DBpia

논문 14-39B-01-04

한국통신학회논문지(J-KICS) '14-01 Vol.39B No.01
http://dx.doi.org/10.7840/kics.2014.39B.1.29

스마트카드 기반 Tsai et al. 인증기법의 안전성 분석과 새로운 보안기법 연구

김 명 선◆°

Security Analysis and Enhancement of Tsai et al.'s Smart-Card Based Authentication Scheme

Myungsun Kim◆°

요 약

최근, Tsai 등의 연구자는 동적 ID 기반 스마트카드 인증 기법을 제안하였다. 본 논문에서 그들이 제안한 기법은 잘못된 패스워드의 검증을 조기에 탐지하지 못하기 때문에 발생하는 서비스거부 공격과 내부자 공격에 취약하고 패스워드 변경시 안전성이 보장되지 않는 문제가 있음을 제시하고, 이러한 문제를 해결하는 기법을 제시하려고 한다. 본 논문에서 제안하는 기법의 안전성은 일방향 해시 함수의 안전성과 이산대수 문제의 어려움에 기반을 둔다. 특히 기존 기법과 거의 대등한 수준의 연산량을 요구하면서 안전성 문제를 해결한다. 추가로 제안하는 기법의 안전성과 연산량에 대한 좀 더 자세한 분석을 제시한다.

Key Words : Remote authentication, Smartcards, DoS attack, Insider attack, Password

ABSTRACT

In this paper we show that a dynamic ID authentication scheme using smart cards proposed by Tsai et al. is not secure against DoS attack and insider attack. Further we claim that their scheme may raise a security problem when a user changes his/her password. Then we come up with a security-enhanced version only with small additional computational cost. Our scheme is based on the security of cryptographic hash function and the infeasibility assumption of discrete logarithm problem. In addition, we provide details of security and computational cost analysis.

Ⅰ. 서 론

인터넷과 같은 공개된 네트워크를 통하여 비밀 정보의 송수신이 이루어지는 IT 시스템뿐만 아니라, 가입자에 대한 관리가 별도로 필요한 IP-TV 등의 서비스는 다양한 보안 요구사항을 만족해야 한다.

예를 들면 Citrix는 인터넷이나 개방 네트워크를 통해서 공유된 어플리케이션 서비스를 제공한다[4]. 특히 ISDN이나 DSL 네트워크을 통하여 다수의 사용자가 동시에 공유된 어플리케이션을 수행할 수 있도록 지원한다. 이러한 응용에서 민감한 정보에 접근하려는 사용자의 신원 (IDentity)을 확인하는 인증 기능은 필수적이다. 인증 (Authentication)이란 메시지의 출처를 확인하고 그 출처가 위조된 것이 아님을 보장하는 서비스이다. 패스워드 기반의 인증 기법이 갖는 문제점을 피하기 위해 스마트카드 기반의 인증 기법들을 사용하는데, 연산의 효율성과 사용의 편리성 때문에 여러 분야에서 적극적으로 활용되고 있다. 통상 스마트

◆° First Author and Corresponding Author : 수원대학교 IT대학 정보보호학과, msunkim@suwon.ac.kr, 정회원
논문번호 : KICS2013-10-469, 접수일자 : 2013년 10월 29일, 심사일자 : 2014년 1월 6일, 최종논문접수일자 : 2014년 1월 15일

www.dbpia.co.kr

카드는 변조방지 기능을 갖는 IC (Integrated Circuit) 카드로서 개인정보를 저장할 수 있는 메모리와 산술 연산을 수행할 수 있는 프로세서로 구성된다.

스마트카드를 이용하는 인증기법은 일반적으로 네 개의 단계로 구성된다: 먼저 설정 (Setup) 단계, 둘째 등록 (Registration) 단계, 셋째 로그인 (Login) 단계, 끝으로 검증 (Verification) 단계. 설정 단계에서 서버와 사용자들이 사용할 시스템 매개변수 (System Parameter)들이 결정되고, 등록 단계에서 서버에 등록하기를 원하는 새로운 사용자가 서버에 자신의 신원을 증명할 수 있는 credential을 제시한다. 등록 요청을 수신한 서버는 비밀키 (Secret Key)와 credential의 내용을 기반으로 필요한 정보를 생성하여 스마트카드의 메모리에 저장하여 사용자에게 발급한다. 이후 그 사용자는 서버가 제공하는 자원에 접근하기 원하는 경우 로그인 요청을 보내면 서버가 로그인 요청을 확인하고 정당한 사용자인지 검증한다.

1.1 본 논문의 기여점

최근에 Tsai 등의 연구자들이 스마트카드를 이용하여 동적 ID 인증 기법을 제안하였다[17]. 추가로 그들은, 그들이 제안한 기법이 여러 가지 공격에 대하여 안전하다는 것을 보였다. 본 논문에서는 스마트카드 메모리의 영역에 접근할 수 없다는 가정 하에, 그들이 제안한 기법이 여러 가지 공격에 취약하다는 것을 보인다. 좀 더 구체적으로 그들이 제안한 기법은 조기에 잘못된 패스워드를 탐지하지 못하고 이 결과로 서비스거부 공격에 취약하다. 둘째, 안전한 패스워드 변경을 지원하지 못한다. 끝으로, 내부자 공격에 안전하지 않다. 본 논문에서는 이러한 안전성 문제를 해결하기 위하여 Tsai 등의 기법을 수정하여 상기 공격에도 안전한 스마트카드 기반의 인증기법을 제안한다. 본 논문에서 제안하는 기법은 기존 기법의 안전성 요구사항을 모두 만족하는 동시에 성능 측면에서 거의 대등한 연산량만을 요구한다. 추가로 네트워크 단위의 동기화가 어려운 경우에 대비하여 nonce를 이용하여 인증할 수 있는 방법을 제시한다.

