Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Vulnerability Analysis on Multi-Server Authentication Scheme using Smart Card and Biometric Data

Kwang-Cheul Shin*

Division of Industrial Management Engineering, Sungkyul University

ABSTRACT

In the past, most of the existing password authentication schemes are based on a single server environment which are inadequate for the multi-server environments. But recently, researches have been performed focusing on the remote user authentication scheme by password and bio-metric data in a multi-server environment. The following study analyzes weaknesses in user Authentication schemes in multiple server environments as suggested by Mishra et al'.s. Over the years, various identifier and password based schemes for multiple server environments have been suggested. However, they have been found of password guessing or dictionary attack based vulnerabilities. In order to overcome such weaknesses, there's been many papers since then that suggested various multiple server verification schemes that utilize biometric data for use in multiple server environments and distributed networks. In order to prevent weaknesses in Mishra et al'.s scheme and Chuang et al'.s scheme, the user verification parameter h(PSK) was utilized to improve upon the weaknesses. However, Mishra et al'.s scheme is vulnerable to user/server spoof attack, denial of service attack, impersonation attack, and man-in-the-middle attack. The following study analyzes C&C scheme and improves it, in order to reanalyze and compare weaknesses and problems to Mishra et al'.s scheme.

KEYWORDS: Key word : Smart card, Biometrics, User/Server impersonation attack, DoS attack

ARTICLE INFO: Received 18 July 2016, Revised 12 August 2016, Accepted 12 August 2016.

*Corresponding author is with the Department of Industrial Management Engineering, Sungkyul University, 53 Sungkyul University-ro Manan-gu, Anyang-si, Gyeonggi-do, 14097, KOREA.

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

1. 서 론

원격지의 응용서버로부터 서비스를 지원받기 위해서는 일반적으로 사용자가 자신의 식별자와 패스워드를 서비스 제공서버에 등록하고 이를 통해서 인증을 진행하여 안전한 서비스를 제공받는 절차로 되어 있다.

이와 같은 패스워드 기반의 사용자 인증방식은 효율성은 높으나 하나의 서버가 공격을 받으면 연쇄적으로 다른 사용자의 식별자와 패스워드가 노출되어 안전성이 취약하다.

이러한 취약성 때문에 각각의 개체들 간의 안전한 통신을 위해서 서로 암호 키가 동일한 대칭키 방식이 사용된다. 그러나 이 방식은 모든 사용자의 식별자와 패스워드를 다중서버환경구조에서 암호화할 경우 키 관리 및 분배의 어려움으로 곤란하다. 반대로 비 대칭키 암호방식이 사용된다면 연산속도 문제가 존재한다. 이러한 문제를 극복하기 위해 다중서버환경에 맞도록 패스워드와 생체정보, 해시함수만을 적용한 스마트카드기반의 패스워드 인증 스킴들이 제안되었다[1][2][3].

그동안 많은 연구가들은 저비용과 효율성이 높은 스마트카드를 이용한 패스워드기반의 인증방식을 제안하였다. 그러나 낮은 보안 엔트로피와 단순한 사전 공격에 쉽게 노출되고 스마트카드에 저장된 정보가 전력소모 분석에 의해 정보가 추출될 수 있는 제약이 존재한다[4][5]. 따라서 다중 서버 환경에서는 스마트카드와 함께 사용자의 생체 인식 및 패스워드를 결합한 인증방식이 제안되었다[6].

지금까지 제안된 다중서버 환경의 인증스킴을 요약해 보면 2004년 Juang[7]은 대칭키 암호시스템을 이용한 다중서버 인증스킴을 제안하였으나 내부자공격에 취약하며 2008년 Tsai[8]는 모든 서버들은 신뢰성 문제로 등록센터를 도입하여 검증테이블을 사용하지 않고 해시함수와 스마트카드를 사용한 인증스킴을 발표했다. 2009년 Liao and Wang[9]은 사용자의 익명성을 보호할 수 있는 동적 ID기반의 원격사용자 인증스킴을 제안했다. 2010년 Yang and Yang[10]은 생체정보를 이용한 다중서버 인증스킴을 제안하였으나 지수연산 수행으로 높은 연산비용을 갖는다. 2011년 Yoon and Yoo[11]의 생체정보기반의 인증키 동의 스킴을 제안하였고 2013년 Wang and Ma[12]의 스마트카드 기반의 인증스킴 등이 제안<표 1>되었다.

표 1. 다중서버 인증 스킴들의 주요 특성요약
Table 1. Summary of the major characteristics and drawbacks of existing multi-server authentication schemes

Scheme	Characteristics	Drawbacks
Juang W. S.	SC, HF	NA
Tsai J. L.	HF	NA
Liao and Wang	HF	SSA, UMA
Yang and Yang	DLP, HF	PIA
Yoon and Yoo	ECC	PIA, SSA, PGA
Chuang and Chang	HF	IA, SSA, MMA

SC:Symmetric Cryptosystem, HF:Hash Function, NA:No Anonymity, SSA:Stolen Smart card Attack, UMA:User Masquerade Attack, DLP:Descrete logarithm Problem, PIA:Privileged Insider Attack, ECC: Elliptic Curve Cryptography, IA:Impersonation Attack, SSA:Server Spoofing Attack, MMA:Man-in-the-Middle-Attack

2014년 M.C. Chuang and M. Chang Chen(이하 C&C)[13]는 D. Yang & B. Yang's 스킴, Yoon-Yoo 스킴의 취약성을 해결하기 위해 다양한 공격을 방지할 수 있는 스킴을 제안했다. 그러나 C&C 스킴은 사용자의 위장공격과 스마트카드 도난공격, 서비스거부(DoS)공격에 취약하다는 것을 Mishra et al's[14] 등이 지적하고 개선된 스킴을 제안했다.

