ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

보안성이 향상된 퍼지추출 기술 기반 사용자 인증 및 키 동의 스킴☆

Security Enhanced User Authentication Scheme with Key Agreement based on Fuzzy Extraction Technology

최 윤 성[1] 원 동 호[2*]
Younsung Choi Dongho Won

요 약

정보기술과 네트워크 기술의 발전에 따라 멀티미디어 시스템을 이용한 다양한 서비스들이 인터넷을 통해서 제공되고 있다. 하지만 이러한 인터넷 기술의 근본적 특징인 개방성 때문에 네트워크를 기반으로 하는 시스템에서는 데이터 보호 기술과 안전하게 사용자를 인증하는 기법을 제공해야만 한다. 그래서 Das, An 그리고 Li&Hwang 과 같은 다양한 연구자들은 스마트카드, 패스워드, 그리고 생체정보를 기반한 사용자 인증 스킴을 제안하였으나, 다양한 보안 취약점이 발견되었다. 이러한 문제를 해결하기 위해 Li 등은 퍼지추출 기술을 활용한 새로운 인증 스킴을 제안하였으나, 그들의 스킴도 여전히 off-line password attack, authentication without biometrics, denial-of-service, insider attack 등의 보안 문제점을 가지고 있었다. 그래서 본 논문에서는 Li 등이 제안한 사용자 인증 스킴의 보안 문제점을 해결할 수 있는 보안성이 향상된 퍼지추출기술 기반의 사용자 인증 및 키 동의 스킴을 제안한다.

☞ 주제어 : 사용자 인증 스킴, 생체정보, 퍼지추출기법

ABSTRACT

Information and network technology become the rapid development, so various online services supplied by multimedia systems are provided through the Internet. Because of intrinsic open characteristic on Internet, network systems need to provide the data protection and the secure authentication. So various researchers including Das, An, and Li&Hwang proposed the biometric-based user authentication scheme but they has some security weakness. To solve their problem, Li et al. proposed new scheme using fuzzy extraction, but it is weak on off-line password attack, authentication without biometrics, denial-of-service and insider attack. So, we proposed security enhanced user authentication scheme with key agreement to address the security problem of authentication schemes.

☞ keyword : User authentication scheme, biometrics, fuzzy extraction

1. 서 론

최근 인터넷 기술이 성장함에 따라 복수의 서버로 구성된 멀티 시스템을 이용하여, 다양한 멀티미디어 서비스가 제공되고 있다. 사용자는 한 번의 인증을 통해 다양한 서버의 서비스를 모두 사용할 수 있기 때문에, 이러한 멀티서버를 통한 서비스에 대한 인증은 단일서버 서비스보다 높은 수준의 보안이 제공되어야 한다. 또한 네트워크를 기반으로 동작하는 원격 응용 서비스에서 디지털 정보에 대한 보호가 중요한 이슈가 되고 있다[1,2].

Lamport는 1981년에 통신내용이 공격자에 의해 노출될 수 있는 네트워크 통신에서 사용할 수 있는 패스워드 기반의 인증 스킴을 처음으로 제안하였다. 하지만 이 스킴은 서버가 패스워드 테이블을 저장해야 하는 구조를 가지고 있어서, stolen-verifier attack에 취약하다는 심각한 문제가 있었다. 이러한 문제를 해결하기 위해서 다양한 연구자들이 보안성이 향상된 패스워드 기반의 인증 스킴을 제안하였으나, 패스워드만을 이용한 기법은 기본적으

[1] Department of Cyber Security, Howon University, 64 Howon University 3Gil, Impi-Myeon, Gunsan-Si, Jeonrabuk-Do 54058, Republic of Korea
[2] Department of Computer Engineering, Sungkyunkwan University, Suwon-si, Gyeonggi-do, 16419, Republic of Korea
* Corresponding author (dhwon@security.re.kr)
[Received 24 August 2015, Reviewed 2 September 2015(R2 21 December 2015, R3 2 March 2016), Accepted 10 March 2016]
☆ 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. R0126-15-1111, 클라우드 보안을 위한 위험기반 인증·접근제어 프레임워크 및 보안상태 점검기술 개발)
☆ 본 논문은 DigitalSec 2014에서 발표한 논문을 확장한 버전임

