Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

A Study on Weakness of a Secure Dynamic Identify based Remote User Authentication scheme for Multi-server Environment using Smart Card

Kwang-Cheul Shin*

Division of Industrial & Management Engineering, Sungkyul University

ABSTRACT

Recently, in the multi-server environment, many studies have been conducted based upon remote user authentication scheme by dynamic identifier. For the access of legally permitted user to application server and protection of sensitive information, smart card and bio-based password authentication scheme were published. Lee-Lin-Chang's scheme found a vulnerability of Hsiang-Shih's scheme and announced an improved scheme in 2011. But Lee et al's scheme showed weakness to various attacks when the smart card was stolen or third party eavesdropped on network. Also, it is vulnerable in smart card stolen attack, malicious user attacks, server attacks (impersonation attacks) and replay attacks since the shared information of each server and registration center are the same. In this paper, I suggest the improved scheme which is secure to user and server impersonation attack, replay attack, smart card stolen attack and password guessing attack by designing to allow access to multi-server with only one registration to the registration center rather than separating registration for each server. Efficiency of security, convenience and operating cost are enhanced by only using one-way hash function.

KEYWORDS: Smart card, Smart card stolen attack, Impersonation attack, Replay attack, Mutual authentication, Password guess attack

ARTICLE INFO: Received 6 August 2015, Revised 8 October 2015, Accepted 8 October 2015.

*Corresponding author is with the Department of Industrial & Management Engineering, Sungkyul University, 53 Sungkyul University-ro Manan-gu, Anyang-si, Gyeonggi-do, 430-742, KOREA.

E-mail address: skcskc12@sungkyul.ac.kr

1. 서 론

오늘날 많은 네트워크 서비스는 원격서버에 의해 사용자 인증을 제공하고 있다. 인증은 비 권한자의 서버접근을 방지하기 위해 네트워크를 통해 사용자에 대한 사전등록을 필요로 한다. 전통적인 단일서버 인증방식은 많은 웹서비스에서 편리성을 이유로 패스워드인증시스템을 주로 사용하며 서버가 사용자 식별자를 보유하고 검증테이블에는 사용자의 패스워드가 등록된다.

이 방식은 네트워크를 통해 전송되는 인증정보를 가로채서 서버나 사용자로 위장하기 쉬우며 가로챈 정보를 사용하여 서버로 로그인을 할 수 있다. 그러므로 패스워드인증은 패스워드 추측공격, 사전공격, KeyLoging 공격 등 다양한 공격에 취약한 것으로 알려져 있다. 이 와 같은 이유로 테이블 수정을 방지하기 위해 해시함수로 패스워드를 인코딩하여 검증테이블에 저장하여 해결하는 등 스마트카드에 의한 원격 사용자 인증의 문제는 다양한 스킴들의 연구로 이미 해결되었다[1-4].

만일 전통적인 패스워드 인증방식이 멀티서버환경에 적용된다면 각 네트워크 사용자는 다양한 원격서버에 로그인 할 때마다 서로 다른 많은 아이디 식별자와 대응 패스워드를 기억해야 하는 것이 비효율적일 뿐 아니라 참여자들 간에 공유하는 비밀정보의 효율적인 관리가 문제가 된다. 이와 같이 멀티서버 환경에서는 다양한 원격서버에 반복적으로 등록해야하고 여러 다른 아이디와 패스워드를 기억해야 하기 때문에 전통적인 인증스킴을 적용하기가 곤란하다.

지금까지 많은 연구에 의해 멀티서버환경의 자원을 접근하기 위한 스킴들이 제안되었다[5-7]. 이들 스킴들은 스마트카드 기반의 스킴들로써 계산복잡도에 따라 해시기반인증과 공개키 기반인증의 형태로 연구가 되었다. 멀티서버환경에서 원격사용자 인증스킴의 안전성과 효율성의 요구사항은 다음과 같다[8].

- 요구 1: 사용자는 하나의 등록센터(RC : Registration Center)에 등록하여 등록된 자원서버 모두에게 접근할 수 있어야 한다.
- 요구 2: 스마트카드는 계산능력의 제한으로 인증스킴은 효율적인 연산이어야 한다.
- 요구 3: 각 등록서버는 패스워드 또는 검증테이블을 사용하지 않아야 한다.
- 요구 4: 패스워드는 자유롭게 선택 및 수정할 수 있어야 한다.
- 요구 5: 사용자와 서버 간에 각각 다른 인증을 위해 상호인증과 키 동의가 제공되어야 한다.
- 요구 6: 인증스킴은 현실적으로 발생할 수 있는 다양한 공격을 방지할 수 있어야 한다.

대부분 전통적인 멀티서버 인증스킴에서 공통적인 특징은 사용자의 식별자가 고정적이므로 제3자가 부분적인 인증정보를 수집하여 동일한 사용자를 식별하고 전송정보를 획득하여 다양한 공격의 대상이 되고 있다. 이러한 위험을 방지하기 위해 2009년 Liao et al's[9]은 멀티서버 환경에서 단방향 해시함수만을 사용하여 사용자의 익명을 제공하는 동적 ID원격사용자 인증스킴을 발표하였다. 그러나 Hsiang et al's[10]는 Liao et al's 스킴이 내부자공격, 위장공격, 서버위조공격, 등록센터 위조공격에 취약함과 상호인증의 실패를 지적하고 개선된 스킴을 발표했다. 2011년 Sood et al's[11]는 Hsiang et al's 스킴이 안전하지 않다고 지적했다. 그들은 Hsiang and Shih스킴이 재생공격, 위장공격, 스마트카드 도난공격, 패스워드변경에 취약함을 발견하고 익명성과 다른 여러 가지 공격을 방지하는 스킴을 발표했다. 그러나 Sood et al's 스킴 또한 스마트카드 분실했을 때 시스템에 합법적인 사용자가 로그인하는 것처럼 위장이 가능하고 세션키 동의와 상호인증의 단점이 있다.

2012년 Tsaur et al's 스킴[12]과 2013년 Xu et al's 스킴[13]에서 사용자가 IDi, pwi를 안전한 채널로 RC에 전송하여 등록을 원할 때 RC는 서비스지원 서버의 ID(SIDj)를 스마트카드 저장정보(예 : Vij=h(Vi‖SIDj)에 포함시켜 다른 서비스지원 서버를 이용할 때는 다시 재등록하여야 하는 문제점이 있다.