이와 같이 다중서버환경에서 인증스킴들은 일반적으로 재생공격, 위장공격, 스마트카드 도난공격, 서비스거부 공격 등의 취약점을 수정하여 개선된 스킴들을 제안하고 있으나 완전한 해결방안을 제시하지 못하고 있다. 본 논문에서는 C&C 스킴을

분석하고 개선하여 제안한 Mishra et al's 스킴의 취약성과 문제점을 재분석하고 비교한다.

2. 관련연구

2.1 다중서버환경에서의 보안특성

대부분의 전통적인 단일서버 환경의 인증방법에서 사용자들은 다양한 원격 응용서버의 서비스를 제공받기 위해 접속하고자 할 때는 식별자와 패스워드를 사용하고 단일서버는 이들의 식별자와 패스워드를 기억하고 있어야 한다. 이와 같은 비효율과 복잡성은 사용자의 식별자와 패스워드를 쉽게 노출시키며 참여한 멤버들 간에 공유하는 비밀 키 관리가 매우 어렵게 된다. 이와 대조적으로 다중서버 인증스킴<그림 1>은 하나의 신뢰하는 등록센터를 통하여 인증을 위한 사용자등록과 서버등록과 같은 초기화 작업을 한 다음 사용자가 다중 응용서버에 의해 인증이 될 수 있도록 설계되었다.

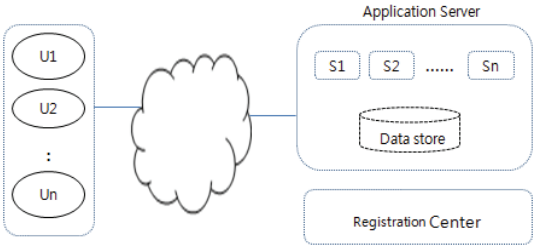

그림 1. 다중서버 인증시스템의 구조
Figure 1. Architecture of a Multi-Server Authentication System

다중서버 환경의 인증시스템은 설계하는 방법에 따라 다양한 형태의 사용자 인증기법들이 있다. 암호알고리즘을 사용하는 방법에 따라 대칭키를 사용하는 방법과 비 대칭키를 사용하는 방법, 해시함수를 사용하는 방법, 혼합사용방법으로 구분할 수 있다. 암호알고리즘을 사용할 경우 키관리와 패스워드관리, 연산량의 증가 등으로 사용하기 곤란하다. 다중서버환경에서는 해시함수와 한 세션동안만 유지되는 대칭키 방식이 안전성측면에서 우수하다고 할 수 있다.

이러한 연구를 바탕으로 다중서버환경에서 인증스킴의 안전성과 효율성에 대한 요구사항은 다음과 같다[7].

- 사용자는 단일등록으로 모든 자원서버에게 접근할 수 있어야 한다.
- 스마트카드는 계산능력의 제한으로 효율적인 연산이어야 한다.
- 각 등록서버는 패스워드 또는 검증테이블을 사용하지 않아야 한다.
- 패스워드는 자유롭게 선택 및 수정할 수 있어야 한다.
- 사용자와 서버 간에 각각 다른 인증을 위해 상호인증과 키 동의가 제공되어야 한다.
- 인증스킴은 현실적으로 발생할 수 있는 다양한 공격을 방지할 수 있어야 한다.

2.2 Mishra et al'.s 등이 분석한 Chuang et al'.s 스킴의 취약성

C&C 스킴은 서로 다른 응용서버의 서비스를 제공받기 위해서 접근할 때 마다 사용자의 식별자를 새롭게 등록해야 하는 단일서버 환경에 대한 설계를 개선하기 위해 제안되었다.

사용자의 패스워드와 생체정보, 스마트카드를 이용하여 익명성을 갖는 다중서버 인증 키 동의 스킴으로 랜덤의 수와 해시함수만을 사용하여 연산비용을 줄인 인증스킴이다.

Mishra et al'.s 는 논문에서 다음과 같은 위협모델을 가정하여 제시하고 있다.

① 제3자는 이미 노출된 정보나 스마트카드로부터 정보를 추출할 수 있다.

② 제3자는 공개채널을 통제하고 있으며 사용자와 서버간의 통신을 도청한다.

③ 제3자는 메시지를 도청, 수정하여 재전송할 수 있다.

④ 제3자는 합법적인 사용자일 수도 있다.

Mishra et al'.s 는 위협모델을 기반으로 C&C 스킴의 취약성을 아래와 같이 지적하고 있다.

• 서비스 거부(DoS) attack

Mishra et al'.s가 지적한 DoS attack의 취약성은 생체정보가 특성상 시간별로 조금씩 차이가 나기 때문에 정확하지 않다는 것이다. 즉, 인증 과정에서 단방향 해시함수의 기본적인 속성상 시간별로 미세한 차이가 있으므로 정당한 사용자는 DoS attack에 직면한다고 지적했다.