로 dictionary attack에 취약하다는 문제점이 발생하였다. 이를 해결하기 위해, 연구자들은 패스워드와 생체정보를 결합하여 보안성이 향상된 서버용 사용자 인증 스킴을 제안하였다. Hwang 등은 ElGamal 방식 기반의 스마트카드를 이용한 원격 사용자 인증 스킴을 제안하였고 Kim 등은 스마트카드와 사용자의 지문을 이용한 ID 기반의 패스워드 인증 스킴을 제안하였다. 그리고 Lin과 Lai는 멀티미디어 시스템을 위한 지문정보를 기반으로 한 사용자 인증 스킴을 제안하였다. Yang과 Yang 그리고 Yoon과 Yoo는 멀티서버 시스템을 위한 생체정보 기반의 사용자 인증 시스템을 제안하였다. Yang과 Yang의 스킴은 지수승 계산이 포함되어 있어서 높은 수준의 컴퓨팅 능력을 필요로 한다. 그리고 He는 Yoon과 Yoo가 제안한 스킴이 insider attack, masquerade attack, 그리고 stolen smart card attack에 취약하다고 분석하였다. 이러한 문제를 해결하기 위해서 Chuang과 Chen은 스마트카드와 사용자 패스워드, 생체정보를 기반으로 하는 멀티 서버용 익명 사용자 인증 스킴을 제안하였다[3,4]. Li 등과 Das는 Li와 Hwang가 제안한 스킴이 설계적 오류가 있으며 보안적 문제점이 있다고 지적하였다. An은 2012년에 Das의 스킴의 보안적 문제점들을 분석하고 보안성을 향상시킨 사용자 인증 스킴을 제안하였다[5]. Li 등은 이러한 An의 스킴을 분석하여 다양한 보안적 문제점을 지적한 후, 이런 문제를 해결할 수 있는 키 동의 스킴을 제안하였으나 여전히 보안적 문제점을 가지고 있다[6]. 본 논문에서는 Li 등의 스킴이 off-line password attack, authentication without biometrics, denial-of-service, insider attack에 취약하다는 것을 보이고 이를 해결하기 위해 퍼지추출기술 기반의 안전한 사용자 인증 및 키 동의 스킴을 제안한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서 본 논문을 이해하는데 필요한 연구에 대해 알아본 후, 3장에서 Li 등이 제안한 스킴을 설명하고 스킴의 문제점을 분석한다. 4장에서 보안성이 향상된 사용자 인증 스킴을 제안한다. 그리고 5장에서 본 논문이 제안한 스킴에 대한 안정성을 분석한다. 그리고 6장에서 본 논문의 결론을 짓는다.

2. 관련 연구

2.1 생체정보를 활용한 인증 기법

사람을 인증하기 위한 요소는 다음과 같이 세 가지로 구분 지울 수 있다. 즉, 그 사람이 알고 있는 것(예를 들어, 패스워드), 그 사람이 소유하고 있는 것(예를 들어, 스마트카드와 같은 사용자 소유 장치 및 물건), 그 사람 자신의 것(예를 들어, 지문과 같은 생체정보)로 나눌 수 있다. 사용자를 인증하기 위한 기법 중 이중요인(Two-factor) 인증에서는 위 3가지 중 2가지를 조합하여 사용한다. 스마트카드와 패스워드만을 이용하는 인증기법에선 off-line password attack으로 인해서 사용자의 패스워드가 노출될 가능성이 높다. 이러한 이중요인에서 발생하는 보안 문제점을 해결하기 위해 생체정보 등을 추가하여 삼요인(Three-factor) 인증을 사용한다. 일반적으로 사람이 불편함 없이 사용할 수 있는 패스워드의 길이는 한계가 있기 때문에 무작위 대입공격에 취약하지만, 생체정보는 무작위 입력 공격으로는 정보를 알아내기 어렵다. 그래서 생체정보를 이용한 인증 기법에서는 사용자 스마트카드가 분실되더라도 공격자로서는 생체정보를 알아낼 수가 없어서 스마트카드를 이용한 공격은 불가능한 것이다.[7,8].

2.2 퍼지추출 기법

퍼지추출기법(Fuzzy extraction)을 이용하면 생체정보를 랜덤 스트링으로 바꿀 수 있는데, 이를 이용하면 생체정보를 암호학적 기법에 사용할 수 있다. 이 방식은 *Gen*과 *Rep* 이라는 효율적인 생성자들로 구성되어 있으며, Generate와 Reproduce를 뜻한다. $Gen(B) = (R, P)$ 에서 생체정보 B 를 이용하여 정규화된 랜덤 스트잉 R과 핼퍼 스트링 P 를 생성한다. 그래서 $R = Rep(B', P)$ 에서 사용자가 조금 다른 B' 를 입력하더라도 P 를 이용하여 정상적인 R 을 생성해낼 수 있는 것이다. 즉, 처음 입력한 생체정보와 논리적으로 유사한 입력값에 대해서 항상 같은 R 를 생성해주기 위해 P 를 사용하므로, 생체정보의 특성상 발생하는 에러에 내성을 가지고 있다고 할 수 있다. 퍼지추출 기법을 이용한 인증 스킴에서는 등록 단계에서 R 과 P 를 생성하고 로그인 절차에서 P 를 이용하여 정상적인 R 를 도출해내므로, 상황에 따라 조금씩 달라지는 생체정보도 정상적으로 로그인할 수 있게 할 수 있다[9,10].

2.3 타원 곡선 문제

타원곡선 암호 시스템에서는 3가지의 수학적 문제가 존재한다. 이때 Elliptic Curve Discrete Logarithm Problem (ECDLP)은 $Q=xP$ 는 Q 와 P 를 알더라도 x 를 알아낼 수 없는 문제이며, Elliptic Curve Computational Diffie-Hellman Problem (ECCDHP)는 aP, bP 값을 알아도 abP 값을 알아

낼 수 없는 문제이며, Elliptic Curve Decisional Diffie-Hellman Problem (ECDDHP)는 $cP = abP$ 일 때, cP 로부터 aP, bP 를 알 수 없는 문제이다[11]. 본 논문에서는 명확한 구분을 위하여 xP 에서 x 와 P 간 타원곡선 연산을 * 로 표시한다. 즉, ECDDHP는 타원곡선연산 * 상에서 $c * P = a * b * P$에서 공격자가 $c * P$ 값을 알더라도 $a * P$ 값과 $b * P$ 값을 알아낼 수 없다는 것을 뜻한다.

3. Li 등이 제안한 인증 스킴 분석

Li 등은 ECC 기법을 이용한 사용자 인증 스킴을 제안하였는데 본 장에서는 Li 등이 제안한 인증 스킴의 동작 과정 및 취약점을 분석한다[2,5,13]. 표 1은 본 논문에서 사용하는 용어를 정리하였다.

