Journal of Knowledge Information Technology and Systems(JKITS), Vol. 14, No. 5, pp. 479~489, October 2019
https://doi.org/10.34163/jkits.2019.14.5.005

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Remote Mutual Authentication Scheme for Anonymity and Un_Traceability Based on Biometric Information Using Public Key Cryptography

Kwang-Cheul Shin*

Division of Industrial Management Engineering, Sungkyul University

ABSTRACT

The growth of Internet technology is providing high quality contents for users to access conveniently. It has been a growing number of application servers to provide services to users. These services are provided through insecure public channels. It is vulnerable to blocking, modification and deletion of transmission information by third parties. Therefore, a mutual authentication mechanism is required to securely communicate between the user and the server. Mechanism is a way for a user to access a remote application server to establish mutual authentication and session key with the server. It is used to combine biometrics and passwords to enhance the security of the authentication scheme. In many studies, authentication schemes have designed the protocol to resist threats by using the characteristics and advantages of hashing bio, public key and secret key cryptography. However, it can be seen that most proposed authentication schemes had limitations in designing perfect security. This paper briefly reviews the proposed schemes. In addition, the proposed scheme prevents the exposure of anonymous and traces in the authentication process and solves the problem of user/server impersonation attack. To improve the scheme, we propose a hashing bio-based authentication and key agreement scheme in a single server using public key cryptography.

KEYWORDS: Public key cryptography, Mutual authentication, Impersonation attack, Biometric information, Smart card, Anonymity, Un_traceability

ARTICLE INFO: Received 25 August 2019, Revised 25 September 2019, Accepted 11 October 2019.

*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

인터넷에서 안전하고 효율적인 통신을 위해서는 당사자(개체)간의 인증 및 키 동의 프로토콜의 설계가 중요하다. 이 프로토콜은 단일서버인증(의료정보시스템, 온라인거래 시스템), 다중서버인증(전자상거래, 종합정보시스템), IoT(가전 홈텍스) 환경에서 주로 설계되는 중요한 메커니즘이다[1].

인증수단에는 세션마다 새로운 비밀번호를 사용하는 OTP, 공인기관에서 발급한 공인인증서, 거래변경 때마다 난수를 적용하는 보안카드, 키나 비밀정보를 안전하게 보관하고 키 생성과 전자서명이 가능하도록 구현된 HSM(Hardware Security Module), 휴대폰 번호를 통한 즉시 인증할 수 있는 SMS, 복제 및 해킹방지를 위한 신체의 일부를 정보로 이용하는 바이오인증 등이 있다.

단일서버 또는 다중서버의 안전한 인증 및 키 동의 프로토콜은 지난 2005년 이후 14년간 해시함수와 공개키 암호(RSA, ECC), 비밀키암호를 이용한 인증프로토콜이 다수 제안[2]되었으며 그 결과 <그림 1, 2>와 같이 인증방식의 설계와 이에 따른 위협요소, 구현모델의 틀에서 보편화된 연구가 이루어졌다. 연구에 의하면 인증방식(scheme)은 인증모델에 따라 생체인식기반 인증(voice, fingerprint, iris), 요소기반 인증(2-factor, 3-factor), ID 및 패스워드기반 인증(원격사용자 인증, 다중서버 원격사용자 인증), 채널기반 인증방식(전자투표, 전이인증)이 연구되어 왔으며 위협요소는 신원기반공격(위장공격, 위조공격, 재생공격 등), 도청기반공격(사전공격, 추적공격, 도청공격), 서비스기반공격(DoS/ DDoS), 조작기반공격(중간자공격)으로 분류하고 있다.

최근 연구되어온 인증스킴들을 살펴보면 2015년 Lu et al.'s[3]는 Arshad et al.'s[4]스킴이 오프라인 패스워드 추측공격이 취약하다고 분석하고 생체정보를 사용하여 Biohashing을 채택함으로써 모듈러 지수 및 타원 곡선 점 곱셈과 비교할 때 매우 효율적이고 계산복잡도를 줄이고 있다. K. C. Shin[5]는 Lu et al.'s 스킴이 익명성과 위장공격의 취약성, 그리고 합법적인 사용자가 시스템을 사용하는 모든 사용자들에 의해 안전하지 않음을 논리적으로 입증하였다.