• 스마트카드 도난(Stolen smart card) attack

제3자가 사용자의 스마트카드를 획득(또는 훔쳤을 때)했을 때 이전의 세션키를 이용하여 합법적인 사용자로 쉽게 서버로 로긴을 할 수 있다고 지적했다.

• 사용자 위장(User impersonation) attack

제3자는 사용자의 스마트카드가 도난되었다는 가정하에 전력분석공격을 통해 스마트카드의 정보를 추출한 다음 이전의 로긴 메시지정보를 이용해서 합법적인 사용자로 위장할 수 있다고 지적했다.

• 서버 가장(Server masquerade) attack

사용자의 스마트카드를 획득한 것을 가정으로 제3자는 사용자 i와 서버 j간 전송정보를 도청하고 서버로부터 전송된 인증메시지에서 서버의 식별자를 검색한 다음 사용자가 서버에게 로긴정보를 전송할 때 이를 가로채서 서버 j로 가장하는 공격에 취약하다고 지적했다.

3. Mishra et al'.s 스킴의 검토

Mishra et al'.s 등은 C&C 스킴의 결점을 보완하기 위해 2.2절에서 기술한 위협모델을 만족하는 "스마트카드를 이용한 다중서버 환경에서 생체정보를 기반으로 한 사용자 인증스킴" 을 제안했다. 이 스킴은 서버등록단계, 사용자등록단계, 로긴단계와 인증단계, 패스워드 변경단계(생략)에 걸친 5단계로 구성된다. 본 논문에서 사용되는 기호는 <표 2>와 같다.

표 2. 약어표기 및 정의
Table 2. Notations used in this paper

표기	정의
IDi	i번째 사용자 식별자
SIDj	j번째 서버의 식별자
SKab	a와 b의 세션 키
PSK	서버의 Pre-shared key
x	등록센터의 마스터키
Tr	사용자의 등록시간
pwi	i번째 사용자 패스워드
BIOi	i번째 사용자 생체정보
Ni	i번째 사용자 무작위수
Nj	i번째 응용서버 무작위수

3.1 서버 등록단계

이 단계는 <그림 2>와 같이 응용서버들이 사용자들의 서비스를 제공하기 위해 등록센터(이하 RC :Registration Center)에 접속을 요청하고 RC는 RFC2409로 표준화된 IKEv2 (Internet Key Exchange Protocol Version 2) 프로토콜[15]에 의해 PSK(Pre-Shared Key)를 정당한 응용서버에게 제공한다. RC로부터 인증된 응용서버는 사용자의 인증메시지를 확인하기 위해 PSK를 사용한다.

3.2 사용자 등록단계

사용자는 자신들의 식별자(IDi)와 패스워드(pwi)를 가지고 응용서버들이 제공하는 서로 다른 서비스를 접근하기 위해서 RC에 등록을 해야 한다<그림 2>.

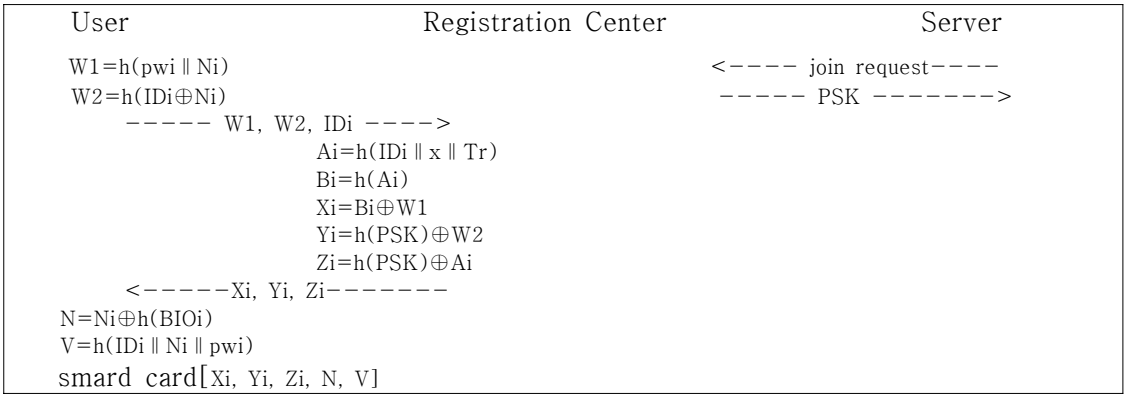

그림 2. 등록단계
Figure 2. Registration Phase

(1) 사용자는 무작위 수 Ni를 생성하고 W1, W2를 연산하여 IDi와 함께 안전한 채널로 RC에 전송한다.

(2) RC는 <W1, W2, IDi>를 수신하여 Ai, Bi, Xi, Yi, Zi를 연산한다.

(3) 연산 후 <Xi, Yi, Zi>를 사용자의 스마트카드(이하 SCi : Smart Card of user i)에 넣어 안전한 채널로 사용자에게 전송한다.

(4) 스마트카드를 수신한 사용자는 생체정보 BIOi를 imprint하여 N과 V를 연산하고 스마트카드를 업데이트<Xi, Yi, Zi, N, V>시킨다.

3.3 로긴 단계

사용자가 서비스제공서버(이하 응용서버)로부터 데이터를 액세스하기를 원할 때 로그인 단계가 실행되며 다음의 과정[그림 3]을 수행한다.