(표 1) 용어 설명
(Table 1) Notations

용 어	설 명
R	등록 센터
S_i	서버 i
C_i	사용자 i
A_i	공격자
ID_i	사용자 C_i의 ID
PW_i	사용자 C_i 의 패스워드
B_i	사용자 C_i 의 생체정보
P	타원곡선의 포인트 값
$h(\cdot)$	안전한 해쉬함수
X_s	R 이 소유하고 있는 비밀정보
R_c	사용자 C_i 가 생성한 랜덤 값
R_s	사용자 S_i 가 생성한 랜덤 값
$\|\|$	연접 연산자
$\oplus$	배타적 논리합 연산자
*	타원곡선 상의 연산자

3.1 Li 등이 제안한 스킴 개요

3.1.1 등록 과정

로그인 및 인증 과정을 하기 전에 C_i 와 R 은 다음과 같은 등록 과정을 거치게 된다. C_i 는 ID_i 와 PW_i 를 선택하고 랜덤 값 K 를 생성한다. 그리고 C_i 는 사용자의 생체정보 B_i 를 퍼지 추출기에 입력한다. C_i 는 자신의 ID_i 와 B_i, $RPW_i = h(PW_i||K)$ 를 등록 센터 R 에 안전한 통신으로 전송한다. R 은 사용자의 메시지와 비밀값 X_s를 이용하여 $Gen(B_i) = (R_i, P_i)$, $f_i = h(ID_i||R_i)$, $e_i = h(ID_i||X_s) \oplus h(f_i||RPW)$, $r_i = h(ID_i||RPW_i)$를 생성한다. R 은 $< e_i, f_i, r_i, P_i, h(\cdot) >$을 스마트카드에 저장하고 안정한 통신과정을 통해 C_i 에게 전송한다. C_i 는 K 를 스마트카드에 입력한다.

3.1.2 로그인 및 인증 과정

C_i 는 S_i 와의 인증과정으로 하기 전에 자신의 정보를 이용하여 적법한 인증 메시지를 생성하는 로그인 과정을 다음과 같이 거치게 된다. C_i 는 자신의 스마트카드를 리더기에 넣고 ID_i 와 PW_i 를 입력한다. 그 후 C_i 는 B_i 를 스캔하고 $R_i = Rep(B_i', P_i)$ 를 계산한다. 스마트카드는 $f_i' = h(ID_i||R)$ 를 계산하고 C_i 의 스마트카드에 저장되어 있는 f_i 와 비교 한다. 만약 두 값이 같으면 C_i 는 생체정보를 이용한 검증과정을 마치고, 다르면 로그인 절차를 중단한다. 스마트카드는 $RPW_i = h(PW_i||K)$, $r_i' = h(ID_i|| RPW_i)$ 를 계산하고 r_i' 와 스마트카드에 저장된 r_i가 같은지 확인한다. 두 값이 같으면 ID 와 패스워드 검증과정을 마치고, 다르면 로그인 절차를 중단한다. 스마트카드는 $M_1 = e_i \oplus h(f_i'||RPW_i)$ 를 계산하고 $a \in Z_n^*$ 를 생성한다. 그 후 스마트카드는 $M_2 = a * P$, $M_3 = h(M_1 ||M_2)$ 를 계산한다. 그리고 C_i 는 S_i 에게 로그인 요청 메시지 $< ID_i, M_2, M_3 >$ 를 전송한다.

S_i 는 C_i 의 요청 메시지를 받은 후, 서로를 인증하고 세션키를 공유하는 인증 과정을 시작한다. S_i 는 메시지의 ID_i 를 체크하고 검증한다. ID_i 가 적법하면, S_i 는 $M_4 = h(ID_i||X_s)$ 를 계산하고 $M_3 = h(M_4||M_2)$ 를 계산하고 메시지의 M_3 와 같은지 검증한다. 같으면 S_i 는 C_i 의 요청 메시지를 받아들이고 인증한다. S_i 는 랜덤 넘버 $b \in Z_n^*$ 를 생성하고 $M_5 = b * P$, $M_6 = h(M_4||M_2||M_5)$ 를 계산하다. 그리고 S_i 는 C_i 에게 상호 인증을 위한 $< M_5, M_6>$ 를 전송한다. C_i 가 S_i 의 $< M_5, M_6 >$ 메시지를 받으면, C_i 는 $M_6 = h(M_1||M_2||M_5)$ 를 생성하여 받은 M_6 과 비교하여 검증한다. 두 값이 같으면 S_i 는 C_i 에 의해 인증을 받게 되어 서로 상호 인증이 된다. C_i 와 S_i 는 서로 공유된 정보를 이용하여 다음과 같은 세션키 $SK = h(a * M_5) = h(b * M_2) = h(a * b * P)$를 생성하게 되고, 향후 통신을 안전하게 진행한다.