멀티서버 환경에서는 사용자의 최초등록이 분할등록이 아닌 통합적으로 이루어져야 하는 것이 필수적이다. 사용자들은 RC에 최초 등록만으로 서비스지원 서버1, 서비스지원 서버2, ... 서비스지원 서버 n을 재등록이 없이 사용하여야 한다.

그러나 대부분의 연구에서는 RC가 초기 등록정보에서 서비스지원 서버를 지정하여 등록하여 스마트카드를 발급함으로써 다른 서비스지원 서버를 이용할 때는 또 다시 초기등록을 해야 하는 문제점이 있다. 즉 초기등록에서 스마트카드의 저장정보에 서비스 서버의 ID를 사용하는 것은 멀티환경에 부적합하다.

최근에는 여러 보안공격에 강하고 보안요구사항을 만족시키는 스마트카드와 생체정보를 이용한 신뢰 컴퓨팅기반 익명의 멀티서버 인증 키동의 스킴이 제안되고 있다[14][15].

본 논문에서는 Hsiang et al's 스킴의 위장공격 취약성을 발전시킨 Lee-Lin-Chang's[16] 스킴을 분석하고 문제점을 개선한 스킴을 제안한다. Lee-Lin-Chang's 스킴에서 취약한 원인은 RC와 각 서버간 공유하는 정보가 동일하다. 그러므로 제3자는 공유정보를 유도하여 다양한 공격에 사용한다. 또한 많은 인증정보의 생성으로 계산비용이 효율적이지 못하다. 이러한 단점을 보완하여 단일등록으로 멀티서버에 접근할 수 있는 스킴으로 검증테이블을 사용하지 않고 암호학적 단방향 해시함수만을 사용한다.

2. Lee et al's Scheme 연구

2011년 Lee-Lin Chang's이 제안한 멀티서버 환경에서의 동적 식별자에 기반을 둔 원격 사용자 인증스킴에 대해 검토하고 분석한다. 이 스킴은 등록, 로그인, 검증, 패스워드 변경단계로 사용자(Ui)와 서비스 제공서버(Sj), RC로 3개의 개체로 구성되어 있다[15].

RC는 자신만이 알고 있는 마스터키 x와 비밀 수 y를 선택하고 h(x‖y)와 h(y)를 계산하여 안전한 채널로 멀티서버들에게 전송하여 공유한다. 이 스킴의 장점은 Tsaur et al's 스킴 또는 Xu et al's 스킴과 달리 사용자의 스마트카드 정보에 서비스지원 서버의 식별자를 지정하지 않음으로써 분할등록을 하지 않는다. 본 논문을 통해서 사용될 표기법은 <Table 1>에 수록하였다.

표 1. 표기법
Table 1. Notation

parameter	context
U_i	i번째 사용자
S_j	j번째 서비스지원 서버
SID_j	서버 Sj의 식별자
x	RC의 마스터비밀키
y	RC만 알고 있는 비밀 수
h(.)	단방향 함수
Na	제3자(adversary)의 임의 난수
RC	등록센터(Registration Center)
->	비보호 채널
⇒	보호채널

2.1 등록단계

사용자 Ui가 서비스를 받기 위해 서비스 제공서버에 접근하기 위해서는 합법적인 클라이언트이어야 하므로 RC에 등록신청을 하고 스마트카드를 받

아야 한다. 등록단계의 과정은 다음과 같다.

(1) Ui는 IDi, pwi를 선택하고 무작위 수 b를 생성하여 h(b⊕pwi)를 계산한 다음 안전한 채널로 RC에게 IDi와 h(b⊕pwi)를 전송한다.

(2) RC는 자신의 비밀키와 비밀 수를 이용하여 Ti=h(IDi ‖ x), Vi=Ti⊕h(IDi ‖ h(b⊕pwi)), Bi=h(h(b⊕pwi) ‖ h(x ‖ y)), Hi=h(Ti)를 계산한다.

(3) RC는 스마트카드에 Vi, Bi, Hi, h(y), h(.)를 저장하여 안전한 채널로 사용자 Ui에게 전송한다.

(4) Ui는 스마트카드에 b를 입력(key in)하여 보유한다.

2.2 로그인단계

Ui가 서비스지원 서버 Sj로 로그인을 할 때 스마트카드를 리더기에 넣고 IDi, pwi, SIDj(서비스를 제공하는 서버의 식별자)를 입력하면 다음과 같은 과정으로 처리된다.

(1) 스마트카드는 Ti=Vi⊕h(IDi ‖ h(b⊕pwi)), Hi'=h(Ti)를 계산하고 Hi'와 스마트카드내장 정보 Hi의 값을 비교하여 일치하지 않으면 스마트카드는 거절하고 일치하면 다음 (2)를 진행한다.

(2) 스마트카드는 Nonce Ni를 생성하여 Ai=h(Ti ‖ h(y) ‖ Ni), CIDi=h(b⊕pwi)⊕h(Ti ‖ Ai ‖ Ni), Pij=Ti⊕h(h(y)) ‖ Ni ‖ SIDj), Qi=h(Bi ‖ Ai ‖ Ni)를 계산한다.

(3) Ui는 Sj로 IDi, CIDi, Pij, Qi, Ni를 전송한다.

2.3 검증단계

Sj는 IDi, CIDi, Pij, Qi, Ni를 수신하여 로그인 요청자의 검증을 위해 다음의 절차를 가진다.

(1) Sj는 Ti=Pij⊕h(h(y)) ‖ Ni ‖ SIDj), Ai=h(Ti ‖ h(y) ‖ Ni), h(b⊕pwi)=CIDi⊕h(Ti ‖ Ai ‖ Ni), Bi=h(h(b⊕pwi) ‖ h(x ‖ y))를 계산한다.

(2) Sj는 h(Bi ‖ Ai ‖ Ni)를 계산하여 Qi와 비교한다. 일치하지 않으면 세션을 종료하고 일치하면 Sj는 Nonce Nj를 생성하여 M'ij=h(Bi ‖ Ni ‖ Ai ‖ SIDj)를 계산하고 M'ij와 Nj를 Ui로 전송한다.