(1) 스마트카드리더기에 SCi를 삽입하고 IDi, pwi, BIOi를 입력하여 Ni와 V'를 생성하고 스마트카드 소유자가 당사자임을 확인한다. V'와 스마트카드에 저장된 V와 비교하여 일치하면 다음 (2) 프로세스를 진행하고 실패하면 세션을 종료한다.

(2) 로긴 메시지를 생성하기 위해 스마트카드의 Bi와 h(PSK)를 추출한다.

(3) 스마트카드는 무작위수 N1을 선택하고 (2)에서 추출한 Bi와 h(PSK)를 이용하여 M1, M2, M3를 계산한다.

(4) 공개채널을 통해 응용서버에게 <M1, M2, M3, Zi>를 전송한다.

3.4 인증 단계

인증단계에서 수행되는 연산은 다음과 같다.

(1) <M1, M2, M3, Zi>를 수신한 응용서버는 Zi와 공유키 PSK로부터 Ai를 연산하고 h(PSK)와 M1으로부터 N1, M2와 h(N1 ‖ Bi)로부터 IDi를 찾아낸다.

(2) 수신한 M3가 h(IDi ‖ N1 ‖ Bi)과 동일하지 않으면 세션을 종료하고 동일하면 다음을 진행한다.

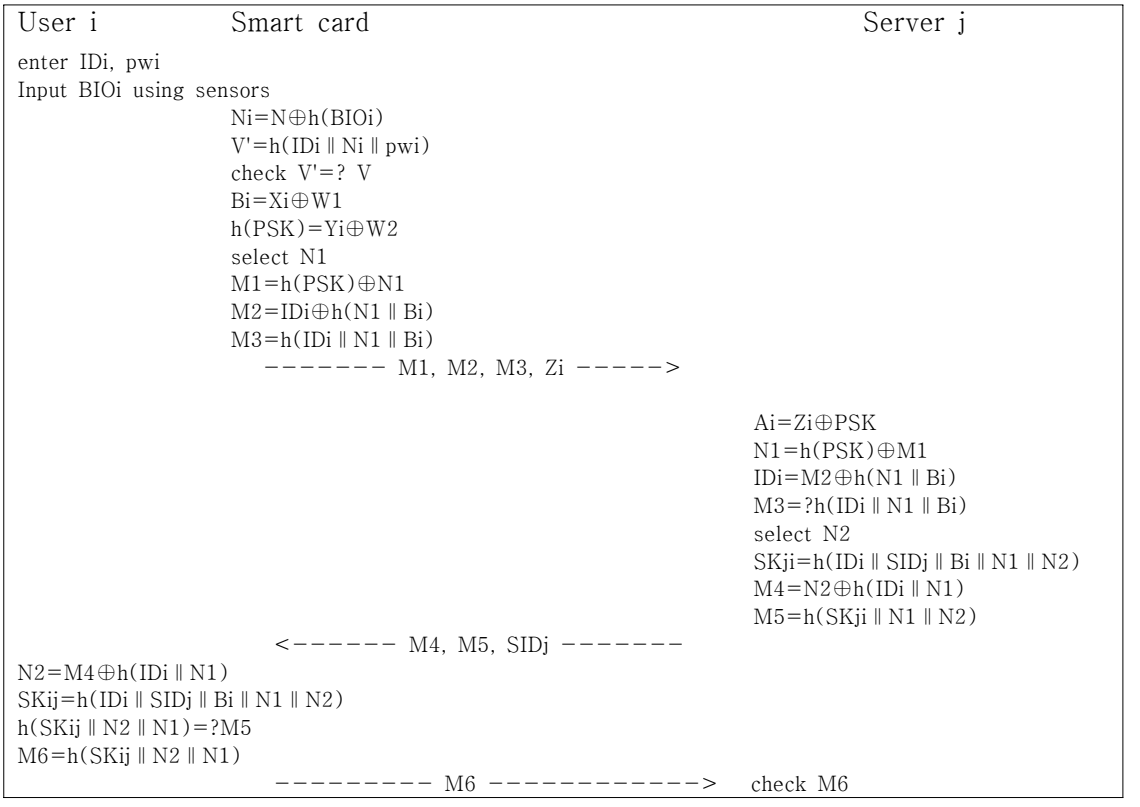

그림 3. 로긴 및 인증단계
Figure 3. Login and Authentication Phase

(3) 응용서버는 랜덤의 수 nonce N2를 선택하고 이후 통신에 사용할 세션키(SKji)를 생성한다.

(4) 응용서버는 M4, M5를 연산하고 자신의 식별자(SIDj)와 함께 사용자에게 전송한다.

(5) <M4, M5, SIDj>을 수신한 스마트카드는 M4로부터 N2를 검색한다. 이후 세션키(SKij)를 연산하고 M5와 h(SKji ‖ N1 ‖ N2)를 연산하여 비교한다. 일치한다면 <M6>를 연산하여 응용서버로 전송한다.

(6) 응용서버는 <M6>를 검증하고 합법적인 사용자로 인증한다.

4. Mishra et al'.s 스킴의 취약성 분석

Mishra et al'.s 등은 Chuang et al'.s 등이 발표한 사용자의 패스워드와 생체정보를 이용한 다중서버 인증스킴의 취약성인 사용자 위장(impersonation)공격, 서버 위장(impersonation)공격과 서비스거부(DoS)공격 등을 개선하여 제안하였다.