1.2 논문의 구성

본 논문은 다음과 같이 구성된다. 우선 2장에서는 기존 스마트카드 기반의 인증 기법들을 개략적으로 살펴본다. 이어서 3장에서는 Tsai 등이 제안한 기법의 안전성 문제를 분석하고, 4장에서 본 연구진이 제안하는 기법을 설명한다. 5장에서는 제안한 기법의 안전성과 연산 복잡도 분석을 기술한다. 6장에서 제안하는 기법을 최종 정리하고 마무리 한다.

Ⅱ. 사전연구

현재까지 다양한 스마트카드 기반의 인증기법이 제안되었다. 예를 들면 [23,8,16,3,9,22,14,21,19,5,12,18,11,17]을 들 수 있다. 좀 더 구체적으로 살펴보면, [23]에서 Yang과 Shieh는 RSA 암호기법[15]을 이용하여 검증테이블 (Verification Table)을 사용하지 않는 ID 기반 스마트카드 인증기법을 제시하였고, 재생 공격 (Replay Attack)에 안전하다는 것을 보였다. 그러나 그들의 기법은 위장 공격 (Impersonation Attack)에 취약하다는 것이 [2]에서 증명되었다. El Gamal 암호기법 [7]을 이용한 원격 사용자 인증기법이 [8]에서 연구되었으나, 그들의 기법 역시 위장 공격에 취약하다는 것이 [1]에서 밝혀졌다. 그후 효율성을 개선하기 위한 여러 연구 결과들이 제안되었는데, 먼저 Sun은 일방향 해시함수를 이용한 원격 사용자 인증기법을 제안하였다[16]. 그러나 이 기법은 사용자가 패스워드를 선택하고 변경하는 것이 불가능하고 상호인증 기능이 빠져있다. 더구나 패스워드 추측 공격(Password Guessing Attack)에 취약하다. 이러한 문제를 해결하기 위해 Chien 등이 새로운 기법을 제안했으나[3], 이들의 기법은 병렬세션 공격 (Parallel Session Attack)에 취약하다[10].

Hwang 등의 연구자가 기존 기법과 달리, 검증테이블을 사용하지 않으면서도 패스워드를 자유롭게 변경할 수 있을 뿐만 아니라 재생 공격에 안전한 원격 사용자 인증기법을 제안하였으나[9], 상호인증 기능을 제공하지 못하며 서비스거부 공격 (Denial-of-Service Attack)에 취약함이 밝혀졌다[22]. 그 후 [3] 기법을 개선하여 내부자 공격과 반사 공격 (Reflection Attack)에 안전한 기법이 [14]에서 제안되었다. 그러나 이 기법은 병렬세션 공격에 취약하고 패스워드 변경이 안전하지 않음이 [21]에서 증명하였고 개선된 기법을 제안하였다. 다시 이들의 기법은 패스워드 추측 공격, 서비스거부 공격 및 위장 공격에 취약함이 [19]에서 밝혀졌다. Yoon 등의 연구자는, [19]에서 제안하여 개선된 기법도 패스워드 추측 공격, Denning-Sacco 공격에 취약함을 증명하였다[20].

동적 ID 기반 원격 사용자 인증 기법은 Das 등의 연구자에 의해 제안되었는데 그들은 일방향 해시 함수를 사용하였다[5]. 이들이 제안한 기법은 재생 공격, 위장 공격, 패스워드 추측 공격, 내부자 공격과 훔친 검증자 공격 (Stolen Verifier Attack)에 안전한 것으

www.dbpia.co.kr

로 제시되었으나, [12,18]에 의해 패스워드 추측 공격과 내부자 공격에 취약하다는 것이 밝혀졌다. 이 기법 역시 상호인증 기능을 제공하지 못한다. Wang 등이 이러한 단점을 개선하는 기법을 제안하였으나, 오히려 패스워드 추측 공격과 서버 위장 공격 (Server Masquerade Attack)에 취약하다는 것이 증명되었다[11]. 이것을 개선한 새로운 기법을 [11]에서 제시하였으나, 이것 역시 동일한 공격에 안전하지 않다는 것이 증명되었다[24]. Tsai 등이 동적 ID 인증기법을 제안하였는데 위에서 언급된 여러 공격에 안전하고 사용자에게 편리하다는 그들의 주장과 달리 위장 공격, 패스워드 추측 공격에 취약하고 동기화 문제가 여전히 해결되지 않고 있음을 본 연구에서 보이고자 한다.

Ⅲ. Tsai et al. 기법 분석

본 장에서는 Tsai 등이 제안한 동적 ID 인증기법을 개략적으로 살펴보고, 그들이 제안한 기법의 안전성 취약점을 설명하려고 한다.

3.1 표기법

표현의 통일과 편리함을 위해 우선 본 논문에서 계속 사용할 표기법을 제시한다.

서버는 S로 표기하고, U_i로 표기되는 임의의 사용자는 자신의 ID와 패스워드 쌍으로 (α_i, β_i)를 사용한다. 서버와 사용자간에 설정된 세션키 (Session Key)는 sk로 표기한다. 큰 소수 p에 대하여 g는 Z_p^*의 생성자 (Generator)라 하자. Timestamp는 T로, nonce는 N으로 나타내자. 끝으로 H는 암호학적 일방향 해시 함수 (Cryptographic One-way Hash Function)라 하자.