(3) Ui는 M'ij, Nj를 수신한 후 h(Bi ‖ Ni ‖ Ai ‖ SIDj)를 계산하여 M'ij와 비교한다. 일치하지 않으면 세션을 종료하고 일치하면 Ui는 M"ij=h(Bi ‖ Nj ‖ Ai ‖ SIDj)를 계산하여 Sj로 M"ij를 전송한다.

(4) Sj는 M"ij를 수신하여 h(Bi ‖ Nj ‖ Ai ‖ SIDj)를 계산하고 수신한 M"ij와 비교하여 일치하면 Ui는 Sj로부터 인증이 된다. 일치하지 않으면 세션을 종료시킨다. 마지막으로 Ui와 Sj는 세션동안 사용할 세션키 SK=h(Bi ‖ Ni ‖ Nj ‖ Ai ‖ SIDj)를 계산한다.

3. Lee et al'.s Scheme의 보안분석

Lee-Lin Chang's 스킴에서 제3자에 의해 스마트카드 정보와 로그인 메시지가 도청되었을 때 비밀정보 파라미터들은 어떻게 유도될 수 있으며 어떠한 취약점이 있는지를 분석한다.

3.1 스마트카드 도난 공격

Lee-Lin Chang's는 제3자에게 스마트카드를 도난당했거나 스마트카드내의 정보를 추출했다하더라도 Sj로 로그인 요청하는 메시지를 위조할 수 없다고 주장했다. 그러나 제3자는 스마트카드에서 Vi, Bi, Hi, h(y), h(.), b를 추출하고 이전의 로그인 메시지 CIDi, Pij, Qi, Ni를 도청했을 때 이들의 정보(Pij,h(y),Ni)를 이용하여 Ti=Pij⊕h(h(y)) ‖ Ni ‖ SIDj)를 계산할 수 있다. Ti가 계산되면 Ai=h(Ti ‖ h(y) ‖ Ni)는 쉽게 계산된다. Ai를 사용하여 h(b⊕pwi)=CIDi⊕h(Ti ‖ Ai ‖ Ni)를 계산하고 이어서 Bi=h(h(b⊕pwi) ‖ h(x ‖ y))를 유도할 수 있다. 그러면 이들 정보로부터 재생공격, 가장공격, 오프라인 패스워드추측공격 등을 할 수 있다. 제3자는 스마트카드 정보와

로그인 메시지를 통해서 쉽게 Ti를 계산할 수 있다는 것이 가장 큰 결점이다. Ti는 로그인 정보 Pij와 Ni그리고 스마트카드 정보 h(y), 수신처의 서비스제공 서버의 ID(SIDj)를 통해서 쉽게 Ti가 계산되며 Ti가 계산됨으로써 Ai를 쉽게 계산한다. 또한 Ai를 계산함으로써 h(b⊕pwi)=CIDi⊕h(Ti ‖ Ai ‖ Ni)를 구할 수 있다. 즉 제3자는 Ti, Ai, h(b⊕pwi)와 같은 3개의 비밀 파라미터 모두를 추출해 낼 수 있다. 이러한 정보를 제3자가 계산함으로써 재생공격과 위장공격, 악의적인 서버공격은 쉽게 이루어진다.

3.2 재생공격

공격자는 사용자가 패스워드를 변경하거나 새로 등록을 하지 않은 상태라면 이전의 로그인 메시지 CIDi, Pij, Qi, Ni를 그대로 전송한다고 가정한다. 여기에는 이전이나 이후에도 어떠한 정보 값들이 변경되지 않았으므로 로그인을 통해 서비스지원 서버의 로그인과정을 통과할 수 있다. 그때 Sj는 M'ij와 Nj를 Ui에게 전송할 것이고 제3자는 응답정보를 도청하여 M"ij=h(Bi ‖ Nj ‖ Ai ‖ SIDj)를 계산하고 세션키 SK=h(Bi ‖ Ni ‖ Nj ‖ Ai ‖ SIDj)를 쉽게 계산함으로써 재생공격이 성립된다.

3.3 위장공격

제3자는 Ti, h(b⊕pwi), Bi, h(y), SIDj를 알고 있다. 제3자는 임의 랜덤수 Na를 생성하고 위조된 로그인 메시지 CID'i, P'ij, Q'i, Na를 A'i=h(Ti ‖ h(y) ‖ Na), CID'i=h(b⊕pwi)⊕h(Ti ‖ A'i ‖ Na), P'ij=Ti⊕h(h(y)) ‖ Na ‖ SIDj), Q'i=h(Bi ‖ A'i ‖ Na)와 같이 생성한다.

재생공격에서와 같이 로그인 메시지인 CID'i, P'ij, Q'i, Na값들은 위조되었다는 것을 찾기 어려워 서버 Sj의 검증을 통과할 수 있다. 그러므로 제3자는 Sj와의 세션키 SKij'를 정확히 만들 수 있다.

3.4 악의적인 서버공격

RC와 모든 서비스지원 서버들은 동일한 비밀정보 h(x ‖ y), h(y)를 공유하는데 문제가 있다. 제3자는 다수의 서비스지원 서버들에 대해 동일한 악의적인 서버공격이 가능하다. 악의적인 서버 Sj는 또 다른 서버 Sk에 로그인을 하기 위해 합법적 사용자 Ui로 위장할 수 있다. 만일 Sj가 로그인 메시지 CIDi, Pij, Qi, Ni(또는 서버 Sl로 전송하는 메시지 CID'i, P'ij, Q'i, N'i를 가로챘거나)를 수신했다면 수신자는 Ti, h(y), h(b⊕pwi), Bi, SIDj값으로 Ti=Pij⊕h(h(y)) ‖ Ni ‖ SIDj), Ai=h(Ti ‖ h(y) ‖ Ni),h(b⊕pwi)=CIDi⊕h(Ti ‖ Ai ‖ Ni), Bi=h(h(b⊕pwi) ‖ h(x ‖ y))를 계산하거나 Ti=P'ij⊕h(h(y)) ‖ N'i ‖ SIDj), A'i=h(Ti ‖ h(y) ‖ N'i), h(b⊕pwi)=CID'i⊕ h(Ti ‖ A'i ‖ N'i), Bi=h(h(b⊕pwi) ‖ h(x ‖ y))를 계산함으로써 서비스지원 서버 Sj는 유효한 로그인 메시지로 위장하는데 성공한다.