3.1.3 패스워드 변경 과정

본 스킴에서는 C_i 가 자신의 패스워드를 새로운 패스워드 PW_{inew} 로 바꾸고자 하면 쉽게 바꿀 수 있다. 또한 C_i 는 등록 센터인 R 의 도움 없이도 자신의 패스워드만 가지고 패스워드를 변경하고 있다. C_i 는 자신의 스마트카드를 리더기에 넣고 ID_i 와 PW_i 를 입력하고 패스워드 변

경을 요청한다. C_i 는 자신의 생체정보를 입력하고 $R_i = Rep(B_i', P_i)$ 를 퍼지 추출기를 이용하여 계산한다. 그 후 C_i는 $RPW_i = h(PW_i||K)$, $r_i' = h(ID_i||RPW_i)$ 를 계산하고 스마트카드 안의 r_i 와 비교한다. 두 값이 같으면 C_i 에게 새로운 패스워드 PW_{inew} 를 입력하게 한다. 스마트카드는 $RPW_i' = h(PW_{inew}||K)$, $e_i' = e_i \oplus h(f_i||RPW_i) \oplus h(f_i||RPW_i')$, $r_i' = h(ID_i||RPW_i')$ 를 계산한다. 스마트카드가 e_i 와 r_i 를 e_i' 와 r_i' 으로 교체하게 되면 패스워드 변경 과정이 안전하게 마무리된다.

3.2 Li 등이 제안한 스킴의 취약점 분석

3.2.1 Insider attack

Li 등이 제안한 스킴에서 하나의 서버에 소속된 내부 공격자는 데이터베이스에 접근하여 S_i 의 비밀정보 X_s 를 알아낼 수 있으며, C_i 와 통신과정에서 사용자의 ID_i 를 알아낼 수 있다. 이를 이용하여 공격자는 다른 서버 즉, 등록 센터 R 에 소속된 다른 여러 서버들에게 정상적인 사용자처럼 로그인 및 인증 과정을 완료할 수 있다.

Li 등이 제안한 스킴에서 내부 공격자는 ID_{ci}, X_s, P, $h(\cdot)$ 를 이용하여 로그인 메시지 < ID_{ci}, M_2, M_3 > 를 생성할 수 있다. 여기서 ID_{ci} 은 정상적인 사용자 중 한명의 ID 라는 뜻이다. 내부 공격자는 정상적인 사용자처럼 $M_1 = e_i \oplus h(f_i'||RPW_i)$ 를 생성할 수 있는데 그 이유는 $M_1 = h(ID_{ci}||X_s)$ 인데 내부공격자는 ID_{ci} 와 X_s 를 모두 알기 때문이다. 공격자는 랜덤 넘버 a 를 생성하고 M_2 와 M_3 를 계산하여 < ID_{ci}, M_2, M_3 >를 만들어서 등록 센터 R 에 소속된 서버 중에서 공격자가 로그인 및 인증을 하고 싶은 서버 S_j에게 인증 메시지를 전송하면 된다. < ID_{ci}, M_2, M_3 > 를 받게 되면, 그들은 먼저 메시지의 정당성을 확인하지만, 이 메시지가 공격자들이 만든 메시지인 것을 확인할 수 없다. 그러므로 S_j 는 < M_{j5}, M_{j6} > 를 생성하여 공격자에게 전송하게 된다. 공격자는 S_j이 전송한 메시지를 이용하여 앞으로 사용할 세션키 $SK = h(a * M_{j5}) = h(b_{Sj} * M_2) = h(a * b_{Sj} * P)$를 생성할 수 있다. 이처럼 하나의 서버에서 내부 공격자는 등록 센터에 소속된 다른 모든 서버들에게 정상적 사용자처럼 로그인 및 인증과정을 완료할 수 있다[14].

3.2.2 Off-line password attack

전력소비량을 물리적으로 모니터링하는 SPA(simple power analysis), DPA(differential power analysis) 방식을 이용하면 스마트카드 안에 저장되어 있는 모든 정보 계산할 수 있다. Li 등의 스킴은 스마트카드 안의 정보만을 이용하여 사용자의 패스워드를 알아낼 수 있다. 공격자는 C_i와 S_i의 통신과정을 관찰하여 ID_i 를 획득한다. 그리고 C_i의 스마트카드에 저장된 e_i, f_i, r_i, P, $h(\cdot)$ 와 K 를 SPA와 DPA를 이용하여 획득한다. 공격자는 이러한 정보를 이용하여 다음과 같은 공식 $r_i = h(ID_i||h(PW_i||K))$을 만든다. 이 공식에서 공격자는 패스워드 PW_i 를 제외한 모든 정보를 알 수 있다[12,13]. 그래서 공격자는 사전 공격, 무작위 공격 혹은 레인보우 테이블 공격 등 다양한 방식을 이용하여 패스워드를 알아 낼 수 있다. 이는 패스워드로 사용할 수 경우의 수가 한정적이라, 패스워드만 모르는 경우 공격자가 어렵지 않게 패스워드를 알아 낼 수 있는 것이다[14].