3.2 Tsai et al. 기법의 개요

이제 위 표기법을 사용하여 Tsai 등이 제안한 기법을 설명한다. 이들이 제안한 기법도 전술한 바와 같이 설정 단계, 등록 단계, 로그인 단계, 검증 단계를 포함하며 추가로 사용자의 편의를 위해 패스워드변경 단계를 갖는다.

설정 단계에서 서버 S는 자신의 비밀키 X를 선택하고 공개키 $Y = g^X \bmod p$를 계산하여 사용자들에게 발급될 스마트카드에 (g, p, Y)를 저장한다.

등록 단계에서 사용자 U_i는 안전한 채널을 이용하여 자신의 ID와 패스워드 쌍 (α_i, β_i)를 전송한다. 서버 S는 수신한 값들로부터

$$R_i = H(\alpha_i \| \beta_i) \oplus H(X \| \alpha_i)$$

을 계산하여 사용자에게 발급할 스마트카드의 안전한 메모리에 저장하여 U_i에게 발급한다.

로그인 단계에서 임의의 사용자 U_i가 서버에 접근하려면 발급된 스마트카드를 삽입한 후 자신의 (α_i, β_i)를 입력한다. 그러면 스마트카드는

$$S_i = R_i \oplus H(\alpha_i \| \beta_i) = H(X \| \alpha_i)$$

를 계산하고, 추가로 사용자의 동적 ID 값으로

$$\begin{aligned} \delta_i &= \alpha_i \oplus H(Y^r \bmod p \| T_u), \\ A &= g^r \bmod p, \\ B &= H(\delta_i \| A \| S_i \| Y \| T_u) \end{aligned}$$

를 계산한다. 여기서 r은 난수이며 T_u는 사용자의 timestamp 값이다. 계산이 완료되면 스마트카드는 (δ_i, A, B, T_u)를 서버에 전송한다.

검증 단계는 다음과 같이 동작한다. 사용자가 (δ_i, A, B, T_u)를 이용하여 로그인을 요청하면 timestamp의 유효기간을 검증하여 수락여부를 우선 결정한다. 다음으로 사용자의 ID를

$$\alpha_i = H(A^X \bmod p \| T_u) \oplus \delta_i$$

를 계산하여 얻고

$$B' = H(\delta_i \| A \| H(X \| \alpha_i) \| Y \| T_u)$$

를 추가 계산하여 $B' == B$를 만족하는지 확인한다. 만족한다면 사용자와 서버간의 세션키와 C를 다음과 같이 계산한다:

$$\begin{aligned} sk &= H(H(X \| \alpha_i) \| T_u \| B \| \delta_i \| T_s, \\ C &= H(sk \| H(X \| \alpha_i) \| T_u \| T_s). \end{aligned}$$

이제 (C, T_s)를 사용자에게 전송한다. 이 값을 서버로부터 수신한 사용자는 먼저 세션키 sk를 계산하기

www.dbpia.co.kr

위해 $sk = H(S_i \| T_u \| B \| \delta_i \| T_s)$를 계산하고 $C' = H(sk \| S_i \| T_u \| T_s)$를 계산하여, $C' == C$을 확인한다. 이것이 성립한다면 상호인증이 이루어진 것으로 간주한다. 이후 서버와 사용자의 메시지는 sk를 사용하여 암/복호화된다.

패스워드변경 단계는 사용자가 기존의 패스워드 β_i를 새로운 패스워드 β'_i로 변경하기를 원하는 경우에 수행된다. 이를 위하여 사용자가 자신의 스마트카드를 삽입하면 $S_i = R_i \oplus H(\alpha_i \| \beta_i)$를 계산하여 $R'_i = H(\alpha_i \| \beta'_i) \oplus S_i$를 수행한다. 그리고 스마트카드에 R_i 대신에 R'_i를 저장하는 것으로 완료된다.

3.3 Tsai et al.기법의 안전성 분석

본 장에서는 Tsai 등이 제시한 기법이 가질 수 있는 취약점을 분석한다. 요약하면 먼저 서비스거부공격에 취약할 수 있는데 그 이유는 로그인 요청을 만들기 전에 조기에 패스워드가 잘못된 것인지 탐지하는 기능이 없기 때문이다. 둘째, 패스워드 변경 단계가 안전하지 않다. 마지막으로 내부자 공격에 취약할 수 있다. 분석을 위하여 사용자와 서버간의 모든 메시지는 공격자가 얻을 수 있다고 가정하자.

(1) 잘못된 패스워드 조기 탐지 실패: 로그인을 요청하는 사용자가 정당한 스마트카드의 소유자인지 판단하는 과정에서, 사용자의 로그인 요청이 서버에 전송되기 전에 스마트카드가 사용자의 패스워드 오류 여부를 먼저 판단할 필요가 있다. Tsai 등의 기법에서 사용자가 패스워드를 잘못 입력한 경우 이 패스워드는 검증단계까지 진행되어야 사용자가 입력한 패스워드에 오류가 있다는 사실을 확인할 수 있다. 그러므로 로그인 단계를 진행하기 전에 사용자의 패스워드가 잘못 입력되었는지 조기에 탐지하지 못한다. 이것은 사용자의 불편을 넘어, 다음과 같은 안전성 문제를 내포한다.