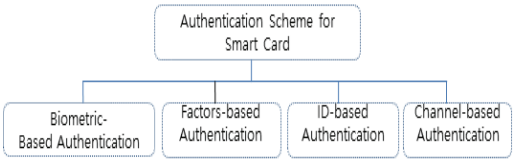

그림 1. 스마트카드 기반 인증스킴 분류
Fig 1. Classification of authentication scheme

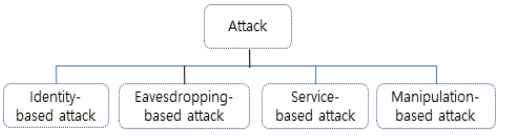

그림 2. 위협모델의 분류
Fig 2. Classification of threat models

2014년 Huang et al's[6]는 익명성인증을 위해 RSA를 사용하여 타임스탬프 기반의 2-요소 원격사용자인증 프로토콜을 제안하였다. 또한 Amin et al.'s[7]은 Huang et al.'s의 제안이 위장공격, 패스워드 추측 및 내부자공격에 취약하며 패스워드 변경 단계에서 오류가 있음을 증명하고 RSA기반의 인증 및 키 동의 메커니즘을 제시하였다. Amin et al.'s 스킴은 2018년 Xu et al.'s[8]등이 분석한 결과 완전한 순방향 보안이 보장되지 않고 사용자 추적 가능과 사용자 위장공격에 취약함을 지적하고 ECC를 사용하여 등록센터를 둔 다중서버 2-factor 인증방식을 제안하였다.

2015년 Li et al.'s[9]은 완벽한 순방향 비밀, 도난 스마트카드공격, 패스워드 추측공격, 위장공격, 내부자공격에 안전한 스킴을 제안하였고 2017년 Srinivas et al.'s[10]에 의해 Li et al.'s 스킴의 주장

을 반박하면서 연산시간과 통신비용을 줄이는 2-요소 인증스킴의 멀티서버구조를 제안하였다.

최근 Chaudhry et al.'s[11]는 스마트카드를 기반으로 한 Islam et al.'s[12] scheme은 사용자 위장 및 서버 위장 공격에 취약하다고 지적하고 이를 해결하기 위해 타원 곡선 암호화를 기반으로 한 향상된 방식을 제시했다.

2017년 Qui et al.'s[13]는 Chaudhry et al.'s의 오프라인 암호, 공격, 사용자/서버 가장 공격 및 MITM(Man-in-Middle) 공격의 위협을 구분하여 개선된 인증 스킴을 제시하였다.

이와 같이 그동안 제안된 공통적인 스킴들의 특성은 인증스킴에 대한 구현시나리오(인증모델정의, 위협모델정의, 스킴설계, 보안분석 및 평가)에 따라 완전한 보안의 안전성을 주장하지만 다른 제안자에 의해 취약점이 노출됨을 알 수 있다. 이것은 다양한 위협모델에 맞추어 스마트카드 기반의 인증스킴을 설계하는데 완벽한 보안에 한계가 있다는 것이다.

<표 1>에서 다중서버 환경에서 사용자는 여러 서버와의 상호작용이 필수이므로 서로 다른 식별자와 패스워드를 사용하는 것은 번거롭다. 이 문제 해결을 위해 인증스킴에서 등록센터(Registration Center)의 활용이 매우 효과적이며 원격 의료정보 시스템과 같은 환자와 의사간의 인증은 단일서버 인증스킴이 효율적이다.

암호기법으로 ECC는 RSA암호방식의 대안으로 적은 비트수의 암호키로 동일한 보안성능을 나타내므로 많이 선호하고 있으나 하드웨어 성능향상으로 효율적인 알고리즘에 중점을 두고 있다. 또한 Diffie-Hellman 키교환방식을 사용한 [9, 10]은 지수연산문제로 속도의 지연을 보인다. 본 논문에서는 지금까지 많은 스킴들[3, 8-11, 13]은 시나리오에서 항상 몇 가지의 위협에 노출됨을 알 수 있으며 공통적인 취약점인 익명성의 노출을 방지하고 오프라인 패스워드 추측공격과 사용자 위장공격의 문제를 해결하기 위해 RSA를 이용한 단일 서버에서의 바이오해싱 기반 인증 및 키 동의 스킴을 설계한다. 본 논문의 구성은 다음과 같다. 2장에서는 생체정보기반의 공개키암호 인증스킴을 제안한다. 3장에서 제안시스템의 안전성, 4장에서 효율성에 대한 분석을 한 다음 5장에서 결론을 맺는다.

2. 생체정보기반 제안스킴

본 논문에서는 익명성과 불 추적성, 사용자/서버 위장공격에 안전한 스킴 설계로 생체정보와 공개키 암호를 사용한 상호인증과 키 동의 스킴을 제

표 1. 비교스킴의 특성
Table 1. Properties of comparison scheme

Scheme	인증요소	암호기법	인증서버	통신횟수	등록센터(RC)
Lu et al.'s[3]	BIO-based	Biohashing	단일서버인증	3	없음
Qui et al.'s [13]	Database	ECC	단일서버인증	3	없음
Chaudhry et al.'s [11]	2-factor	ECC	단일서버인증	2	없음
Amin et al.'s[8]	Nonce-based	RSA	단일서버인증	3	없음
Li et al.'s [9]	Nonce-based	D-H 키교환	다중서버인증	3	사용
Srinivas et al.'s [10]	Self-verifier, password-based	D-H 키교환	다중서버인증	3	사용

안한다. 새로운 사용자는 먼저 서버에 등록을 완료하고 SC(스마트카드)를 발급받으면 합법적인 사용자로 서버와의 인증을 통해 세션을 설정할 수 있다.