3.2.3 Authentication without biometrics

Li 등이 제안한 스킴에서 공격자는 사용자의 생체정보가 없더라도 인증과정을 통과할 수 있다. 공격자는 C_i와 S_i 간의 통신에서 ID_i를 획득하고 사용자의 스마트카드를 습득한 후, 3.2.2 장의 Off-line password attack을 이용하여 사용자의 PW_i 를 알아낸다. 그 후 공격자는 PW_i, K, e_i, f_i , P 값을 이용하여 $RPW_i = h(PW_i||K)$을 포함한 다양한 값을 만들어 낼 수 있다. 공격자는 이처럼 계산된 RPW_i 과 e_i 와 f_i 을 이용하여 공격자의 $M_{A1} = e_i \oplus h(f_i||RPW_i)$ 을 계산할 수 있다. 그 후, 공격자는 임의의 랜덤 넘버 a_A 를 생성하고, a_A 와 P 를 이용하여 $M_{A2} = a_A*P$ 를 생성한다. 공격자는 앞의 M_{A1} 과 M_{A2} 를 이용하여 $M_{A3} = h(M_{A1} ||M_{A2})$를 계산하고 ID_i, M_{A1} 그리고 M_{A3} 를 S_i 에게 전송한다. S_i 는 공격자로부터 받은 인증 메시지를 이용하여 사용자를 인증하게 되는데, S_i 는 받은 메시지가 공격자로부터 온 것을 알아 낼 수 없다. 그러므로 S_i 는 공격자를 인증하게 되고 정상적으로 M_5 와 M_6 를 계산하고 공격자에게 전송하게 된다. 그 후 공격자는 받은 메시지를 바탕으로 세션키 SK 를 만들 수 있으며 이를 이용하여 S_i 와 사용자처럼 암호화된 통신을 할 수 있다[14].

3.2.4 Denial-of-service

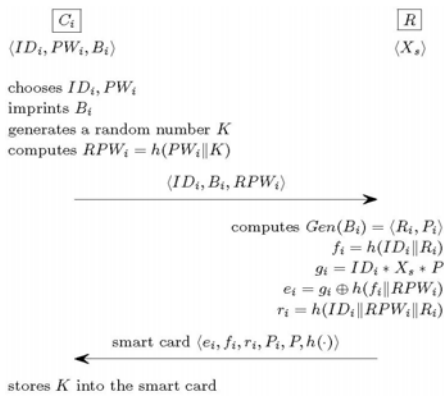
Li 등의 스킴에서는 S_i 는 사용자를 인증할 때, ID_i와 M_3 를 이용하여 확인한다. 그리고 S_i가 M_3를 인증하는 과정에서는 ID_i, X_s, M_2 만을 이용하게 된다. 그래서 S_i는 사용자가 보낸 < ID_i, M_2, M_3 > 가 예전 메시지인지 아닌지 확인할 방법이 없다. 그러므로 공격자가 C_i 와 S_i 간의 정

상적인 통신에서 < ID_i, M_2, M_3 >를 획득한 후, 추후에 S_i 에게 전송하더라도 S_i 는 이상 유무를 확인할 수가 없다. 공격자가 예전 메시지와 동일한 A_1, A_2, A_3… A_n을 생성하여 S_i 에게 보내게 되면 S_i 는 하나의 메시지를 받을 때마다 많은 연산을 진행하게 된다. S_i 는 우선 랜덤 넘버를 생성하는 연산 1회, 그리고 스칼라 곱셈 연산 1회, 해쉬함수 연산 3회 그리고 응답 메시지를 보내는 연산 1회를 하게 된다. 해쉬함수 연산은 그 계산 량이 적기 때문에 중요하지는 않지만, 랜덤 넘버를 생성하고 스칼라 곱을 하는 연산은 한꺼번에 처리할 경우 서버에게 부담이 될 수 있는 계산 량이기 때문에, 공격자가 많은 메시지를 보낼 경우, 정상적인 서비스를 제공하기 어렵게 되는 것이다[14].

4. 제안하는 보안성이 향상한 스킴

Li 등은 ECC와 해쉬함수를 이용하여 효율적인 원격 인증 스킴을 제안하였다. 하지만 앞에서 분석한 것처럼 Li 등의 스킴은 다양한 보안 문제점이 있어 개선할 필요가 있다. off-line password attack을 해결하기 위해서는 언제나 패스워드를 생체정보와 함께 사용해야 한다. 그리고 authentication without biometrics 문제를 해결하기 위해서는 패스워드와 사용자 스마트카드만으로는 C_i와 S_i 사이의 인증과정에서 사용하는 메시지를 생성할 수 없도록 해야 한다. 즉, 사용자의 B_i 없이는 인증 메시지를 만들 수 없도록 해야 한다. denial-of-service 공격을 해결하기 위해서는 타임스탬프를 이용하여 메시지의 최신성을 확인 할 수 있도록 해야 한다. 그리고 insider attack을 해결하기 위해서는 S_i 마다 서로 다른 비밀값을 가질 수 있도록 설정하고, 그 값을 이용하여 모든 사용자를 인증할 수 있도록 수정하여야 한다.

Li 등이 제안한 사용자 인증 스킴의 문제점을 해결하기 위해서 본 논문에서는 안정성이 향상된 퍼지 추출기술을 활용한 삼요인 원격 사용자 인증 및 키 동의 스킴을 제안한다. 제안하는 스킴은 등록 과정, 로그인 과정, 인증과정, 패스워드 변경과정으로 나뉜다. 사용자는 ID_i, PW_i 그리고 B_i 를 이용하며, R 은 비밀값 X_s 를 소유하고 있다. Li 등의 스킴에서 나타난 각각의 서버 상의 내부자로 부터 발생하는 문제를 해결하기 위해서, 본 논문에서는 S_i 에게 $A_i = S_n * X_s * P$ 를 전달하게 된다. Li 등의 스킴에서 모든 S_i 가 동일한 X_s 를 소유하고 있었던 반면, 제안하는 스킴에서는 각각의 S_i 가 자신의 S_n 에 따라 각기 다른 A_i 값을 소유하게 되어, 다른 S_j 의 A_j 값은 알 수 없게 된다. 그리고 타임스탬프를 추가하고 기존의 연산과정을 보다 안전하게 변경하였으며 4.1 등록 과정부터 4.4 패스워드 변경과정을 통해 상세한 내용을 알 수 있다.