사용자 자신이 패스워드를 옳지 않게 입력한 사실을 늦게 알게 되는 문제점 이외에. 사용자 연산 단계가 아니라 서버의 연산 단계에서 패스워드 오류를 탐지하는 특성을 공격자가 능동적으로 활용할 수 있다[22]. 공격자가 임의의 패스워드를 사용하여 서버에 끊임없이 로그인을 요청하면 정당한 사용자의 서비스 요청을 처리할 수 없는 서비스거부 공격에 취약하게 된다. 서비스거부 공격을 피하려면 사용자가 로그인 요청을 하는 단계에서 사용자에게 패스워드의 오류가 있다면 알려줄 수 있도록 수정할 필요가 있다.

(2) 내부자 공격에 취약: 서버에 접근할 수 있는 모든 내부자는 등록 단계에서 사용자의 ID와 패스워드를 탈취할 수 있다. 왜냐하면 등록 단계에서 사용자가 안전한 채널로 (α_i, β_i)를 전송하더라도 내부자는 언제든지 자신이 원하면 사용자의 패스워드를 얻을 수 있다. 내부자에 의해서 비밀정보가 누설될 수 있는 문제뿐만 아니라, 이렇게 탈취된 정보는 해당 사용자가 다른 서버에 서비스를 요청할 때 공격자가 위장공격에 이용될 수 있는 문제도 있다. 이러한 공격은 [14]에서 이용된바 있다.

(3) 패스워드 변경 단계의 안전성 문제: 사용자가 패스워드 변경을 요청하는 경우, Tsai 등의 기법은 기존 패스워드에 대한 검증 절차 없이 새로운 패스워드로 대체된다. 스마트카드를 분실하거나 도난당한 경우, 탈취자는 자신이 원하는 패스워드로 쉽게 변경하여 서비스를 이용할 수 있기 때문에 사용자 측면의 안전성을 강화하기 위해 이전 패스워드를 확인한 후 새로운 패스워드로 변경할 수 있도록 수정할 필요가 있다.

Ⅳ. 제안하는 기법

본 장에서는 본 연구진이 제안하는 스마트카드 기반 인증기법을 제시한다. 상위 수준에서 보면 기존 기법과 마찬가지로 네 단계로 구성되는 것으로 볼 수 있으나 본 논문에서는 패스워드 변경 단계를 별도로 나누어 설명한다.

안전성 가정. 스마트카드의 안전한 영역은 외부에서 접근할 수 없으며, 서버는 다른 서버들과의 공모가 허용되지 않는다. 그러므로 사이드채널 공격이나 서버가 자신의 비밀값을 다른 서버와 공유하는 것은 허용되지 않는다.

4.1 설정 단계

기존 기법과 마찬가지로, 서버 S는 안전성 조건을 만족하는 충분히 큰 소수 p를 선택하고, 난수 r을 생성하여 안전하게 보관한다. 그리고 자신의 비밀키 X와 공개키 $Y = g^r \bmod p$를 계산하고 X를 안전하게 보관한다. 시스템에서 사용할 암호학적 해시 함수 H를 결정한 후, 공개키 (p, g, Y, H)를 사용자들에게 발급할 스마트카드에 저장한다. 이러한 H는 일방향성, 강일방향성과 충돌회피성을 모두 만족한다.

4.2 등록 단계

사용자 U_i는 자신의 ID와 패스워드 쌍인 (α_i, β_i)

www.dbpia.co.kr

를 만든 후, $(\alpha_i, \overline{\beta}_i = H(\beta_i))$를 안전한 채널을 통해 서버에게 전송한다. 등록 요청을 수신한 서버는 자신의 비밀 난수값 r을 이용하여 $u_i = g^{\overline{\beta}_i \cdot r} \bmod p$와 $v_i = H(\alpha_i \| X)$를 계산한다. 그리고 (u_i, v_i, r)을 스마트카드의 안전한 메모리 영역에 저장한 후 사용자 U_i에게 발급한다.

4.3 로그인 단계

서버의 서비스를 이용하려는 사용자 U_i는 스마트카드를 삽입한 후, 자신의 ID α_i와 패스워드 β_i을 입력한다. 스마트카드는 입력된 값들을 사용하여 $u'_i = g^{H(\beta_i) \cdot r} \bmod p$를 계산하여 $u_i == u'_i$를 확인한다. 조건을 만족하지 않으면 적절한 메시지를 출력한 후 로그인 단계를 종료한다. 조건을 만족하면 스마트카드는 timestamp T_u를 생성한 후,

$$\begin{aligned} \overline{\alpha_i} &= \alpha \oplus H(u_i \| T_u), \\ w_i &= H(\beta_i) + H(\alpha_i \| u_i \| v_i \| T_u) \bmod p - 1, \\ z_i &= g^{H(\beta_i)} \bmod p \end{aligned}$$

를 차례로 계산한다. 스마트카드는 사용자의 로그인 요청 메시지로 $(\overline{\alpha_i}, w_i, z_i, T_u)$를 서버에 전송한다. 그림으로 정리하면 다음과 같다.