그러나 Mishra et al'.s 스킴은 등록센터에서 발급하는 공유키(PSK)가 등록하는 모든 서버에게 제공되기 때문에 사용자 및 서버위장공격과 서비스거부공격, 중간자(man-in-the-middle)공격, 가장(Masquerade)공격의 다양한 취약점이 발견되었고 또한 이로 인하여 파생되는 재생(replay)공격, 익명성(anonymity)의 문제가 도출되는 취약함을 증명한다.

4.1 서버 위장(impersonation)공격

서버 위장공격은 일종의 스푸핑(spoofing)공격으로 합법적인 서버가 제3의 서버(adversary)로 위장하는 것이다. 정당하게 등록된 제3의 서버는 공통의 공유 비밀 키 PSK를 사용하여 다른 서버 또는 합법적 사용자로 위장 할 수 있다.

제3의 서버(adversary)는 RC에 등록된 합법적 SIDx로 다른 서버(SIDj)로 스푸핑할 수 있다. 모든 서비스제공 응용서버들은 RC에서 제공된 공통의 비밀키(PSK)를 공유하고 있다. 따라서 SIDx는 제3의 서버 역할을 하기 위한 다음과 같은 위장공격이 가능하다.

① 사용자 i는 로긴메시지<M1, M2, M3, Zi>를 서버 j로 전송할 때 제3의 서버(SIDx)는 메시지를 차단하고 가로채서 다음과 같은 연산이 가능하다.

Ai=PSK⊕Zi

N1=h(PSK)⊕M1

IDi=M2⊕h(N1 ‖ Bi)

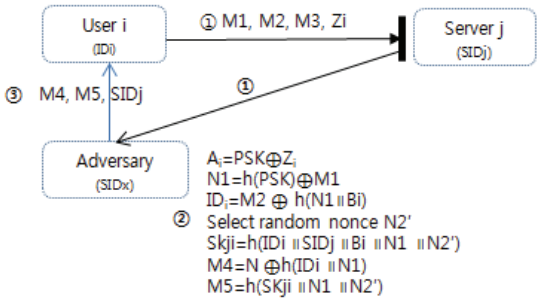

그림 4. 서버 위장공격 시나리오

Figure 4. Server impersonation attack scenario

② 제3의 서버는 무작위 수 N2'를 선택하여 세션키(SKji), M4, M5를 연산한다. 세션키 생성에서 자신의 식별자 대신 SIDj로 대체하여 생성한다.

SKji=h(IDi ‖ SIDj ‖ Bi ‖ N1 ‖ N2')

M4=N2'⊕h(IDi ‖ N1)

M5=h(SKji ‖ N1 ‖ N2')

③ 제3의 서버는 <M4, M5, SIDj>를 사용자 i에게 전송한다.

④ 사용자 i는 메시지<M4, M5, SIDj>를 수신하지만 SIDx의 위장공격을 인식하지 못하고 상대가 SIDj로 인식하여 세션키 SKij를 생성한다.

4.2 사용자 위장(impersonation)공격

정당하게 등록된 서버 SIDx는 사용자 i와 이전의 통신정보를 이용하여 제3의 사용자(adversary) 역할을 할 수 있다.

제3의 사용자인 SIDx는 사용자 i로 위장하여 서버 j를 완벽하게 속일 수 있다.

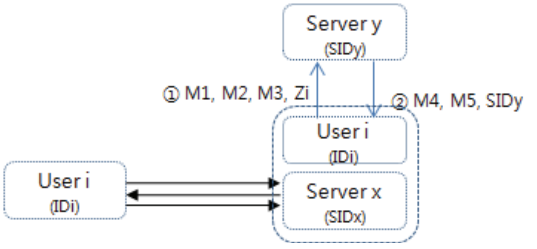

그림 5. 사용자 위장공격 시나리오

Figure 5. User impersonation attack scenario

SIDx는 이전의 통신에서 IDi=M2⊕h(N1 ‖ Bi)와 Zi를 이용하여 사용자 i가 생성하는 동일한 로그인 메시지를 작성할 수 있다.

SIDx는 무작위 수 N1'를 선택하여 유효한 로그인 요청 메시지를 다음과 같이 생성한다.

M1=h(PSK)⊕N1'

M2=IDi⊕h(N1' ‖ Bi)

M3=h(IDi ‖ N1' ‖ Bi)

① 생성된 메시지 <M1, M2, M3>는 Zi와 함께 인증을 위한 공개 채널을 통해 합법적인 서버 y에 전달된다.

② 서버 y는 제3의 서버인 SIDx가 생성한 로그인 정보를 사용자 i의 로그인 정보로 간주하여 <M4, M5, SIDy>를 SIDx에게 전송함으로써 세션을 성립시킨다.

Ai=PSK⊕Zi

N1'=h(PSK)⊕M1

IDi=M2⊕h(N1' ‖ h(Ai))

random nonce N2선택

SKyi=h(IDi ‖ SIDy ‖ Bi ‖ N1 ‖ N2)

M4=N2⊕h(IDi ‖ N1)

M5=h(SKyi ‖ N1 ‖ N2)

4.3 중간자(Man-in-the-middle)공격

Mishra et al'.s는 스킴에서 이 공격에 안전하다고 주장했으나 통신을 연결하는 두 개체 사이에 중간자인 제3의 서버가 침입한다면 통신 내용을 도청, 조작이 가능하다.