(그림 1) 제안하는 스킴의 등록 과정
(Figure 1) Registration on proposed scheme

4.1 등록 과정

로그인 및 인증 과정을 하기 전에 C_i 와 R 은 그림 1과 같은 등록과정을 거치게 된다.

(1) 사용자 C_i 는 ID_i 와 PW_i 를 선택하고 생체 정보 B_i 를 퍼지 추출기에 입력한다. 그리고 랜덤 값 K를 생성한다. C_i 는 사용자 ID_i 와 B_i 와 $RPW_i = h(PW_i \| K)$를 등록 센터 R 에 안전한 통신으로 전송한다.

(2) R 은 사용자의 메시지와 비밀값 X_s를 이용하여 $Gen(B_i)$, f_i, g_i, e_i, r_i를 생성한다.

$$Gen(B_i) = < R_i, P_i >$$
$$f_i = h(ID_i \| R_i),\ g_i = ID_i * X_s * P$$
$$e_i = g_i \oplus h(f_i \| RPW_i)$$
$$r_i = h(ID_i \| RPW_i \| R_i)$$

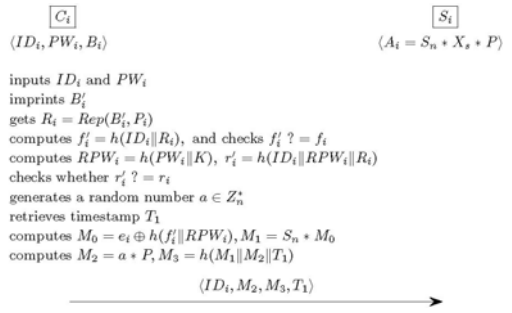
(3) R은 이 중 g_i 값을 제외한 < e_i, f_i, r_i, P_i, P, $h(\cdot)$ >을 스마트카드에 저장하고 안정한 통신과정을 통해 C_i 에게 전송한다.

(4) C_i 는 K 를 스마트카드에 입력한다.

4.2 로그인 과정

C_i 는 그림 2과 같이 로그인 과정을 통해 적법한 사용자인지 검증받게 된다. 그리고 로그인 과정 전에 S_i 는 R 과의 통신을 통해 S_i 만의 $A_i = S_n * X_s * P$ 값을 공유하고 향후 과정을 진행한다.

(1) 사용자 C_i 는 스마트카드를 리더기에 넣고 ID_i 와 PW_i를 입력한다. 그리고 B_i' 를 추출하고 하고 $R_i = Rep(B_i', P_i)$ 로 R_i 를 계산한다.



(그림 2) 제안하는 스킴의 등록 과정
(Figure 2) Login on proposed scheme

(2) 그리고 스마트카드는 $f_i' = h(ID_i||R)$ 를 계산하고 스마트카드에 저장되어 있는 f_i 와 비교 한다. 만약 두 개가 같으면 다음 과정을 진행한다.

(3) 스마트카드는 $RPW_i = h(PW_i||K)$, $r_i' = h(ID_i || RPW_i||R_i)$를 계산하고 r_i' 와 스마트카드에 저장된 r_i 가 같은지 확인한다.

(4) 스마트카드는 $a \in Z_n^*$ 와 현재 타임스탬프 T_1을 생성하고 M_0, M_1, M_2, M_3 를 계산한다. 그리고 사용자 C_i 는 S_i 에게 타임스탬프를 포함한 로그인 요청 메시지를 전송한다.

$M_0 = e_i \oplus h(f_i'||RPW_i)$, $M_1 = S_n * M_0$,
$M_2 = a * P$, $M_3 = h(M_1||M_2||T_1)$,
로그인 요청 메시지 $< ID_i, M_2, M_3, T_1 >$

4.3 인증 과정

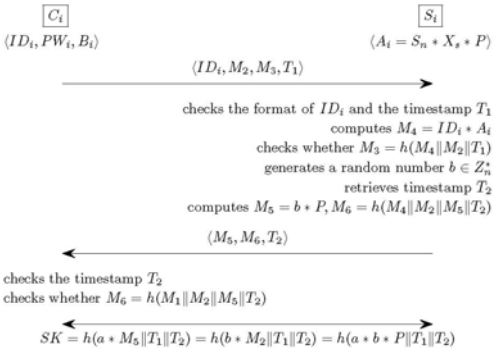
그림 3과 같이 서버 S_i 는 C_i 의 로그인 요청 메시지를 받고 난 뒤, 서로 간의 인증 및 세션키를 공유하는 인증 과정을 시작하게 된다.

(1) S_i 는 메시지의 ID_i 의 포맷과 T_1 를 검증한다.

(2) 모두가 적법하면, S_i 는 $M_4 = ID_i * A_i$ 를 계산하고 $M_3 = h(M_4||M_2||T_1)$ 를 계산하고 메시지의 M_3 와의 동일성을 검증한다. 같으면 C_i의 메시지를 인증한다.

(3) S_i 는 랜덤 값 $b \in Z_n^*$ 와 타임스탬프 T_2를 생성하고 $M_5 = b * P$, $M_6 = h(M_4||M_2||M_5||T_2)$ 를 계산한다. S_i 는 C_i 에게 상호 인증을 위한 메시지 $< M_5, M_6, T_2 >$ 를 전송한다.