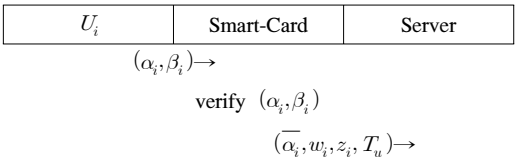

Fig. 1. Log-in Phase

4.4 검증 단계

로그인 요청 메시지를 수신한 서버 S는 우선 사용자의 timestamp T_u를 검증하여 유효하지 않으면 검증 단계를 종료하고 적절한 메시지를 전송한다. 이 값이 유효하다면 $u_i = z_i^r \bmod p$를 얻은 후, $\alpha_i = \overline{\alpha}_i \oplus H(u_i \| T_u)$를 계산하여 사용자의 ID를 복구한다. 복구한 ID α_i가 등록된 사용자의 ID인지 확인하고 유효한 ID가 아니면 검증 단계를 종료하고 적절한 메시지를 전송한다. 유효한 ID이면 차례대로

$$\begin{aligned} v_i &= H(\alpha_i \| X), \\ B &= z_i \cdot g^{H(\alpha_i \| u_i \| v_i \| T_u)} \bmod p, \\ B' &= g^{w_i} \bmod p \end{aligned}$$

를 계산하여, $B' == B$ 조건이 성립하는지 확인하여 성립하지 않으면 검증 단계를 종료하고 적절한 메시지를 전송한다. 성립한다면 자신의 timestamp T_s를 생성한 후

$$C = H(H(\alpha_i \| u_i \| v_i \| T_u) \| T_u \| T_s)$$

를 계산하여 $(\overline{\alpha}_i, C, T_s)$를 응답으로 사용자 U_i에게 전송한다.

이 값을 수신한 사용자 U_i는

$$C' = H(H(\alpha_i \| u_i \| v_i \| T_u) \| T_u \| T_s)$$

를 계산하여 $C' == C$ 조건을 만족하는지 확인한다. 조건이 성립하지 않으면 서버의 인증 실패 메시지를 출력하고 검증 단계를 종료한다. 조건이 성립하면 서버 S와 사용자 U_i간의 상호인증이 성공한 것으로 메시지를 출력하고, 그들 간의 세션키 값을

$$sk = H(\alpha_i \| u_i \| v_i \| T_u \| T_s)$$

로 설정한다. 위 내용은 다음 Fig. 2로 정리할 수 있다.

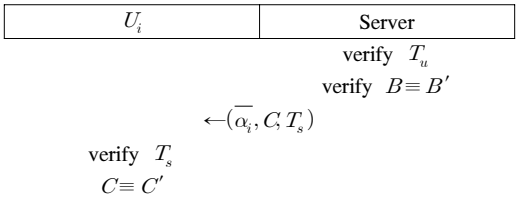

Fig. 2. Verification Phase

4.5 패스워드 변경 단계

사용자 U_i가 자신의 패스워드를 변경하기 원하는 경우, 스마트카드를 삽입한 후 자신의 ID와 패스워드의 쌍 (α_i, β_i)를 입력한다. 그러면 스마트카드는 $u = g^{H(\beta_i) \cdot r} \bmod p$를 수행하여 $u == u_i$ 조건을 확인한다. 조건이 성립하지 않으면 패스워드 변경 단계를 종료하고 적절한 메시지를 출력한다.

www.dbpia.co.kr

조건이 성립하면 사용자에게 새로운 패스워드를 요청한다. 사용자가 새로운 패스워드 β'_i를 입력하면 스마트카드는 $u'_i = g^{H(\beta'_i)\cdot r} \bmod p$를 계산하여 u_i에 덮어쓴다. 스마트카드를 분실한 경우 공격자의 패스워드 추측 공격을 방지하기 위해 패스워드 입력 오류 횟수를 지정하는 방법을 추가할 수 있다.

Remark: 만약 네트워크 간의 동기화가 어려운 문제로 timestamp의 유효성을 검증할 수 없는 환경을 생각할 수 있다. 이러한 경우에는 timestamp 대신 nonce를 이용하는 방법을 이용할 수 있다. 설정/등록/패스워드 변경 단계는 timestamp를 필요로 하지 않기 때문에 수정할 필요 없다. 대신 로그인 단계와 검증 단계에서 timestamp 대신 nonce를 사용한다. 즉 T_u 대신 사용자는 nonce N_u를 생성하여 사용하고, 서버는 T_s 대신 N_s를 만들어서 사용한다. 그러면 검증 단계를 완료하면 사용자와 서버가 공유하는 세션키는

$$sk = H(\alpha_i \| u_i \| v_i \| N_u \| N_s)$$

이 된다.

Ⅴ. 제안하는 인증기법 분석

본 장에서는 제안하는 기법이 기존에 알려진 여러 가지 공격에 안전하다는 것을 먼저 확인하고, 이어서 기존 기법들과 연산의 횟수를 모두 구하는 방법으로 효율성을 비교하고 분석한다. 먼저 안전성 분석을 기술한다.

5.1 안전성 분석

• 위장 공격에 대한 안전성. ID 위장 공격은 대상 사용자의 통신내용을 도청한 후 그의 ID를 탈취하여 이후의 통신에서 탈취한 ID를 이용하여 그 사용자로 가장하고 통신하는 것이다. 공격자가 ID를 탈취할 수는 있으나 이를 사용할 수 없도록 하는 방법이 필요하다.

제안된 기법에서, 사용자 U_i로부터 서버에 전송되는 로그인 요청 메시지는 $(\overline{\alpha_i}, w_i, z_i, T_u)$로 구성되는데 여기서 $\overline{\alpha_i} = \alpha_i \oplus H(u_i \| T_u)$, $w_i = H(\beta_i) + H(\alpha_i \| u_i \| v_i \| T_u) \bmod p - 1$와 $z_i = g^{H(\beta_i)} \bmod p$이고 T_u는 U_i의 timestamp이다. 그러므로 공격자가 사용자 U_i로 위장하기 위해서는 $(\alpha_i, u_i, v_i, \beta_i)$를 모두 추측해서 맞추어야 한다. 만약 공격자가 올바른 패스워드 β_i를 고른다 하여도 u_i를 계산하기 위해 필요한 서버의 비밀값 r과 v_i를 알아야 한다. 이것은 이산대수 문제의 어려움과 암호학적 해시 함수의 안전성을 가정하면 제안하는 기법은 위장 공격에 안전하다는 것을 의미한다. 서버를 위장하려는 공격 또한 유사한 이유로 회피할 수 있다.