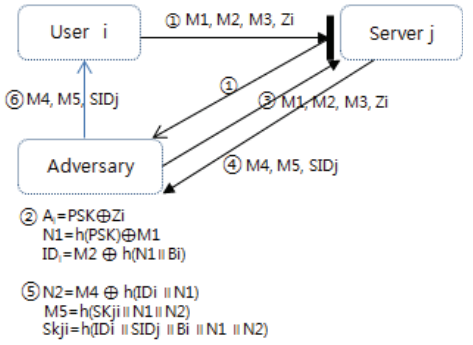

그림 6. 중간자공격 시나리오
Figure 6. Man-in-the-middle attack scenario

두 개체(사용자 i와 서버 j)는 상대방과 세션이 연결되었다고 생각하지만 실제로 두 개체는 중간자에게 연결되어 있으며 중간자가 사용자 i에서 전달된 정보를 도청 및 조작한 후 서버 j로의 전달이 가능하다.

① 사용자 i는 인증을 위해 로긴메시지 <M1, M2, M3, Zi>를 서버 j로 전송할 때 제3의 서버는 이 메시지를 차단, 도청한다.

② 제3의 서버는 정당하게 등록된 서버로 PSK를 공유하고 있다. 따라서 제3의 서버는 PSK를 사용하여 식별뿐만 아니라 사용자의 난수 N1을 추출한다.

Ai=PSK⊕Zi

N1=h(PSK)⊕M1

IDi=M2⊕h(N1 ‖ Bi)

③ 제3의 서버는 서버 j에게 메시지 <M1, M2, M3, Zi>를 전송한다.

④ SIDj는 난수 N2를 생성하고, 메시지 <SIDj, M4, M5>를 사용자에게 전송한다.

⑤ 제3의 서버는 메시지를 가로채서 서버가 생성한 N2(=M4⊕h(IDi ‖ N1))를 추출한다. 이 정보를 사용하여 제3의 서버는 세션키(SKji=h(IDi ‖ SIDj ‖ Bi ‖ N1 ‖ N2))를 생성한다.

⑥ 사용자 i는 제3의 서버와 동일한 세션키 SKji를 생성한다. 이와 같이 제3의 서버는 사용자 i와 서버 j의 세션키를 보유하게 된다.

4.4 서비스거부(DOS) 공격

Mishra et al'.s 스킴은 로그인 메시지에 대해 실시간으로 생성된 정보인지를 판단할 수 있는 새로운 메시지(신선성)에 대한 질문을 하지 않는다. 또한 RC로부터 연산된 Ai 값을 체크하지 않는 것도 문제이다.

제3의 서버는 이전의 채널에서 로긴 메시지 <M1, M2, M3, Zi>를 획득한다.

① 제3의 서버는 메시지 수정없이 <M1, M2, M3, Zi>를 대량 복사해서 서버 j로 전송한다.

② 서버 j는 <M1, M2, M3, Zi>를 수신하지만 새로 작성된 메시지인지 확인과정이 없다. 또한 연속되는 수신메시지가 동일한 메시지인지 확인하는

과정이 없다.

Ai=Zi⊕PSK

N1=h(PSK)⊕M1

IDi=M2⊕h(N1 ‖ Bi)

M3=?h(IDi ‖ N1 ‖ Bi)

select N2

SKji=h(IDi ‖ SIDj ‖ Bi ‖ N1 ‖ N2)

M4=N2⊕h(IDi ‖ N1)

M5=h(SKji ‖ N1 ‖ N2)

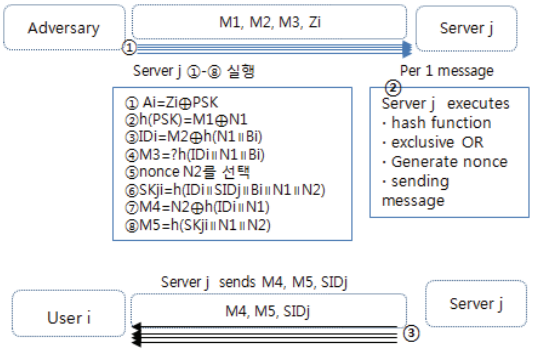

그림 7. 서비스거부 공격 시나리오

Figure 7. Denial of Service attack scenario

서버 j는 1회의 로긴 메시지에 대해 연산과정은 해시함수 6번 수행, ⊕연산 4번, 랜덤넘버 1회생성이 포함되어 있다. 제3자가 가로챈(intercept)메시지를 동시에 다수를 사용한다면 서버나 네트워크 자원을 사용할 수 없도록 만들기 위해 시도할 수 있다.

③ 서버 j는 M4, M5, SIDj를 사용자 에게 전송한다.

이와 같이 Mishra et al's 스킴은 서버 j가 사용자 i로부터 인증메시지의 신선성을 검사하지 않는다. 제3자가 서버 j에 대해 가로챈 메시지를 보냈을 때 서버 j는 이 메시지가 과거데이터인지 현재데이터인지 알 수가 없다. 이것은 또한 재생(reply) 공격으로부터도 자유롭지 못하다.

4.5 가장(Masquerade) 공격

제3자는 사용자 i가 로긴을 위해 서버 j로 전송하는 메시지를 차단, 도청하여 또 다른 서버 k와 연결시켜 사용자 i는 원하지 않는 서버 k와 세션을 연결시켜도 사용자 i는 알아채지 못한다.