4. 제안스킴

본 논문에서는 Lee-Lin Chang's 스킴의 스마트카드 도난에 따른 위장공격과 재생공격, 악의적인 서버공격에 대한 결점을 보완한 개선된 스마트카드기반의 원격 사용자인증 스킴으로 등록단계, 로그인단계, 인증 및 패스워드 변경단계로 제안한다.

Lee-Lin Chang's 스킴에서 정당한 사용자와 서비스지원 서버간의 인증에서 사용자의 스마트카드 분실과 로그인 메시지 도청에 따른 여러 공격을 근본적으로 차단할 수 있는 개선된 스킴을 제안한다.

세부 제안내용은 RC에 등록할 때 Nonce와 패스

워드를 해시 값으로 생성하여 보안성을 유지하고 사용자 로그인 정보에 대해서 서비스지원 서버에서 무결성 검사를 하여 메시지 위조여부를 검증한다. 또한 해시함수를 이용하여 중간자가 위조된 인증데이터를 생성할 수 없도록 구성하고 스마트카드의 사용자패스워드를 임의로 변경할 수 있도록 함으로써 중간자에 의한 도청 및 재 전송공격, 위장공격을 효율적으로 차단할 수 있는 프로토콜이다.

4.1 사용자 등록

<그림 1>과 같이 사용자는 IDi, pwi를 선택하고 Nonce b를 생성하여 h(b⊕pwi)를 계산, IDi, h(b⊕pwi)를 안전한 채널로 RC에게 전송한다. RC는 Bi=h(b⊕pwi)⊕h(x ‖ y)),Vi=h(IDi ‖ h(b⊕pwi) ‖ (h(y))를 계산하여 스마트카드에 Bi,Vi를 저장하여 Ui에게 전송한다.

4.2 서버 등록

서비스지원 서버 Sj는 아이디 SIDj를 선택하여 안전한 채널로 RC로 전송한다.

Sj로부터 등록요청을 수신한 RC는 서버 비밀파라미터인 SSj=h(SIDj ‖ h(x ‖ y)⊕h(y))를 계산하고 SSj와 h(y)를 Sj로 전송한다.

4.3 로그인 단계

<그림 2>와 같이 사용자 Ui는 다음과 같은 단계로 로그인 과정을 진행한다.

(1) 사용자 Ui는 스마트카드를 삽입하고 단말 입력장치를 통해 IDi와 pwi, SIDj를 입력한다.

스마트카드는 Vi'=h(IDi ‖ h(b⊕pwi))을 연산하여 스마트카드 소유자에 대한 카드유효성을 검증(Vi'=?Vi)한다. 이 때 Vi'와 Vi의 값이 다를 경우 종료된다.

(2) 정당한 스마트카드 소유자를 검증 후 Nonce N1과 시스템 시간 T1를 획득하여 ai=Bi⊕h(b⊕pwi), bi=h(SIDj ‖ ai), Qi=h(b⊕pwi)⊕h(bi) ‖ T1), CIDi=h(Vi ‖ N1)=h(h(IDi ‖ h(b⊕pwi)) ‖ N1)를 연산한다.

(3) 사용자 Ui는 CIDi,Qi,N1,T1를 비보호채널을 통해 시스템 S로 전송한다.

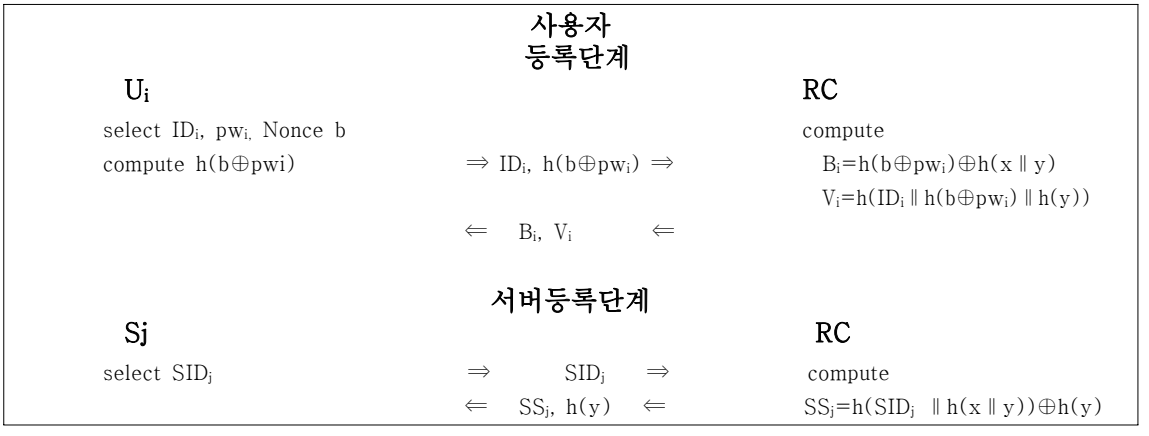

그림 1. 제안 스킴(등록단계)
Figure 1. Proposed Scheme(Registration Phase)

로그인단계

U_i		S_j
input ID_i, pw_i, SID_j		
compute		
$V_i'=h(ID_i \| h(b \oplus pw_i))$		
check $V_i'=?V_i$ //accept or reject		
generate Nonce N_1, timestamp T_1		
$ai=B_i \oplus h(b \oplus pw_i)$		
$bi=h(SID_j \| ai)$		
$Qi= h(b \oplus pw_i) \oplus (h(bi) \| T_1)$		
$CID_i=h(V_i \| N_1)$	----CID_i, Qi, N_1, T_1, ID_i---->	