제안스킴은 등록단계, 로그인단계, 인증단계로 구성되며 사용되는 약어에 대한 기술은 <표 2>와 같다.

2.1 가정

• 제3자의 공개키도용을 고려하여 서버 S는 합법적인 신뢰된 사이트이다.

• 사용자와 서버 간에 상호인증은 각각 서로 다른 파라미터에 의해 이루어지고 키 동의가 제공되어야 한다.

• 인증스킴은 현실으로 발생할 수 있는 다양 한 공격을 방지할 수 있어야 한다.

• 제3자는 공개채널을 통해 메시지 내용을 도청, 삭제, 수정 및 재전송 할 수 있다.

• 제3자는 악성장치를 통해 스마트카드의 정보를 획득할 수 있다.

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

기호표기	정의
U, S	사용자, 서버
ID_i, pw_i, Bio_i	i의 식별자, 패스워드, 생체정보
e	public key of S
d	private key of S
SC	smart card
p	1024비트 소수
⊕, ‖	Exclusive-or 연산, 연접

2.2 등록단계

1) U_i는 <그림 3>과 같이 식별자 ID_i와 패스워드 pw_i를 입력하고 임의의 난수 r을 선택하여 $pwr_i=h(pw_i \| r)$를 계산한다. 자신의 생체정보 BIO_i를 장치를 통해 추출하여 해시값으로 만든 다음 안전한 매체를 통해 서버 S_j에 등록요구 메시지 $\{ID_i, h(BIO_i), pwr_i\}$를 전송한다.

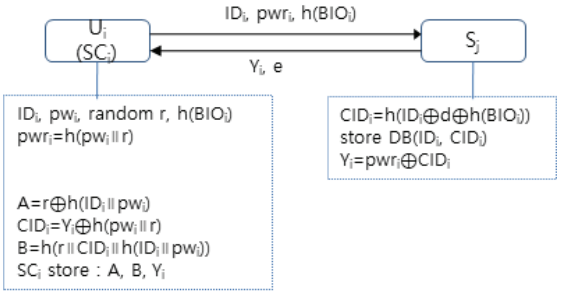

그림 3. 제안하는 스킴의 등록과정
Fig 3. Registration phase of proposed scheme

2) 사용자 U_i로부터 요청 메시지 $\{ID_i, h(BIO_i), pwr_i\}$를 수신하면 S_j는 $CID_i=h(ID_i \oplus d \oplus h(BIO_i))$, $Y_i=pwr_i \oplus CID_i$을 계산하여 새로운 카드 SC에 내용 $\{Y_i, e\}$를 저장하고 U_i로 보낸다. 서버 S_j는 신규 등록하는 사용자의 데이터베이스에 식별자 ID_i와 CID_i를 저장한다.

3) 사용자 U_i는 $\{Y_i, e\}$를 수신하여 $A=r \oplus h(ID_i \| pw_i)$와 $CID_i=Y_i \oplus h(pw_i \| r)$를 구하고 $B=h(r \| CID_i \| h(ID_i \| pw_i))$을 계산하여 SC_i에 A와 B, Y_i를 저장한다. 최초 임의의 난수 r은 U_i 자신을 증명하기 위해서만 사용하는 A와 CID_i를 계산하기 위해서 Y_i를 SC에 저장한다.

2.3 로그인 및 인증단계

등록된 스마트카드를 소유한 합법적인 사용자는 로그인 메시지를 생성하여 서버 S_j로 전송하는 과정[그림 4]이다. 사용자와 서버는 서로 상호인증하고 세션 키를 설정한다.

1) S_j와의 세션을 시작하기 위해 U_i는 SC_i를 카드

판독기에 삽입하고 ID_i 및 pw_i를 포함하여 로그인 세부 사항을 입력하면 $r=A\oplus h(ID_i \| pw_i)$을 계산하고 SC_i 소유자임을 증명하기 위해 $Y_i\oplus h(pw_i \| r)$을 이용하여 CID_i를 구한다. 그 다음 $h(r \| CID_i \| h(ID_i \| pw_i))$을 계산하여 SC_i내의 B와 비교하여 값이 틀리면 세션을 종료시킨다. 그렇지 않으면 세션 키 생성을 위한 파라미터 random N_1, 타임스탬프 T_i을 선택하고 생체정보 BIO_i를 입력하여 $L_i=(ID_i \| N_1 \| h(BIO_i))^e \bmod n$을 계산한 다음 공개채널을 통해 $\{L_i, T_i\}$를 S_j로 전송한다.