• 재생 공격에 대한 안전성. 재생 공격은 대상 사용자와 서버간의 통신 내용을 모두 기록한 후, 기존의 통신 내용을 재사용하는 것이다. 그러면 공격자는 공개된 채널을 통해 이전에 습득한 메시지를 재전송하는 방법을 이용하여 인증된 사용자처럼 시도할 수 있다. 제안하는 기법은 사용자 U_i와 서버 S가 각자의 timestamp T_u와 T_s를 송수신하는 메시지의 계산에 이용한다. 그러므로 공격자는 이전에 전송된 메시지를 이용하여 정당한 사용자를 흉내 낼 수 없다. 예를 들어, 만약 공격자가 사용자 U_i의 timestamp T_u를 수정하여 U_i를 흉내 내려면 $\overline{\alpha_i}$와 w_i를 다시 계산해야 하는데 이를 위해서는 (α_i, u_i, v_i)를 모두 알아야 하고, 전술한 바와 같은 이유로 제안하는 기법은 재생 공격에 대하여 안전하다.

• 패스워드 추측 공격에 대한 안전성. 패스워드 추측 공격은 공격자가 대상으로 하는 사용자의 ID를 알아낸 후, 그 사용자가 사용할 것으로 예상되는 패스워드를 입력하는 공격방법이다. 패스워드를 추측으로 맞추는 것이 가능하기 때문에 이러한 패스워드 이외의 정보가 인증에 이용될 필요가 있다.

제안한 기법에서 패스워드는 항상 $H(\beta_i)$ 연산을 수행한 후 그 결과를 이용하여 다른 연산을 수행하거나 공개된 채널로 전송된다. 이제 사용자 U_i의 로그인 요청 메시지 $(\overline{\alpha_i}, w_i, z_i, T_u)$를 공격자가 가로챘다고 하자. 그러나 $(\overline{\alpha_i}, w_i, z_i)$를 계산하는데 이용된 $(\alpha_i, u_i, v_i, \beta_i)$를 동시에 모두 맞추는 것은 거의 불가능하다. 특히 z_i를 계산하기 위해서는 이산대수 문제를 풀 수 있어야 하고 동시에 암호학적 해시 함수의 역상도 구해야 한다. 그러므로 제안하는 기법은 패스워드 추측 공격에 안전하다. 온라인 (On-line) 상의 패스워드 추측 공격을 막기 위해서는 패스워드 입력의 오류 횟수를 제한하는 방법을 이용할 수 있다.

• 훔친 검증자 공격에 대한 안전성. 검증자 역할을 하는 서버의 일정 정보를 탈취하여 서버의 검증 기능을 흉내 내는 공격으로, 공격자는 이를 통하여 사용자의 비밀 정보를 알아낼 수 있다. 제안하는 기법에서 서버는 검증하는 단계에서 사용자 U_i의 민감한 정보

www.dbpia.co.kr

에 접근할 수 있다. 그러나 여기서 제안한 기법은 기존 기법과 같이 검증테이블에 사용자의 패스워드를 저장하는 것이 아니라 서버의 비밀값 (X,r)을 이용하도록 한다. 그러므로 서버는 검증 단계에서 자신의 비밀값에는 접근할 수 있으나 사용자의 ID α_i를 제외한 어떠한 비밀값도 알 수 없다.

• **내부자 공격에 대한 안전성**. 내부자 공격은 서버를 운영하는 기관이 악의적인 경우로서 기관 내부 직원이 사용자의 비밀정보에 접근하여 탈취한다. 특히 일반 사용자들은 다양한 서비스를 얻기 위해 여러 서버를 이용하더라도 동일한 패스워드를 사용하는 경향이 있다. 이럴 경우 서버를 관리하는 관리자등의 경우 정당한 사용자의 비밀값에 접근하는 것이 허용되면 공격자는 이러한 특징을 악용할 수 있다. 여기서 제안한 기법은 패스워드가 $\overline{\beta}_i = H(\beta_i)$로 변환되어 전송되고 저장된다. 그래서 암호학적 해시 함수가 안전하다면 제안하는 기법도 내부자 공격에 대하여 안전하다.

• **반사 공격과 병렬세션 공격에 대한 안전성**. 두 공격 방법모두 사용자와 서버 간에 전송되는 메시지가 송수신되는 메시지의 특징을 이용하는 것으로 사용자나 서버의 메시지를 그대로 재사용하는 것이 가능한 경우에 허용된다. 제안하는 기법은 메시지의 규격을 비대칭적으로 구성함으로써 이러한 공격을 회피하는 방법을 이용한다. 예를 들어 사용자가 $(\overline{\alpha}_i, w_i, z_i, T_u)$를 전송하고 $(\overline{\alpha}_i, C, T_s)$를 수신하는 경우를 살펴보자. 여기서

$$\begin{aligned}\overline{\alpha_i} &= \alpha_i \oplus H(u_i \| T_u),\\ w_i &= H(\beta_i) + H(\alpha_i \| u_i \| v_i \| T_u) \bmod p - 1,\\ z_i &= g^{H(\beta_i)} \bmod p,\\ C &= H(H(\alpha_i \| u_i \| v_i \| T_u) T_u \| T_s)\end{aligned}$$

이므로 값들의 대칭성이 존재하지 않는다. 그래서 공격자는 사용자의 로그인 요청 메시지를 서버의 응답 메시지로 활용하는 병렬세션 공격과 서버의 응답 메시지를 사용자의 로그인 요청 메시지로 활용하는 반사 공격에 안전하다.