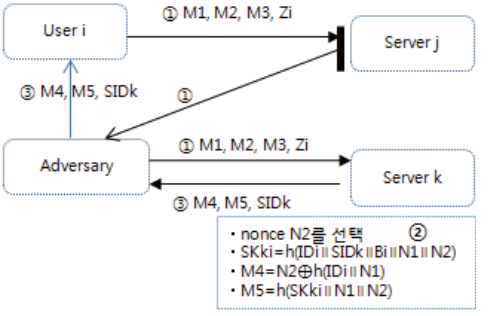

그림 8. 가장공격 시나리오

Figure 8. Masquerade attack scenario

① 사용자 i가 서버 j에게 로긴을 할 때 서버 j로 메시지 <M1, M2, M3, Zi>를 보낸다. 제3의 서버는 로긴 메시지를 가로챈 후 다른 서버 k에게 그대로 전송한다. 이것은 로긴 메시지에 수신하는 개체인 서버 j에 대한 어떤 정보도 포함되어 있지 않기에 가능하다. [그림 8]의 ② ③에서 서버 k는 공격에 대한 의심 없이 M4, M5, SKki를 연산하고 인증된 메시지< M4, M5, SIDk>를 제3의 서버에게 보낸다. 제3의 서버는 사용자 i에게 메시지를 그대로 전송시킨다. 사용자 i는 서버 j에 대한 SIDj를 체크하지 않는다.

④ 사용자 i는 <M4, M5, SIDk>를 수신하여 N2를 연산하고 세션키 SKki=h(IDi ‖ SIDk ‖ Bi ‖ N1 ‖ N2)를 생성한다.

세션 키를 생성 후 수신된 데이터 M5와 h(SKki ‖ N2 ‖ N1)를 비교하면 일치되므로 원하지 않는 서버 k와 세션이 성립된다.

4.6 분석결과

• Mishra et al'.s의 위협모델에 대한 만족도

Mishra et al'.s 는 2.2 절에서 언급한바와 같이 논문에서 위협모델을 가정하여 제시하였다. 본 논문에서 분석한 결과 Mishra et al'.s 스킴은 2.2 절의 ①에서 제3자가 스마트카드를 획득했을 때 스마트카드로부터 정보를 추출한다고 해도 스마트카드 발급 후 사용자의 생체정보와 패스워드를 이용하여 N과 V를 갱신했으므로 소유자의 생체정보를 모르고는 사용할 수 없다. 그러므로 ①은 만족시키고 있으나 ②③④는 4장 취약성 분석에서와 같이 만족하지 못한다.

• 본 논문에서 분석한 Mishra et al'.s 스킴의 특징

Mishra et al'.s 등은 C&C 스킴의 서버/사용자 위장공격과 중간자공격, 서비스거부공격과 스마트카드 도난공격에 대한 취약성을 보완하기 위해 스마트카드를 자신의 생체정보와 패스워드를 사용하여 갱신(N, V)하고 RC로부터 발급된 SCi의 정보 중 h(PSK)를 사용하여 서버와 인증할 수 있는 파라미터를 추가하였다. 이 외에 사용자의 로긴 메시지와 서버의 인증메시지의 내용에는 다소 차이가 있으나 C&C와 Mishra et al'.s의 기법은 유사하다. 그 결과 4장에서 Mishra et al'.s 스킴을 분석한 결과를 요약하여 <표 3>에 나타냈다.

C&C는 제안논문에서 RC의 overhead를 최소화하였고 다중서버환경에 맞는 스킴이면서 또한 최소의 연산비용으로 여러 공격을 저지할 수 있는 고효율의 보안성을 갖는 안전한 원격사용자 인증 스킴을 제안했다고 주장했다.

표 3. 안전성 재분석 결과
Table 3. The Reanalysis result of security properties

security components	C&C scheme analysis	Mishra et al'.s reanalysis for C&C scheme	Mishra et al'.s scheme analysis	Reanalysis result for Mishra et al'.s scheme
Resist server impersonation	Yes	No	Yes	No
Resist user impersonation	Yes	No	Yes	No
Resist masquerade attack	–	–	–	No
Resist man-in-the-middle attack	Yes	No	Yes	No
Resist DoS attack	–	No	Yes	No
Resist stolen smart card attack	Yes	No	Yes	Yes
User anonymity	Yes	Yes	Yes	No
Resist reply attack	Yes	Yes	Yes	No
Mutual authentication	Yes	Yes	Yes	Yes
Session key agreement	Yes	Yes	Yes	Yes

C&C는 [표 3] 이외에도 조기에러탐지, 오프라인 패스워드 공격 저지, 안전한 패스워드 선택과 변경, 생체정보 템플릿 보호 등에서 안전하다고 주장했다. 그러나 Mishra et al'.s 은 C&C 스킴을 재분석한 결과 사용자/서버 위장공격, 가장공격, 서비스거부공격, 중간자공격 등에서 취약하다고 분석하고 이 스킴을 개선하여 발표하였다. 그러나 본 논문에서 Mishra et al'.s 스킴을 재분석한 결과 4장에서와 같이 사용자/서버 위장공격, 가장공격, 서비스거부공격, 중간자공격, 스마트카드 도난공격에 취약함을 증명하였다.