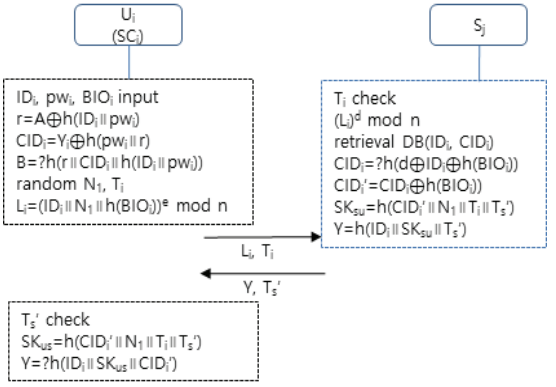

그림 4. 제안하는 스킴의 인증과정
Fig 4. Authentication phase of proposed scheme

2) U_i로부터 로그인 요구를 수신하면 S_j는 현재 타임스탬프 T_s에 대응하는 타임스탬프 T_i를 검증 $(T_s-T_i\le\triangle T)$한다. 타임스탬프 T_i가 유효하다면 다음 단계들을 계속 실행하고 그렇지 않으면 세션을 중단한다. 그 다음 S_j는 ID_i, N_1, $h(BIO_i)$를 얻기 위해 L_i를 해독$((L_i)^d \bmod n)$하고 데이터베이스에서 사용자의 식별자 ID_i에 대응하는 CID_i를 검색한 후 $h(d\oplus ID_i\oplus h(BIO_i))$를 구하여 CID_i와 일치여부를 비교한다. $CID_i=?h(d\oplus ID_i\oplus h(BIO_i))$와 같이 일치하면 사용자가 정당함을 인증한다. 일치하지 않으면 세션은 거절된다.

3) 인증이 완료되면 S_j는 위장된 서버가 아님을 증명하기 위해 $CID_i'=CID_i\oplus h(BIO_i)$를 계산한다. 타임스탬프 T_s'를 선택한 다음 세션키 $SK_{su}=h(CID_i' \| N_1 \| T_i \| T_s')$를 생성하고 사용자에게 S_j가 합법적임을 증명하기 위해 $Y=h(ID_i \| SK_{su} \| T_s')$를 계산하여 U_i에게 $\{Y, T_s'\}$을 전송한다.

4) S_j로부터 응답 메시지를 받으면 SC_i는 T_s'의 유효성 검증$(T_i'-T_s'\le\triangle T)$을 마친 후 SC_i는 약속된 세션키 $SK_{us}=h(CID_i' \| N_1 \| T_i \| T_s')$를 생성한 다음 $Y=?h(ID_i \| SK_{us} \| CID_i')$를 비교하여 일치하면 U_i는 S_j가 정당함을 인증하고 세션이 성립된다.

3. 제안스킴 안전성 분석

제안된 스킴의 안전성은 <표 1>에서 보는바와 같이 [3, 8-11, 13]에서 취약한 부분인 익명성 및 불 추적성, 사용자/서버 위장공격, 상호인증, 순방향 비밀성보장, 스마트카드 도난공격 등을 중점적으로 분석하여 <표 3>에 요약하였다.

3.1 상호인증

S_j는 로긴 메시지의 해독 결과인 파라미터(ID_i, N_1, $h(BIO_i)$)를 가지고 $h(d\oplus ID_i\oplus h(BIO_i))$를 계산하여 DB의 CID_i와 일치성 비교로 검증하고 사용자는 서버로부터의 검증파라미터 Y와 $h(ID_i \| SK_{us} \| CID_i')$의 일치여부로 서버가 합법적임을 인증하도록 설계되었다. 서버 S_j에 의한 사용자의 합법성여부는 서버의 비밀키 d에 의해 복호화된 인증파라미터 ID_i, N_1, $h(BIO_i)$에 의해 실현되며 서버 S_j의 DB에 저장된 CID_i와 비밀키 d가 포함된 해시값 $h(d\oplus ID_i\oplus h(BIO_i))$의 일치성으로 사용자를 인증하게 된다. 사용자가 정당한 서버인지를 인증하기 위해서는 CID_i'를 정확하게 계산할 수 있는지의 여부이다. CID_i는 서버의 DB에 보유하며 정당한 서버만이 $h(BIO_i)$를 추출함을 의미한다. 서버에서 전송된 Y와

사용자가 생성한 $h(ID_i \| SK_{us} \| CID_i')$의 일치성으로 서버가 정당함을 인증한다.

3.2 사용자 익명 및 불 추적성

제안스킴에서는 ID_i가 로그인과정에서 평문으로 전송되지 않고 $\{L_i, T_i\}$는 사용자의 식별자와 임의 난수, 해시된 생체정보가 서버의 공개키로 암호화 $((ID_i \| N_1 \| h(BIO_i))^e \bmod n$)되어 있다. 제3자는 L_i로부터 식별자를 검색하지 못하며 SC_i도 사용자의 식별자를 보유하지 않으므로 로긴 메시지를 식별할 수 없다. 타임스탬프 T_i는 매번의 세션마다 시스템 시간이 다르므로 세션마다의 고유한 로그인 메시지가 보장된다. 제3자는 각 세션마다의 추적이 불가능하며 식별자 익명성이 보호된다.