인증단계

U_i		S_j
		Check T_1
		$SS_j'=h(SS_j) \oplus h(y)$
		$h(b \oplus pw_i)=Q_i \oplus h(SS_j') \| T_1)$
		$Q_i'=h(SS_j') \| T1) \oplus h(b \oplus pw_i)$
		Check $Q_i'=?Q_i$ //accept or reject
		$CID_i'=h(h(ID_i \| h(b \oplus pw_i) \| h(y)) \| N_1)$
		check $CID_i'=?CID_i$ //accept or reject
		if accept
		generate Nonce N_2, timestamp T_2
		$M'ij=h(SID_j \| h(SS_j \oplus h(y) \| N_2)$
		$M1'ij=h(M'ij \| T_2)$
	<------M1'ij, N_2, T_2----------	
Check T_2		
compute		
$M'ij'=h(SID_j \| h(h(SID_j \| h(x \| y)) \| N_2))$		
$M1'ij'=h(M'ij \| T_2)$		
verify whether M1'ij'=?M1'ij or not		
if it hold, compute $M"ij=h(M'ij \| N_1 \| N_2)$		
	--------M"ij-------->	compute $M"ij'=h(M'ij \| N_1 \| N_2)$
		verify whether M"ij'=?M"ij or not

세션 키 설정

$SK_{ij}=h(h(SID_j \| h(x \| y)) \| N1 \| N2)$	$SK_{ij}=h(h(SID_j \| SS_j \oplus h(y)) \| N1 \| N2)$

그림 2. 제안 스킴(로그인 및 인증단계)

Figure 2. Proposed Scheme(Login and Authentication Phase)

4.4 인증 단계

로그인 메시지 CIDi, Qi, N1, T1를 수신한 Sj는 로그인 요청에 대한 검증을 위해 다음 단계를 진행한다.

(1) 사용자 Ui의 IDi를 체크하여 유효성을 검사하고 메시지를 전달받은 시각 t1을 구하고 (T1-t1)≥△t이면 사용자 Ui의 로그인 요청을 거절한다. 여기서 △t는 전송시간을 고려한 최소 인증시간이다.

(2) 시스템 Sj는 Qi의 유효성 판단을 위해 h(b⊕pwi)를 생성할 수 있어야 한다. h(b⊕pwi)를 생성하기 위해 h(y)를 제거한 SSj'=SSj⊕h(y)=h(h(SSj ‖ h(x ‖ y))를 계산한다. SSj'는 Ui의 h(b⊕pwi)를 유도하는데 이용된다. 그 다음 SSj'를 사용하여 Qi'를 계산하고 Ui의 로그인 메시지 Qi와 비교하여 승인 또는 거절한다.

(3) CIDi의 값을 검사하기 위해 CIDi'=h(h(IDi ‖ h(b⊕pwi)) ‖ h(y) ‖ N1)를 계산한다. 그리고 Ui의 로그인 메시지 CIDi와 비교하여 승인 또는 거절한다.

(4) Sj는 Nonce N2, timestampT2를 생성하여 Ui에게 정당한 서버 Sj임을 증명하고 세션키를 생성할 M'ij를 계산한다. 다음 M'ij와 T2를 연접한 해시값 M1'ij를 계산하여 Ui에게 M1'ij, N2, T2를 전송한다.

(6) 사용자 Ui는 M1'ij, N2, T2를 수신하여 시각 t을 구하고 (t-T2)≥△t이면 Sj의 응답메시지를 거절하고 세션을 끊는다. 그렇지 않으면 M1'ij를 계산하기 위해 M'ij'를 계산하고 M1'ij'를 산출한다.

산출된 M1'ij'와 수신한 M1'ij를 비교하여 일치하지 않으면 세션을 거절한다. 일치하면 응답메시지 M"ij를 계산하여 Sj에게 M"ij를 전송하고 세션키(SKij)를 생성한다.

(7) M"ij를 수신한 Sj는 M"ij'를 생성하여 수신한 M"ij와 일치하는지 확인하고 일치하지 않으면 세션을 거절하고 그렇지 않으면 세션키(SKij)를 생성한다.

4.5 패스워드 변경 단계

(1) 사용자 Ui는 패스워드를 업데이트할 때 스마트카드를 리더기에 삽입하고 IDi와 pwi를 입력하면 스마트카드는 Vi'=h(IDi ‖ h(b⊕pwi))을 계산한다.

(2) 로그인 단계의 (1)과 같이 스마트카드는 Vi'=h(IDi ‖ h(b⊕pwi))을 연산하여 스마트카드 소유자에 대한 카드유효성을 검증(Vi'=?Vi)한다. 이 때 Vi'와 Vi의 값이 다를 경우 종료된다. Vi'=Vi를 만족하면 Ui는 새로운 패스워드pwinew를 입력한다. 이 때 스마트카드는 Binew=Bi⊕h(b⊕pwi)⊕h(b⊕pwinew)와 Vinew=h(IDi ‖ h(b⊕pwinew))계산한다.

(3) 스마트카드는 Vi,Bi를 대신하여 Vinew와 Binew를 저장한다. RC와 서비스지원 서버 Sj의 참여 없이 독립적으로 변경한다.

5. 보안성분석

본 절에서는 제안스킴에 대한 안전성과 효율성이 향상된 스킴을 논리적으로 증명한다. 가장 큰 특징은 Lee-Lin Chang's 스킴에서 스마트카드 도난/분실공격, 재생공격, 서버위장공격에 취약한 원인은 RC와 각 서비스지원 서버 간 공유하는 정보가 동일하다는 것이다. 이로 인해 스마트카드 저장정보인 Vi, Bi, Hi, h(y), h(.), b를 추출하고 이전의 로그인메시지 CIDi, Pij, Qi, Ni를 도청했을 때 Ti, Ai, h(b⊕pwi), Bi를 유도하는 취약점을 보완하고 많은 해시함수의 사용으로 계산비용이 효율적이지 못한 점에 중점을 두고 개선하였다.

5.1 스마트카드 분실공격

Lee-Lin Chang's 스킴에서는 제3자가 Pij'=Ti⊕h(h(y) ‖ Na ‖ SIDj)를 계산할 수 있고 Ai'=h(Ti ‖ h(y) ‖ Na)를 계산한다. 연속하여 Qi'와 CIDi'를 계산하

기 때문에 재생공격이나 사용자 위장공격 및 서버 위장공격에 취약하다. 제안 스킴에서 Ui가 스마트 카드를 분실 또는 도난당했을 때 제3자가 패스워드 pwi를 변경하거나 유도하기가 어렵다. 제3자가 스마트카드에 저장된 정보 Bi, Vi, h(.)를 추출할 수 있다고 가정하고 이들 정보로 유효한 로그인 요청 메시지를 위조하기 위해서 유효한 값인 pwi, b, x, y를 획득하기가 어렵다. 사용자 Ui의 올바른 패스워드와 비밀의 수(Nonce) b를 모르고는 Sj로 로그인을 하기위해 스마트카드 소유자로 위장할 수 없다. 이전의 로그인 메시지인 CIDi, Qi, N1, T1이 제3자에 의해 도청되었다 하더라도 Bi가 CIDi, Qi, N1, T1이나 Vi로부터 계산되지 않는다.