• **세션키의 안전성**. 제안된 기법은 세션이 만들어질 때 마다 서로 다른 세션키를 만들 수 있도록 한다. 즉 세션키는 $sk = H(\alpha_i \| u_i \| v_i \| T_u \| T_s)$ 계산을 통하여 유도되므로 T_u와 T_s에 따라 값이 변경된다. 또한 공격자는 전술한 바와 같이 (α_i, u_i, v_i)를 동시에 맞추는 것은 불가능하다.

• **서비스거부 공격에 대한 안전성**. 서비스거부 공격은 공격자가 서버와의 통신을 독점하여 다른 사용자가 서버에 접근할 수 없도록 하는 공격이다. 제안하는 기법은 전술한 바와 같이 패스워드 검증이 서버 측에서 이루어지지 않고 사용자 측에서 조기에 검증되는 기능은 서비스거부 공격을 회피하기 위한 중요한 기능이다. 제안하는 기법에서도 스마트카드가, 등록 단계에서 저장한 $u_i = g^{\overline{\beta}_i \cdot r} \bmod p$ 값과 로그인 단계에서 사용자가 입력한 패스워드를 사용하여 동일한 계산을 수행한 후 값을 먼저 비교하는 방법을 사용한다. 그러므로 스마트카드는 사용자가 입력한 패스워드의 오류를 조기에 탐지하여 오류 메시지를 출력할 수 있기 때문에 공격자에 의해 서비스거부 공격에 역이용되는 것을 피할 수 있다.

• **사용자의 익명성**. 제안하는 기법은 부분적으로 사용자의 익명성을 보장할 수 있다. 완전하게 사용자의 익명성을 보장할 수는 없으나 공개된 채널에 사용자 ID α_i를 직접 사용하는 대신 익명 ID $\overline{\alpha}_i = \alpha_i \oplus H(u_i \| T_u)$를 사용한다. 원래의 ID를 복원하는 서버의 내부자에게는 드러나지만 공개된 채널을 통해 공격자는 정확한 사용자를 알아내는 것은 해시 함수의 안전성에 의해 보장된다.

5.2 연산량 분석

연산량 측면에서 기존 기법과 비교하기 위해 별도의 표기법을 도입한다. 이를 위해 H는 암호학적 해시 함수 1회 수행을 의미하며, A/M/E는 각각 modulus p 상의 덧셈/곱셈/지수승 연산 1회 수행을 의미한다. 이러한 표기법을 이용해 제안하는 기법과 Tsai 등의 기법의 연산량 비교 결과를 정리하면 아래 Table 1과 같다.

정리하여 설명하면, 제안하는 기법은 1번의 해시함수 연산과 대략 4번의 유한체 지수승 연산을 추가하여 기존 기법에서 만족하지 못하는 서비스거부 공격에 대한 취약점, 내부자 공격에 대한 취약점과 패스워드 변경시 발생할 수 있는 안전성 문제를 해결한다.

Table 1. Computational Complexity Comparison

	Tsai et al. Scheme	Proposed Scheme
Setup	1E	1E
Registration	2H	2H+1E
Login	3H+2E	3H+1A+1M+2E
Verification	7H+2E	7H+1M+3E
Change Pwd	1H	2H+2M+2E
Total	13H+5E	14H+1A+4M+9E

www.dbpia.co.kr

서버 측면에서 연산량은 1M+2E 증가하였고, 사용자 측면에서는 1A+3M+2E 만큼 증가하였다. 서버 측면에서의 연산량 증가보다는 사용자 측면의 연산량 증가량이 많은 것은 사실이나 스마트카드의 연산 능력을 고려할 때 modulus p 상에서 대략 지수승 3번을 더하는 것이 실용성을 저해할 수준의 연산량 증가라 할 수 없다. 그 이유는 다음과 같다.

- 등록 단계에서 modulus p상의 지수승 연산이 추가되었으나 이는 서버가 수행하는 연산이다.
- 로그인 단계는 Tsai 등의 기법과 마찬가지로 두 번의 지수승 연산을 사용하고 추가로 제안하는 기법은 1번의 덧셈과 1번의 곱셈을 추가로 사용하는데 [6]의 결과를 이용하면 약 700ms의 시간만 추가된다.
- 검증 단계에서 modulus p상의 곱셈 1번과 지수승 1번을 추가로 필요로 하는데 서버가 모두 수행하는 연산이다.
- 패스워드 변경 단계는 Tsai 등이 제안한 기법에 비교하여 2번의 곱셈과 2번의 지수승 연산을 추가로 필요로 하므로 사용자 측면에서 가장 큰 연산이나 서버와의 통신을 필요로 하지 않고 스마트카드만 연산을 수행하면 된다.

Ⅵ. 결 론

IT 시스템에서 인증기법은 핵심적인 암호기법의 하나로 특히 패스워드 기반의 스마트카드를 이용하는 인증기법에 대한 다양한 연구가 요구되는 상황에서 Tsai 등의 연구자가 스마트카드를 이용한 동적 ID 인증기법을 제시하였으나, 서비스거부 공격과 내부자 공격에 취약하고 사용자의 필요에 의해 패스워드를 변경하는 경우 안전성이 훼손될 수 있음을 제시하였다. 이러한 문제를 해결하기 위해 본 논문에서 Tsai 등의 기법을 수정하여, 연산량을 추가하는 대신 이러한 공격에 안전하고 패스워드 변경 시 발생할 수 있는 안전성 문제를 해결하였다.