3.3 효율적인 로그인 검사

다음과 같이 스마트카드 SC_i는 입력의 정확성을 식별 할 수 있다. 사용자가 패스워드(pw_i)와 식별자(ID_i)중 어느 하나라도 잘못 입력했을 때 SC_i는 $h(ID_i \| pw_i)$의 값을 계산하고 $r(=A \oplus h(ID_i \| pw_i))$를 추출하여 SC_i의 $B(=?h(r \| CID_i \| h(ID_i \| pw_i)))$와 비교한다. 비교한 값이 다르면 식별자 자신의 인증이 실패되어 세션을 종료시킴으로써 효율적인 로그인 단계를 갖는다.

3.4 스마트카드 도난공격

스마트카드를 사용자가 분실했거나 제3자가 훔쳤을 때 정보의 유출로 인해 악의적인 공격이 있을 수 있다. 제3자는 차분공격이나 전력분석을 통해 스마트카드내 $\{Y_i, A, B\}$를 추출해 유용한 로그인 메시지의 생성을 시도할 수 있다. 그러나 유효한 로그인 메시지를 작성하려면 사용자의 식별자(ID_i)와 패스워드(pw_i), 생체정보(BIO_i)를 포함하는 $CID_i(=h(ID_i \oplus d \oplus h(BIO_i)))$를 계산할 수 있어야 한다. 제3자가 스마트카드 소유자의 식별자 ID_i를 알고 있다고 해도 생체정보 BIO_i를 알지 못하면 로긴 메시지 L_i를 생성할 수 없다. 만약 제3자가 임의의 BIO_i'로 위장했을 때 서버에서 생성하는 CID_i와 일치되지 않으므로 거절된다. 또한 스마트카드의 패스워드를 추측하기 위해 사전공격을 시도한다. 패스워드는 다음 값 $Y_i=h(pw_i \| r) \oplus CID_i$, $A=r \oplus h(ID_i \| pw_i)$, $B=h(r \| CID_i \| h(ID_i \| pw_i))$들과 관련되어 있다. 식 B를 사용하여 패스워드를 확인하려면 r과 CID_i를 알아야 하며 $CID_i=Y_i \oplus pwr_i$에서 r을 알지 못하고는 패스워드를 확인할 수 없다.

$r=A \oplus h(ID_i \| pw_i)$이므로 r을 검색하기 위해서는 사용자 식별자 ID_i와 pw_i가 필요하다. 스마트카드나 전송 된 메시지에는 사용자의 신원 정보가 포함되어 있지 않으므로 패스워드 추측 공격에 안전함을 보여준다. 무엇보다 제안된 스킴에서 패스워드는 3.1.3에서와 같이 정당한 SC의 소유자 인증에 한정되어 사용되기 때문에 중요한 파라미터는 아니며 위협을 하려면 합법적 사용자의 생체인식정보인 BIO_i 필요하다.

3.5 사용자 위장공격

제3자는 재생공격으로 합법적 인 사용자로 위장하여 서버에 로그인 할 수 있다. 제3자는 임의의 값으로 유효한 로그인 메시지 $\{L_i', T_E\}$를 생성하려고 할 것이다. 랜덤 값 r_E, 타임스탬프 T_E 생성 후 $L_i'=(ID_i \| r_E \| h(BIO_E'))^e \bmod n$을 시도한다. 이와 같이 L_i'를 계산하려면 제3자가 합법적 사용자의 식별자 ID_i와 생체정보 $h(BIO_i)$를 알고 있어야 한다. 그러나 권한이 없는 사용자는 다음 사실 때문에 L_i'를 계산할 수 없다. 제3자가 L_i'를 계산하기 위해서 서버 DB의 사용자정보 CID_i를 해킹했다고 하더

표 3. 보안특징(속성) 비교
Table 3. Comparison of security features

	Lu et al.'s [3]	Qui et al.'s [13]	Chaudhry et al.'s [11]	Admin et al.'s [8]	Li et al.'s [9]	Srinivas et al.'s [10]	Proposed scheme
s1	×	√	√	×	×	×	√
s2	√	√	×	×	×	×	√
s3	√	√	×	√	√	√	√
s4	√	×	√	√	√	√	√
s5	√	×	×	√	×	√	√
s6	√	√	√	√	√	√	√
s7	√	√	√	×	√	√	√
s8	×	×	×	√	×	√	√
s9	×	×	×	×	×	×	√

* √:공격에 안전, ×: 공격에 취약
s1: 익명성 및 불추적성, s2: 사용자위장공격,
s3: 서버위장공격, s4: 재생공격, s5: 중간자(도청, 수정)공격, s6: 상호인증, s7: 순방향 기밀성,
s8: 서비스거부공격, s9: 스마트카드 도난공격