5.2 사용자 위장공격

위장공격은 제3자가 프로토콜에 참여하여 자신을 임의의 합법적인 사용자로 가장하는 것으로 이를 위해선 사용자의 비밀의 수 b와 패스워드 pwi를 알아야 한다. 제안 스킴에서 로그인요청 메시지는 CIDi, Qi, N1, IDi, T1으로 Qi=h(b⊕pwi)⊕h(bi)‖T1)=h(b⊕pwi)⊕h(h(SIDj‖h(x‖y)))‖T1), CIDi=h(Vi‖Ni)=h(h(IDi‖h(b⊕pwi)‖h(y))‖N1)로 위장공격을 안전하게 수행하기 위해서는 제3자는 올바른 h(b⊕pwi)와 h(x‖y), h(y)를 추측해야한다.

5.3 서버 위장공격

제3자가 합법적인 서버로 가장하는 것은 불가능하다. 서버 응답메시지 M1'ij, N2, T2는 오직 Sj에 의해서 만 계산된 비밀파라미터 (SSj⊕h(y))를 사용하여 생성되었기 때문에 합법적 사용자로 속이기 위해 시도하기란 불가능하다. 이는 각 서비스지원 서버마다 SSj, SSk와 같이 서로 비밀파라미터의 값이 다르기 때문이다. SSj는 SIDj와 h(x‖y)를 연접한 해시 값이며 각 서버는 h(x‖y)를 구할 수 없다. 또한 클라이언트인 각 사용자에게는 h(y)의 파라미터 값이 주어지지 않았기 때문에 정당한 서버로 위장할 수 없다.

5.4 재생 공격

하나의 세션에서 로그인정보 CIDi, Qi, N1, T1, IDi을 가로채어 보관하다 로그인 정보로 재사용한다고 하면 서비스지원 서버 Sj는 h(b⊕pwi)=Qi⊕h(SSj')‖T1)를 계산할 때 일치하지 않은 정보로 실패한다. 로그인 및 인증단계에서 서로 다른 세션간 Nonce인 N1, N2, Timestamp인 T1, T2는 독립적으로 생성되었다. 때문에 전송된 새로운 메시지의 값으로 재생공격에 실패한다. 그래서 공격자는 합법적인 사용자로 위장하기 위해서는 전에 전송된 메시지를 재전송하여야 하는데 이것은 시스템에 진입할 수 없다.

5.5 패스워드 추측공격

사용자 Ui는 임의로 독립적인 IDi와 pwi를 선택하므로 낮은 엔트로피를 갖는다. 때문에 제3자는 로그인정보와 스마트카드정보를 추출하여 패스워드를 추측할 수 있다. 제안 스킴에서 제3자는 스마트카드정보 Bi,Vi그리고 로그인 메시지 CIDi, Qi, N1, T1를 획득했다 하더라도 Vi, Bi, CIDi, Qi로부터 h(x‖y), h(y)와 b를 알지 못하고서는 pwi를 추측하기 어렵다.

5.6 사용자 익명의 취약성

본 논문에서는 계산비용의 효율성을 증가시키고 스마트카드도난공격으로부터 안전한 인증을 수행하기 위해 파라미터 정보를 간략하게 유지하는 반

면에 사용자의 익명을 다루지 못했다. 대신에 로그인 과정에서 동적으로 생성되는 CIDi와 Qi의 정보를 활용하므로 동적식별자의 개념을 계승하고 있다.

5.7 멀티서버 환경 요구사항 충족

서론의 멀티서버환경에서 원격사용자 인증스킴의 안전성과 효율성의 요구사항에 대한 충족조건의 만족이다. 각 서버는 사용자 인증을 위해 사용한 유일한 파라미터 SSj=h(SIDj ‖ h(x ‖ y))⊕h(y)를 가진다. 그러므로 스마트카드에서 모든 접근 서비스 지원 서버에 대한 비밀 파라미터를 저장할 필요가 없다. 또한 사용자 Ui가 잘못된 패스워드를 입력했을 때 Vi'=h(IDi ‖ h(b⊕pwi))를 계산하여 Vi'=?Vi를 검사함으로써 조기에 패스워드 오류를 검사할 수 있다.

(1) 요구1(단일등록) : Tsaur et al's 스킴과 Xu et al's 스킴에서처럼 RC는 스마트카드정보에 Vij=h(Vi ‖ SIDj)와 같이 서비스지원 서버의 아이디를 포함시킴으로써 또 다른 서비스지원 서버에 접근을 위해서는 등록서버에 다시 등록해야하는 불편이 있다. 제안스킴에서는 Bi=h(b⊕pwi)⊕h(x ‖ y)), Vi=h(IDi ‖ h(b⊕pwi) ‖ h(y))와 같이 서버의 아이디를 포함하지 않음으로 단일등록을 만족시킨다.

(2) 요구2(저비용계산) : Tsaur et al's 스킴과 Xu et al's 스킴에서는 암복호화 함수모듈과 해시연산을 사용하여 계산비용의 비효율을 가져왔다. Lee et al's스킴과 제안스킴에서는 해시함수만 사용하여 계산비용을 높였다. Lee et al's 스킴과 비교해 볼 때 6Th의 연산비용 절감효과를 가져왔다[테이블 5].

(3) 요구3(검증테이블 불사용) : RC는 사용자의 해시된 패스워드를 보유하고 있지 않다. RC는 비밀키 x와 비밀 수 y를 비밀리에 간직하고 있다. 그러므로 도난검증공격(stolen verifier attack)에 안전하다. 또한 서버스서버는 사용자를 인증하기 위해서 유일한 비밀정보 SSj=h(SIDj ‖ h(x ‖ y))⊕h(y)를 사용함으로 스마트카드 메모리에 저장할 필요가 없다.