(4) 그 후, C_i 가 S_i의 $< M_5, M_6, T_2 >$ 메시지를 받으면, C_i 는 타임스탬프 T_2 를 검증하고 $h(M_1||M_2||M_5||T_2)$ 를 생성하여 받은 M_6 과 비교한다. 두 값이 같으면 S_i 는 C_i 에 의해 인증을 받게 되어 상호 인증이 완성된다.



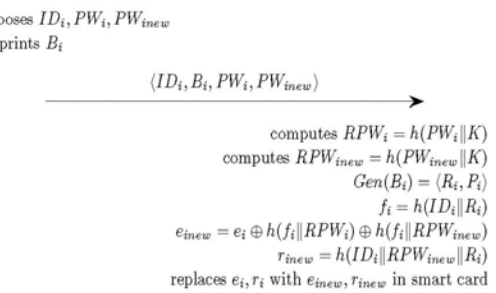
(그림 3) 제안하는 스킴의 등록 과정
(Figure 3) Authentication on proposed scheme

(5) C_i 와 S_i 는 서로 공유된 정보를 이용하여 다음과 같은 세션키 SK 를 생성하고, 이 값을 이용하여 앞으로의 통신을 안전하게 진행하게 된다.

$SK = h(a * M_5||T_1||T_2) = h(b * M_2||T_1||T_2)$
$= h(a * b * X_s * P||T_1||T_2)$

4.4 패스워드 변경 과정

사용자 C_i 가 새로운 패스워드 PW_{inew} 를 설정하고자 할 때 인증센터 R 나 서버 S_i 도움 없이 쉽게 변경할 수 있다. 그림 4는 제안하는 스킴의 패스워드 변경 과정을 보여주고 있다.



(그림 4) 제안하는 스킴의 패스워드 변경과정
(Figure 4) Password change on proposed scheme

(1) C_i 는 스마트카드를 리더기에 넣고 ID_i 와 PW_i 와 PW_{inew} 를 입력하고 패스워드 변경을 요청하고 생체정보를 입력한다. 그 후 스마트카드는 $RPW_i = h(PW_i||K)$, $RPW_i' = h(PW_{inew}||K)$ 를 계산한다. C_i 는 $Gen(B_i) = < R_i', P_i >$ 를 퍼지 추출을 이용하여 R_i 를 추출한다. 그리고 $f_i = h(ID_i||R_i)$ 를 계산한다.

(2) 스마트카드는 e_{inew}, r_{inew} 를 계산한다.

$e_{inew} = e_i \oplus h(f_i||RPW_i) \oplus h(f_i||RPW_{inew})$

$r_{inew} = h(ID_i||RPW_{inew}||R_i)$

(3) 스마트카드가 기존의 e_i 와 r_i 를 e_{inew} 와 r_{inew} 으로 교체하게 되면 모든 패스워드 변경과정이 끝난다.

5. 제안하는 스킴의 안전성 분석

제안하는 스킴의 보안성을 검증하기 위해 본 장에서는 제안하는 스킴에 대한 안정성 분석을 수행한다. 그리고 다른 스킴과 비교하여 제안하는 스킴이 보안성이 향상되었다는 것을 확인한다.

① Mutual authentication : 제안하는 스킴에서는 상호인증을 제공하고 있다. C_i 는 로그인 요청 메시지 $< ID_i, M_2, M_3, T_1 >$를 S_i 에게 전송하고, S_i 는 ID_i와 T_1을 검사한 후 $M_4 = ID_i * A_i$ 를 계산한다. 적법한 C_i 와 S_i 만이 M_4를 만들 수 있고 이를 이용하여 M_3 와 $h(M_4||M_2||T_1)$을 비교한다. 두 개의 값이 일치하면 S_i 는 C_i 를 적법한 사용자로 인증 한다. M_5 와 M_6 를 계산하여 그리고 $< M_5, M_6, T_2 >$ 를 C_i 에게 전송한다. C_i 는 $h(M_1||M_5||T_2)$ 를 계산하여 M_6 와 비교한다. 적법한 S_i 만에 M_6 를 계산할 수 있기 때문에, 두 값이 같다면 C_i 는 S_i 를 인증한다. 그러므로 제안하는 스킴은 상호인증을 제공한다.

② Session key agreement : 제안하는 스킴은 로그인 및 인증 과정이 마친 후 C_i와 S_i 간의 SK 를 생성한다. 즉, C_i 는 자신의 랜덤 값 a 와 S_i 가 보내온 M_5 를 이용하여, $h(a*M_5)$ 를 생성하고 이를 SK 로 사용한다. S_i 는 자신의 랜덤값 b와 C_i 가 보내온 M_2 를 이용하여 $h(b*M_2||T_1||T_2)$을 생성하고 SK 로 이용한다. $h(a*M_5||T_1||T_2)$ 와 $h(b*M_2||T_1||T_2)$ 는 모두, $h(a*b*X_s*P||T_1||T_2)$ 로 두 값은 같은 값을 공유하게 되며 이를 SK 로 이용한다. 더욱이 타임스탬프 T_1, T_2 를 사용하여 매번 다른 SK 값을 사용하게 된다.

③ Change password freely : 제안하는 스킴은 C_i 가 자신의 패스워드를 바꾸고자 할 때, 등록 센터 R_i 나 서버 S_i 의 도움 없이 자유롭게 패스워드를 변경할 수 있다. 그리고 사용자는 자신의 ID_i, B_i 그리고 기존 패스워드 PW_i 와 새로운 패스워드 PW_{inew} 를 입력하고 새로운 e_{inew} 와 r_{inew}를 다음과 같이 생성할 수 있다.