라도 사용자 ID_i와 서버의 비밀키 d, 사용자의 생체정보 BIO_i가 해시값으로 저장되어 합법적사용자의 생체정보를 도출해 낼 수 없다. 만약 제3자가 임의 BIO_E'를 선택하여 사용할 경우 서버의 검증과정 CID_i=?h(ID_i⊕d⊕h(BIO_E'))에서 일치하지 않으므로 거절된다. Y_i에서 CID_i를 검색하려면 패스워드 (pwr_i=h(pw_i ‖ r))가 필요하다. 패스워드와 임의의 수 r은 처음 등록할 때 사용된 이후 로그인 메시지 생성이나 인증정보를 생성할 때는 더 이상 사용되지 않으므로 제3자는 CID_i를 얻을 수 없다. 이는 제안된 스킴이 사용자 위장 공격에 강력함을 보여준다.

3.6 사용자 위장공격

제3자가 서버로 위장하여 서버의 인증메시지 {Y, T_s}를 조작하거나 생성하여 인증메시지로 보내올 때 메시지의 확인과정에서 정당한 서버가 아님을 증명하는 시나리오이다.

사용자 U_i가 로그인 메시지 {L_i, T_i}를 서버에 전송하면 제3자는 메시지를 가로 채고 유효한 메시지로 응답을 시도할 수 있다. 그러나 제3자는 다음과 같이 정당화 된 유효한 사용자를 위장 할 수 없다.

첫째 제3자는 Y를 생성하기 전에 CID_i'를 계산하여야 하는데 서버의 데이터베이스로부터 사용자의 CID_i를 도용하였다 해도 사용자의 생체정보인 BIO_i를 생성할 수 없다. 즉 제3자의 서버 위장을 방지하기 위해 합법적인 서버만이 생성할 수 있도록 알고리즘에 CID_i'를 추가하였다. 정당한 서버만이 CID_i'를 합리적인 세션키 SK_{su}를 생성할 수 있고 응답메시지 Y를 계산할 수 있다.

둘째 제3자는 이전에 전송 된 메시지 {Y, T_s}를 사용자에게 응답하려고 시도 할 수 있다. 그러나 이전의 무작위수와 타임스탬프가 포함된 SK_{su}= h(CID_i'⊕N_1⊕T_i⊕T_s)와 Y=h(ID_i ‖ SK'_{su} ‖ T_s)가 해시값으로 계산되어 현재의 타임스탬프로 수정할 수가 없다. 이는 제안 된 스킴은 서버위장공격을 거부한다는 것을 나타낸다.

3.7 완전 순방향 기밀성

일반적으로 전방향 또는 순방향 기밀은 서버의 세션키가 노출되어도 다음 세션에서 안전성에 영

향을 미칠 수 없어야 하는 성질로 RSA방식에서 제3자는 도청공격을 통해 트래픽을 가로채서 송수신 데이터를 찾아낼 수 없다. 사용자/서버의 해시된 출력인 $SK=h(CID_i \| N_1 \| T_i \| T_s)$가 손실되어도 제3자가 추측할 수 없다. 더욱이 각 세션마다 키를 보장하기 위해 서로 다른 타임스탬프를 포함하므로 이전의 세션키가 손실되어도 다음의 세션키는 생성에 필요한 파라미터 N_1, T_i, T_s가 다시 생성되므로 안전함을 의미한다.

4. 제안스킴 효율성 분석

이 절에서는 공개키 암호를 사용한 제안 인증프로토콜의 효율성과 다른 스킴들과의 특성을 비교한다. e, L_i, n이 모두 1024 비트이고 식별자 ID_i, 패스워드 pw_i, 임의 수 r, 타임스탬프 T_i, 생체정보 BIO_i의 함수출력 크기는 128비트를 기준으로 한다. 시간복잡도는 Te(모듈러 지수연산 실행 시간), Tpm(포인트 곱셈연산 실행시간), Tpa(모듈러 역 연산의 실행시간), Th(해시 연산의 실행시간)로 정의하고 일반적인 관계는 Te〉 Tpm〉 Tpa〉 Th로 표현하고 XOR 연산과 서버에서의 해시함수연산은 무시한다[14].

표 4. 암호연산시간[15]
Table 4. The time of executing cryptographic operations[15]

Symbol	Te	Tpm	Th	Tpa
User/Client	380ms	130 ms	1ms	100ms
Server	3.16ms	1.17ms	0.01ms	0.1 ms

<표 4>와 같이 D. He 스킴[14]에서 실험한 결과에 의하면 각각 Tpa, Tpm, Tme 및 Th는 클럭 속도 36MHz의 Philips Hiper-smart 카드와 클럭 속도 3GHz의 서버 측 펜티엄 IV 프로세서에서 100ms/0.1ms, 130ms/1.17ms, 380ms/3.16ms 및 1ms/0.01ms 걸리는 실행 시간을 나타낸다.

