드 추측 공격, 메시지 재전송 공격, 위장공격, Scott의 소극적 공격에 안전성을 제공한다.

참 고 문 헌

[1] Diffie W. and Hellman M. E., "New directions in cryptography," *IEEE Trans., IT-22*, No.6, pp.644~654, 1976.

[2] A. Shamir, "Identity-based cryptosystems and signature schemes," *CRYPTO'84*, pp.47~53, 1985.

[3] E. Okamoto and K. Tanaka, "Key distribution system based on identification information," *Proc. GLOBECON'87*, pp.108~111, 1987.

[4] S. P. Shieh, W. H. Yang, and H. M. Sun, "An authentication protocol without trusted third party," *IEEE Commun. Lett.*, Vol.1, pp.87~89, 1997.

[5] S-M. Yen, "Cryptanalysis of an authentication and key distribution protocol," *IEEE Commun. Lett.*, Vol.3, pp.7~8, 1999.

[6] S. Tsujii and K. Kurosawa, "ID-based cryptosystem," *ISEC89-51*, pp.25~31, 1989.

[7] S. J. Wang and J. F. Chang, "Smart card based secure authentication scheme," *Computers and Security*, Vol.15, No.3, pp.231~237, 1996.

[8] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," *Computers and Security*, Vol.18, No.8, pp.727~733, 1999.

[9] H. S. Kim, S. W. Lee, and K. Y. Yoo, "ID-based Password Authentication Scheme using Smart Cards and Fingerprints," *ACM Operating Systems Review*, pp.32~41, 2003.

[10] M. Scott, "Cryptanalysis of an ID-based Password Authentication Scheme using Smart Cards and Fingerprints," *Cryptology ePrint Archive : Report 2004/017*, http://eprint.iacr.org/2004/017, 2004.

전 일 수

e-mail : isjeon@kumoh.ac.kr

1984년 경북대학교 전자공학과(공학사)

1988년 경북대학교 대학원 전자공학과(공학석사)

1995년 경북대학교 대학원 전자공학과(공학박사)

1984년~1985년 삼성전자(주)

1989년~2004년 경일대학교 컴퓨터공학과 교수

2004년~현재 금오공과대학교 전자공학부 조교수

관심분야 : 정보보호, 보안 프로토콜

김 현 성

e-mail : kim@kiu.ac.kr

1996년 경일대학교 컴퓨터공학과(공학사)

1998년 경북대학교 대학원 컴퓨터공학과(공학석사)

2002년 경북대학교 대학원 컴퓨터공학과(공학박사)

2000년~2002년 (주)디토정보기술 선임연구원

2002년~현재 경일대학교 컴퓨터공학부 교수

관심분야 : 정보보호, 보안 프로토콜, 공개키 암호화 시스템 설계