(4) 요구4(pwi의 임의변경) : 사용자 Ui는 패스워드 변경을 원할 때 서버스지원 서버나 RC의 참여없이 변경할 수 있으므로 효율적이며 편리하다.

(5) 요구5(상호인증과 키 동의) : 사용자 Ui와 서버스지원 서버 Sj간의 상호인증은 RC의 참여없이 각각 세션마다 사용자와 서버가 유효한 개체인지 인증한다. 생성된 세션키는 SKij=h(h(SIDj ‖ SSj⊕h(y)) ‖ N1 ‖ N2)으로 각 세션마다 다른 값이 산출된다.

(6) 요구6(보안성충족) : 멀티서버환경에서 세션키 SKij=h(h(SIDj ‖ SSj⊕h(y)) ‖ N1 ‖ N2)는 제3자에게 알려지지 않은 h(b⊕pwi), h(x ‖ y), h(y)와 연관되어 있다. 이전에 사용된 세션 키가 노출되더라도 임의의 수(Nonce), 타임스탬프가 세션마다 상이하며 단방향 해시함수로부터 이들 파라미터 값을 제3자는 추출할 수 없다.

5.8 보안기능과 계산비용분석

제안 인증스킴과 Lee et al's 스킴에 대한 보안성 기능분석과 계산비용 분석을 Table2~ Table5와 같이 비교하였다. 보안기능분석에서는 제3자에게 스마트카드 도난시 정보유출을 가정하고 로그인 정보를 도청되었을 때를 가정하여 비교하였다.

Lee et al's 스킴의 가장 큰 취약점은 도청된 파라미터 값을 가지고 로그인정보를 합법적인 사용자인 것처럼 생성하여 위장할 수 있다는 것이 가장 큰 취약점이다. 이로 인해 재생공격과 위장공격, 악의적인 서버공격 등 연쇄적으로 취약점이 드러났다.

<Table 2>는 Lee-Lin-Chang's 스킴과 제안스킴을 비교한 보안기능의 차이점으로 RC와 각 서버스 서버들 간의 공유정보가 동일하며 또한 제3자에 의해 로그인 메시지를 도청하고 스마트카드가 도난 되었을 때 합법적인 로그인 메시지를 생성할 수 있는 약점을 가진다.

표 2. 제안스킴과 Lee et al's 스킴의 기능비교
Table 2. Functionality Comparisons of proposed Scheme.

구분	Lee et al's scheme	제안스킴
스마트 카드 도난 공격	·스마트카드정보유출과 로그인메시지 도청시 Ti파라미터 산출로 취약	·스마트카드정보 Bi, Vi, 전송정보 CIDi, Qi에서 pwi와 SSj 생성불가
재생 공격	·제3자는 임의의 Ni'로 로그인 메시지 생성으로 취약	·타임스탬프, Nonce
위장 공격	·로그인메시지 CID'i, P'ij, Q'i, N'i로 위장하여 취약하며 RC와 Sj의 공유비밀정보(h(x‖y), h(y)의 공유로 취약	·h(x‖y), h(b⊕pwi) ·SSj=h(SIDj‖h(x‖y))⊕h(y)는 각 서버마다 상이한 값 유지
패스워드추측 공격	·해시값 h(b⊕pwi)으로 안전	·해시값 h(b⊕pwi)으로 안전
사용자 익명성	·사용자의 식별자보호로 익명성유지	·사용자 익명성 취약

표 3. 제안스킴과 이전 제안 스킴의 기능비교
Table 3. Functionality Comparisons of proposed Scheme and previously proposed scheme.

기능	Sood et al's	Hsiang et al's	Lee et al's	제안스킴
계산비용	high	high	middle	low
단일등록	yes	yes	yes	yes
재생공격	yes	no	no	yes
위장공격	no	no	no	yes
스마트 카드도난 공격	no	no	no	yes
상호인증	no	yes	yes	yes
세션키 동의	no	yes	yes	yes
사용자 익명성	yes	yes	yes	no

<Table 3>는 이전에 발표된 스킴들과 보안기능에 대해 비교하였다. 제안스킴은 스마트카드정보와 로그인 메시지를 통해서 유도되는 파라미터의 값들을 산출하지 못하도록 설계되었다.

표 4. 제안스킴과 Lee et al's 스킴의 연산비교
Table 4. Cost Comparisons of proposed Scheme.

구분	Lee et al's scheme		제안 스킴	
	사용자	서버	사용자	서버
등록단계 연산	1Th	4(RC)Th	1Th	3(RC)Th
로그인 단계연산	7Th		5Th	
인증단계 연산	2Th	9Th	3Th	4Th
세션키 생성연산	1Th	1Th	1Th	1Th
스마트 카드정보	Vi, Bi, Hi, h(y)		Vi, Bi	

<Table 4>와 <Table 5>는 Lee et al's 스킴과 이전에 제안된 스킴들과의 연산비용을 비교하였다. 제안된 스킴의 연산복잡도 분석을 위해 단방향 해시함수 연산시간을 Th로 표기한다. exclusion-OR과 연접(‖)은 아주 적은 연산을 요구하므로 계산비용에 포함하지 않았다.

<Table 4>, <Table 5>에서 Sood et al's스킴과 Hsiang et al's 스킴의 계산비용은 24~25Th로 높게(high), Lee et al's 스킴의 계산비용은 18Th로 중간(middle), 제안 스킴의 계산비용은 12Th로 낮아서(low) 연산효율성에서 가장 높게 평가된다.