제안된 기법에서는 로그인 단계에서 $h(pw_i \| ID_i)$, pwr_i, B, L_i를 계산하고 검증 단계에서 $(L_i)^d \bmod n$, CID_i, SK_{su}, Y, SK_{us}를 계산한다. 따라서 로그인 단계의 계산 오버 헤드는 5Th + 1Te이고 인증 단계는 4Th + 1Te이다.

<표 5>에서와 같이 Li et al.'s , Srinivas et al.'s의 Diffie-Hellman 키교환 방식의 이산대수 연산과 Chaudhry et al.'s의 타원곡선 암호방식을 사용한 스킴에서의 계산 overhead가 774ms로 가장 높음을 알 수 있다. Lu et al.'s , Qui et al.'s 스킴은 지수연산이 포함되지 않은 포인트 곱셈연산만을 사용하여 270ms로 계산 overhead를 단축시켰다. [8]의 제안스킴에서 분석한 Amin et al.'s 스킴의 계산복잡도는 7.723ms로 사용자 측의 연산시간을 배제하고 서버의 암호연산시간만을 적용하였기 때문에 오차가 있다.

제안스킴에서는 RSA 공개키 암호를 사용하여 사용자와 서버측에서 1회씩의 암복호화에 필요한 지수연산을 사용하여 388ms로 분석되었다. 제안 된 스킴은 익명과 추적불능의 프라이버시를 보호하고 사용자/서버의 위장공격과 스마트카드 도난공격 및 서비스 거부 공격에 보안의 안전성을 만족시키고 관련 스킴과의 통신 및 계산 오버 헤드 측면에서 효율적이다.

<표 6>은 제안 스킴에 대해서 등록센터를 사용하지 않는 단일서버 원격 사용자 인증으로 공개키 암호와 함께 생체정보를 기반으로 설계한 것으로 바이오 해싱만의 인증기법이 효율적이나 RSA를 대체하여 사용한 ECC기법으로 사용하여 효율성을 향상시켰어도 서버신뢰를 가정했을 때 공개키암호인 RSA를 사용하여도 안전성과 효율성에 큰 차이가 없었고 로그인과 인증과정의 메시지 통신횟수를 2회로 줄였다.

표 5. 계산복잡도 비교
Table 5. Comparison of computation complexity

	Lu et al.'s [3]	Qui et al.'s [11]	Chaudhry et al.'s [9]	Amin et al.'s [6]	Li et al.'s [7]	Srinivas et al.'s [8]	Proposed scheme
User	8Th+2Tpm	8Th+2Tpm	5Th+4Tpm+1Tpa	1Te+9Th	2Te+8Th	2Te+8Th	1Te+5Th
Server	4Th+2Tpm	5Th+2Tpm	4Th+3Tpm+1Tpa	1Te+6Th	2Te+5Th	2Te+4Th	1Te+4Th
Complexity	≈270	≈270	≈628.85ms	≈392ms	≈774ms	≈774ms	≈388ms

표 6. 제안스킴의 특성
Table 6. Properties of comparison scheme

Scheme	인증요소	암호기법	인증서버	통신횟수	등록센터(RC)
Proposed scheme	Biohashing	RSA	단일서버인증	2	없음

5. 결 론

사용자와 원격서버간의 상호인증은 스마트카드 기반의 인증을 위주로 여러 위협요소에 맞추어 메커니즘이 설계, 구현되었다. 사용자에게 편리한 인증 메커니즘을 설계하기 위해서는 단일서버와 다중서버환경에서 역할에 맞게 등록센터(신뢰센터)의 역할을 필요로 한다. 또한 효율적인 인증을 위해 스킴에 맞는 생체정보, 식별자, 넌스, 패스워드 등의 인증파라미터를 사용하며 암호의 강도와 연산시간을 고려한 다양한 암호기법을 사용한다. 스마트카드는 집적회로가 내장되어 저장, 계산, 데이터의 암복호화 등의 기능을 갖추므로 금융기관, 의료기관 등의 응용프로그램에서 많이 사용된다. 또한 지문, 홍채 같은 생체인식의 특성은 일반적으로 고유하며 중복되거나 분실의 우려가 없으므로 사용자인증을 위한 좋은 방법이다.

본 논문에서는 생체정보 기반의 단일서버환경에서 공개키를 사용하여 인증 및 키동의 메커니즘의 제안으로 잘못된 입력을 신속하게 탐지 할 수 있는 효율적인 로그인 단계를 유지하며 익명성과 불추적성, 사용자/서버 위장공격 등 방지에 효과적으로 설계된 스킴이다.

안전성과 효율성 분석을 통해 제안 된 기법은 RSA기반 공개키암호 인증기법을 사용하여 일반적인 위협요소를 방지하고 통신 및 계산 오버 헤드 측면에서 비교할 수 있음을 보여주었다.