5. 결 론

최근 인터넷과 같은 다중서버구조에서의 사용자 인증은 필수적이다. 그러나 그동안 연구되어온 인증스킴들은 공통적으로 다중서버 환경에서 필수적인 보안의 특성들은 고려하지 않으므로 해서 제3자에 의한 위장공격, 서비스거부공격, 재생공격, 가장공격, 중간자공격에 취약하다. 본 논문은 Mishra et al'.s 등이 제시한 생체정보기반의 인증스킴에서 노출될 수 있는 보안 취약점을 다중서버환경에서 보안의 특성들을 고려하여 분석하였다.

Mishra et al'.s 등의 스킴은 위의 대표적인 공격에 대한 취약성 노출을 본 연구에서 밝혀냈다. 향후 이러한 취약점을 보완하기 위해서

• 로긴메시지의 신선성을 검사하는 프로토콜을 추가하여 서비스거부공격, 재생공격, 가장공격을 방지할 수 있다.

• 상호인증을 위한 인증정보(식별자)를 추가하여 정당한 개체인지를 검사할 수 있는 스킴을 설계한다.

• 위장공격, 중간자공격을 피하고 완전 전방향 비밀을 보장하기 위해 통신메시지로부터 세션키를 추측할 수 없도록 해야 한다.

References

[1] 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.

[2] 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.

[3] Kwang-Cheul Shin, *A study on weakness of a secure dynamic identify based remote user authentication scheme for multi-server environment using smart card*, Journal of Knowledge Information Technology and Systems(JKITS), Vol. 10, No. 5, pp. 523-536, Oct. 2015.

[4] P. Kocher, J. Jaffe, and B. Jun, *Differential power analysis,* in *Advances in Cryptology—RYPTO '99*, Lecture Notes in Computer Science, Springer, Berlin, Germany, pp. 388–97, 1999.

[5] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, *Examining smart-card security under the threat of power analysis attacks, IEEE Transactions on Computers*, Vol. 51, No. 5, pp. 541–52, 2002.

[6] C. T. Li, and M. S. Hwang, *An efficient biometrics-based remote user authentication scheme using smart cards*, Journal of Network and Computer Applications, Volume 33, Issue 1, pp. 1–5, Jan. 2010.

[7] W. S. Juang, *Efficient multi-server password*

authenticated key agreement using smart cards, Consumer Electronics, IEEE Transactions on, Vol. 50, No.1, pp. 251−.255, 2004.

[8] J. L. Tsai, *Efficient multi-server authentication protocol based on one-way hash function without verification table,* Computers & Security, Vol. 27, No. 3, pp. 115−121, 2008.

[9] Y. P. Liao and S. S. Wang, *A secure dynamic ID based remote user authentication scheme for multi-server environment, Computer Standards and Interfaces*, Vol. 31, No. 1, pp. 24−29, 2009.

[10] D. Yang, and B. Yang, *A biometric password-basedmulti-server authentication scheme with smart card,* in *Proceedings of the International Conference on Computer Design and Applications (ICCDA '10)*, Vol. 5, pp. 554−59, Qinhuangdao, China, Jun. 2010.

[11] E.-J. Yoon, and K.-Y. Yoo, *Robust biometrics-based multiserver authentication with key agreement scheme for smart cards on elliptic curve cryptosystem,* The Journal of Supercomputing, Vol. 63, No. 1, pp. 235−55, 2013.

[12] B. Wang, and M. Ma, *A smart card based efficient and secured multi-server authentication scheme*. Wireless Personal Communications, Vol. 68, No. 2, pp. 361-378, 2013.

[13] M. C. Chuang, and M. C. Chen, *An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics*, *Expert Systems with Applications*, Vol. 41, No. 4, pp. 1411−418, 2014.

[14] D. Mishra, A. K. Das, and S. Mukhopadhyay, *A secure user anonymity-preserving biometricbased multi-server authenticated key agreement scheme using smart cards,* Expert Systems with Applications, Vol. 41, No. 18, pp. 8129−8143, 2014.

[15] C. Kaufman, *Internet key exchange* (ikev2) protocol, 2005.

스마트카드와 생체정보를 이용한 다중서버 인증스킴의 취약성 분석

신광철

성결대학교 산업경영공학부

요 약

과거에는 대부분의 패스워드 인증스킴들이 다중서버 환경에는 부적합한 단일서버환경에 기반을 두고 있었다. 그러나 최근에는 멀티서버 환경에서 패스워드와 생체정보에 의한 원격 사용자 인증스킴에 중점을 두고 많은 연구가 이루어지고 있다. 본 논문에서는 Mishra et al'.s 가 제안한 다중서버 환경에서 사용자 인증스킴의 취약점을 분석한다. 그동안 식별자 및 패스워드기반의 다중서버 환경에 대한 스킴들이 많이 제안되었으나 패스워드추측공격과 사전공격 등으로 안전성에 취약성이 발견되었다. 이와 같은 취약성을 극복하기 위하여 다중서버환경과 분산네트워크에서 사용될 수 있는 생체정보를 이용한 다중서버 인증스킴을 제안한 이래 많은 연구가 이루어져 왔다. Mishra et al'.s 스킴은 Chuang et al'.s 스킴의 취약점을 방지하기 위해 사용자 인증 파라미터 h(PSK)를 사용하여 개선하였다. 그러나 Mishra et al'.s 스킴은 사용자/서버 위장공격, 서비스거부공격, 가장공격과 중간자공격에 취약하다. 본 논문에서는 C&C 스킴을 분석하고 개선하여 제안한 Mishra et al'.s 스킴의 취약성과 문제점을 재분석하고 비교한다.

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