표 5.제안스킴과 이전 제안 스킴의 연산비교
Table 5. Cost Comparisons of proposed Scheme and previously proposed scheme.

scheme	login phase	verification phase	total
Sood et al's	7Th	18Th	25Th
Hsiang et al's	7Th	17Th	24Th
Lee et al's	7Th	11Th	18Th
제안	5Th	7Th	12Th

6. 결 론

본 논문에서는 Lee et al's 스킴이 멀티서버 원격 사용자 인증스킴에서 각 서버와 RC의 공유정보인 h(x‖y), h(y)가 동일함으로써 제3자가 스마트카드도난과 로그인 메시지를 도청했을 때 서버위장공격과 악의적인 서버공격에 대해 취약함을 보였다. 이러한 악의적인 공격을 방지하기 위해 각 서버는 RC와 서로 다른 비밀정보(SSj=h(SIDj‖h(x‖y))⊕h(y))를 제공함으로써 재생공격, 서버위장공격, 악의적인 서버공격에 대응할 수 있었다. 본 논문의 장점은 멀티서버환경의 요구조건인 단일등록, 저비용계산, 검증테이블의 불필요, 선택적인 pwi의 변경, 합리적인 상호인증과 키 동의, 보안성충족을 만족시키고 있는 반면 보완할 문제는 사용자의 익명을 위해 수행시간을 줄이면서 비밀파라미터의 보호를 위해 효율적인 설계 메커니즘이 필요하다.

References

[1] L. Lamport, *Password authentication with insecure communication*, Communications of the ACM, Vol. 24, No. 11, pp. 770-772. 1981.

[2] C. Chang, and K.F. Hwang, *Some forgery attacks on a remote user authentication scheme using smart cards*, Informatics Vol. 14, no. 3, pp. 289-294, 2003.

[3] M.L. Das, Saxena, and A. V.P. Gulati, *A dynamic ID-based remote user authentication scheme*, IEEE Trans. Consum. Electron. Vol. 50, no. 2, pp. 629-631, 2003.

[4] C. I. Fan, Y. C. Chan, and Z. K. Zhang, *Robust remote authentication scheme with smart cards*, Computers & Security, Vol. 24, pp. 619-28, 2005.

[5] J. Y. Kim, H. K. Choi, and J. A. Copeland, *Further improved remote user authentication scheme*, IEICE Transaction on Fundamentals, E94-A, pp. 1426-1433, 2011.

[6] S. K. Kim, and M. G. Chung, *More secure remote user authentication scheme*, Computer Communications, Vol. 32, pp. 1018-1021, 2009.

[7] W. C. Ku, and S. M. Chen, *Weakness and improvements of an efficient password based remote user authentication scheme using smart cards*, IEEE Transaction on Consumer Electronics, Vol. 50, pp. 204-207, 2004.

[8] W.S.Juang, *Efficient multi-server password authenticated key agreement using smart cards*, IEEE Trans. Consum. Electron. Vol. 50, No. 1, pp. 251-255, 2004.

[9] Y. P. Liao, and S. S. Wang, *A secure dynamic ID based remote user authentication scheme for multi - server environment*, Computer Standards & Interfaces, Vol. 31, pp. 24-29, 2009.

[10] H. C. Hsiang, and W. K. Shih, *Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment*, Computer Standards & Interfaces, Vol. 31, pp. 1118-1123, 2009.

[11] S. K. Sood, A. K. Sarje, and K. Singh, 2011 *A secure dynamic identity based authentication protocol for multi-server architecture,* Journal of Network and Computer Applications, Vol. 34, No. 2, pp. 609-618, 2011.

[12] W. J. Tsaur, J. H. Li, and W. B. Lee, *An efficient and secure multi-server authentication scheme with key agreement*, The Journal of System and Software, Vol. 85, pp. 876-882, 2012.

[13] C. Xu, Z. Jia, F. Wen, and Y. Ma, *A novel of dynamic identity based authentication scheme for multi-server environment using smart cards*, International Journal of Security and Its Applications, Vol. 7, No. 4, pp. 105-118, July 2013.

[14] M.C. Chuang, and M. Chang Chen, *An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics*, Expert Systems with Applications, Vol. 41, Issue 4, pp. 1411-1418, March 2014.

[15] C.T.Li, C.C.Lee, H.H.Chen, M.J.Syu, and C.C.Wang, *Cryptanalysis of an anonymous multi-server authenticated key agreement scheme using smart cards and biometrics,* Information Networking (ICOIN), 2015 International Conference on, pp. 498-502, Jan 2015.

[16] C. C. Lee, T. H. Lin, and R. X. Chang, *A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards*, Expert Systems with Applications, Vol. 38, pp. 13863-13870, 2011.

[17] C. Xu, Z. Jia, F. Wen, and Y. ma, *A secure and efficient dynamic identity based authentication scheme for multi-server environment using smart cards*, International Journal of Future Generation Communication and Networking, Vol. 6, No. 3, pp. 25-39, June 2013.

멀티서버환경에서 스마트카드를 이용한 동적식별자기반의 원격사용자 인증스킴의 취약성에 관한 연구

신광철

성결대학교 산업경영공학부

요 약

최근 멀티서버 환경에서 동적식별자에 의한 원격 사용자 인증스킴에 중점을 두고 많은 연구가 이루어지고 있다. 합법적 권한이 부여된 사용자들을 위한 용용서버의 접근과 민감정보의 보호를 위해 스마트카드와 생체기반 패스워드 인증 스킴들이 발표되었다. 2011년 Lee-Lin-Chang's는 Hsiang-Shih's 스킴의 취약점을 발견하고 이를 개선한 스킴을 발표했다. 그러나 Lee et al's 스킴에서 스마트카드 도난이나 제3자가 네트워크를 도청했을 때 각종 공격에 취약함을 보였다. 또한 각 서버와 등록센터의 공유정보가 동일하므로 스마트카드 도난공격과 악의적인 사용자공격 및 서버공격(위장공격), 재생공격에 취약하다. 본 논문에서는 사용자가 각 서버 간 분할 등록이 없이 등록센터에 한번 등록만으로 멀티서버에 접근할 수 있도록 설계함으로써 사용자 및 서버 위장공격, 재생공격, 스마트카드 분실공격, 패스워드 추측공격 등에 안전한 향상된 스킴을 제안한다. 단방향 해시함수만을 사용하여 보안성과 편리성, 연산비용에 효율을 높였다.

Kwang Cheul Shin received the bachelor's degree in the department of Computer Science, National University of Science and Technology in 1985. He received the M.S. degree in the department of Computer Science, Korea National Defense University 1990 and the Ph.D. degree in the department of Information and Communication Engineering, Sungkyunkwan University 2003, respectively. He has been a professor in the Division of Industrial & Management Engineering at Sungkyul University since 2004.

E-mail address: skcskc12@sungkyul.ac.kr