References

[1] K. Sambasiva Rao, and M. Kameswara Rao, *A lightweight digital signature generation mechanism for authentication of IoT devices*, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Vol. 7, Issue 6, Mar. 2019.

[2] M. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, *Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research Issues"*, arXiv:1803.10281v1 [cs.CR], pp. 1-50, Mar. 2018.

[3] Y. Lu, L. Li, H. Peng, and Y. Yang, *An enhanced biometric-based authentication scheme for telecare medicine information*

system using elliptic curve cryptosystem, Journal of Medical Systems, Vol. 39, No. 32, pp. 1-9, Feb. 2015.

[4] H. Arshad, and M. Nikooghadam, *Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems*. J. Med. Syst. Vol. 38, No. 12, pp. 1-12, 2014.

[5] K. C. Shin, *A study on design of robust remote user authentication scheme with enhanced for anonymity and confidentiality,* Journal of Knowledge Information Technology and Systems(JKITS), Vol. 14, No. 1, pp. 11~24, Feb. 2019.

[6] H-F. Huang, H-W. Chang, and P-K. Yu. *Enhancement of timestamp-based user authentication scheme with smart card*. Int. J. Netw. Secur. pp. 463-467, 2014.

[7] R. Amin, T. Maitra, D. Giri, and P. D. Srivastava, *Cryptanalysis and improvement of an RSA based remote user authentication scheme using smart card*. Wirel. Pers. Commun. pp. 4629–4659, 2017.

[8] G. Xu, S, Qiu, H. Ahmad, G. Xu, Y. Guo, M. Zhang, and H. Xu, *A multi-server two-factor authentication scheme with un-traceability using elliptic curve cryptography*, Sensors (Basel). 2018 Jul 23;18(7). pii: E2394. doi: 10.3390/s18072394.

[9] X. Li, J. Niu, S. Kumari, J. Liao, and W. Liang, *An enhancement of a smart card authentication scheme for multi-server architecture.* Wirel. Pers. Commun. pp. 175-192, 2015.

[10] J. Srinivas, S. Mukhopadhyay, and D. Mishra, *A self-verifiable password based authentication scheme for multi-server architecture using smart card.* Wirel. Pers. Commun. pp. 6273–6297, 2017.

[11] S. A. Chaudhry, H. Naqvi, T. Shon, M. Sher, and M. S. Farash, *Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems*, J. Med. Syst., April, Vol. 39, No. 6, pp. 1-11, 2015.

[12] S. Islam, and M. Khan, Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems. J. Med. Syst. 38(10):135, 2014.

[13] S. Qiu, G. Xu, H. Ahmad, and L. Wang, *A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems*, IEEE Access, Vol. 6, pp. 7452-7463, Mar. 2018.

[14] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, *A study \of the energy consumption characteristics of cryptographic algorithms and security protocols*. IEEE Trans. Mob. Comput. Vol. 5, No. 2, pp. 128-143, 2006.

[15] D. He, *An efficient remote user authentication and key agreement protocol for mobile client-server environment from pairings,* Ad Hoc Netw., August, Vol. 10, No. 6, pp. 1009-1016, 2012.

공개키암호를 이용한 생체정보기반의 익명과 불추적성을 위한 원격 상호인증 스킴

신광철

성결대학교 산업경영공학과 교수

요 약

인터넷 기술의 발전은 양질의 컨텐츠를 편리하게

사용자들이 접할 수 있도록 제공하고 있다. 사용자들에게 서비스를 제공하기 위한 많은 응용서버들이 증가되어 왔다. 이러한 서비스는 안전하지 않은 공개채널을 통해 제공되므로 제3자에 의한 전송정보의 차단, 수정, 삭제에 취약하다. 그러므로 사용자와 서버 간에 안전하게 통신할 수 있는 상호인증 메커니즘이 필수적으로 되었다. 메커니즘은 원격 응용서버에 접근하려는 사용자가 서버와 상호인증 및 세션 키를 설정하는 방식이다. 인증스킴의 보안을 강화하기 위해 생체인식과 패스워드를 결합하는 방식이 주로 사용된다. 그동안 많은 연구에서 인증방식은 해싱바이오, 공개키 및 비밀키 암호의 특성과 장점을 이용하여 위협요소에 저항할 수 있는 프로토콜을 설계하였다. 그러나 대부분의 제안된 인증스킴들은 완벽한 보안을 설계하는데 한계가 있었음을 알 수 있다. 본 논문에서는 지금까지 제안된 스킴들을 간략히 살펴본 다음 인증과정에서 익명과 추적의 노출을 방지하고 사용자/서버 위장공격의 문제를 해결한다. 이를 위해 공개키 암호를 이용한 단일 서버에서의 바이오해싱 기반 인증 및 키 동의 스킴을 제안한다.

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