제안하는 기법은 위장 공격, 내부자 공격, 패스워드 추측 공격, 반사 공격, 병렬세션 공격, 재생 공격에 안전하다. 또한 사용자가 원하는 경우 언제든지 자신의 패스워드를 변경하는 것이 가능하다. 스마트카드 수준에서 사용자가 입력한 패스워드의 오류 여부를 조기에 판단할 수 있기 때문에 서비스거부 공격에 안전하다. 끝으로 상호인증 기능이 지원되는 특징이 있다. 특히 사용되는 연산이 단순하고 가벼워 다중서버 인증 [13]과 IP-TV와 같은 환경에서 적합할 것으로 기대한다.

References

[1] C. Chan and L. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.*, vol. 46, no. 4, pp. 992-993, Nov. 2000.

[2] C. Chan and L. Cheng, "Cryptanalysis of timestamp-based password authentication scheme," *J. Computers and Security*, vol. 21, no. 1, pp. 74-76, 1st Quarter 2001.

[3] H. Chien, J. Jan, and Y. Tseng, "An efficient and practical solution to remote authentication: Smart card," *J. Computers and Security*, vol. 21, no. 4, pp. 372-375, Aug. 2002.

[4] Citrix, http://support.citrix.com.

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

[6] N. Duif, "Smart card implementation of a digital signature scheme for twisted Edwards curves," M.S. Thesis, Technische Universiteit Eindhoven, May, 2011.

[7] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inform. Theory*, vol. 31, no. 4, pp. 469-472, Jul. 1985.

[8] M. Hwang and L. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.*, vol. 46, no. 1, pp. 28-30, Feb. 2000.

[9] M. Hwang, C. Lee, and Y. Tang, "A simple remote user authentication scheme," *Math. and Computer Modelling*, vol. 36, no. 1, pp. 103-107, Nov. 2002.

[10] C. Hsu, "Security of two remote user authentication schemes using smart cards," *IEEE Trans. Consumer Electron.*, vol. 49, no. 4, pp. 1196-1198, Nov. 2003.

[11] Z. Hao and N. Yu, "A security enhanced remote password authentication scheme using smart card," *ISDPE*, pp. 56-60, Buffalo, NY, Sept. 2010.

www.dbpia.co.kr

[12] I. Lee, C. Lee, and M. Hwang, “Security enhancement for a dynamic ID-based remote user authentication scheme,” *NWeSP*, pp. 437-440, Seoul, Korea, Aug. 2005.

[13] M. Kim, “A brokered authentication scheme based on smart-card for multi-server authentication,” *J. KICS*, vol. 38, no B.3, pp. 190-198, Mar. 2013.

[14] W. Ku and S. Chen, “Weakness and improvements of an efficient password based remote user authentication using smart cards,” *IEEE Trans. Consumer Electron.*, vol. 50, no. 1, pp. 204-207, Feb. 2004.

[15] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[16] H. Sun, “An efficient remote use authentication scheme using smart cards,” *IEEE Trans. Consumer Electron.*, vol. 46, no. 4, pp. 958-961, Nov. 2000.

[17] J. Tsai, T. Wu, and K. Tsai, “New dynamic ID authentication scheme using smart cards,” *IJCS*, vol. 23, no. 12, pp. 1449-1462, Dec. 2010.

[18] Y. Wang, J. Liu, F. Xiao, and J. Dan, “A more efficient and secure dynamic ID-based remote user authentication scene,” *Computer Comm.*, vol. 32, pp. 583-585, 2009.

[19] X. Wang, W. Zhang, J. Zhang, and M. Khan, “Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards,” *Computer Standards and Interfaces*, vol. 29, no. 5, pp. 507-512, Jul. 2007.

[20] E. Yoon, E. Lee, and K. Yoo, “Cryptanalysis of Wang et al.’s remote user authentication scheme using smart cards,” *ICIT: New Generations*, pp. 575-580, Las Vegas, USA, Apr. 2008.

[21] E. Yoon, E. Ryu, and Y. Yoo, “Further improvement of an efficient password based remote user authentication scheme using smart cards,” *IEEE Trans. Consumer Electron.*, vol. 50, no. 2, pp. 612-614, May 2004.

[22] E. Yoon, E. Ryu, and Y. Yoo, “An improvement of Hwang-Lee-Tang’s simple remote user authentication scheme,” *Computers & Security*, vol. 24, no. 1, pp. 50-56, Feb. 2005.

[23] W. Yang and S. Shieh, “Password authentication schemes with smart cards,” *Computers and Security*, vol. 18, no. 8, pp.727-733, 1999.

[24] H. Zhang and M. Li, “Security vulnerabilities of an remote password authentication scheme with smart card,” *CECNet*, pp. 698-701, Xianning, China, Apr. 2011.

김 명 선 (Myungsun Kim)

1994년 2월 : 서강대학교 전자계산학과 졸업

2002년 8월 : 한국정보통신대학원대학교 컴퓨터공학과 석사

2012년 8월 : 서울대학교 수리과학부 박사

2012년 9월~현재 : 수원대학교 정보보호학과 조교수

<관심분야> 암호학, 다자간 연산

www.dbpia.co.kr