$e_{inew} = e_i \oplus h(f_i||RPW_i) \oplus h(f_i||RPW_i)$

$r_{inew} = h(ID_i||RPW_{inew}||R_i)$

그 후 생성 e_{inew} 와 r_{inew} 를 기존의 e_i 와 r_i 와 교체하는 것만으로 패스워드 변경과정을 완료할 수 있다.

④ Resist forgery attack : 제안하는 스킴에서는 공격자가 C_i 와 S_i 간의 메시지를 위조하여 인증을 받을 수 없다. C_i 는 S_i 에게 $< ID_i, M_2, M_3, T_1 >$ 를 전송하게 되는데, M_3 는 $h(M_1||M_2||T_1)$로 M_1에는 적법한 사용자만이 생성할 수 있는 g_i 즉 $ID_i * X_s * P$ 가 포함되어 있어 위조할 수 없다. S_i 가 C_i에게 $<M_5, M_6, T_2>$를 전송하게 되는데, M_6 는 $h(M_4||M_5||T_2)$ 인데 이 중에서 M_4 에는 $S_n * X_s * P$ 이 포함되어 있어 적법한 S_i 만이 생성할 수 있다. 더욱이 M_3 와 M_6 모두 타임스탬프를 포함하고 있어 타임스탬프만 변경하고 기존의 메시지를 그대로 보내는 위조방식도 불가능하다.

⑤ Resist replay attack : 공격자는 C_i 와 S_i 간의 메시지를 수집한 후, 이를 다시 재전송함으로써 C_i 혹은 S_i 에게 인증을 받는 공격을 할 수 있다. 하지만 제안하는 스킴에서는 C_i 와 S_i 가 랜덤값 a, b 그리고 타임스탬프 T_1, T_2 를 사용함으로써, 이러한 재전송공격을 차단하였다. 랜덤값 a, b 는 매 세션 마다 달라지며, T_1, T_2 는 현재 타임스탬프이므로 공격자는 본 세션의 M_3 과 M_6 를 계산할 수 없다.

⑥ Quickly detect the wrong password : C_i 가 잘못된 패스워드를 입력하였을 때, 이를 빠르게 알 수 있어야 사용자에게 로그인 과정을 재시도할 수 있도록 신속하게 안내할 수 있다. 본 스킴은 저장된 r_i 와 계산한 $h(ID_i||RPW_i||R_i)$ 를 비교하여 로그인 과정에서 패스워드를 빠르게 체크할 수 있다. 그 이유는 $RPW_i = h(PW_i||K)$ 이기에 잘못된 패스워드를 입력하면 r_i 값이 다른 값이 생성되기 때문이다.

⑦ Resist insider attack: 본 스킴에서는 insider attack 을 해결하기 위해서, S_i 마다 서로 다른 비밀값을 가질 수 있도록 설정하였다. 즉 R_i 가 S_i 에게 앞으로 사용자 인증에 사용할 비밀값을 전달할 때, $S_n * X_s * P$ 값으로 설정하여 모든 S_i 마다 서로 다른 값을 가질 수 있도록 하였다. 그래서 하나의 서버 S_i 를 관리하는 내부 관리자가 서버의 비밀값을 획득한다고 하더라도 다른 S_i 의 서버 비밀값은 알 수 없으므로 내부자 공격이 불가능하다.

⑧ Resist off-line password attack : 공격자는 SPA와 DPA와 같은 전력 모니터링 분석 방법으로 스마트카드 내의 모든 정보를 추출할 수 있다[12,13]. 이렇게 추출한

정보를 이용함으로써, 공격자는 사용자의 패스워드 정보가 들어있는 값에서부터 패스워드를 유추할 수 있다. 그건 패스워드로 사용할 수 있는 정보의 양이 적어 무작위 대입 공격을 통해 패스워드를 유추할 수 있기 때문이다. 하지만 제안하는 스킴에서는 패스워드 정보가 포함된 모든 값에 사용자 생체정보값을 함께 삽입하여, 생체정보값을 모르면 패스워드도 알아낼 수 없도록 설계하였다. 즉, 공격자가 유추할 수 생체정보값을 이용하여 패스워드를 유추할 수 없도록 하였다. 스마트카드 내 패스워드 정보가 포함된 값은 $r_i = h(ID_i||RPW_i||R_i)$ 뿐인데, 공격자가 r_i에서 PW_i 을 유추해내기 위해서는 R_i 값도 알아야하는데, R_i 값은 사용자의 생체정보인 B_i 값을 알아야만 생성할 수 있는 값이다. 생체정보인 B_i 값은 공격자가 임의로 생성해 낼 수 없으며 무작위 대입 공격으로 유추할 수 없으므로 본 스킴은 패스워드 유추 공격에 안전할 수 있다.

⑨ Authentication without biometrics : 패스워드와 사용자 생체정보를 모두 사용하는 스킴에서 설계상의 오류 때문에, 공격자가 사용자의 스마트카드와 패스워드만으로 인증과정을 정상적으로 완료할 수 있는 문제가 발생할 수 있다. 하지만 본 논문에서 제안하는 스킴에서는 반드시 사용자의 스마트카드, 패스워드 그리고 생체정보를 모두 아는 적법한 사용자만이 C_i 와 S_i 사이 인증과정에서 사용하는 메시지를 생성 및 검증 할 수 있도록 하였다. 본 스킴에서 사용자가 인증을 받기 위해 반드시 필요한 값인 $g_i = ID_i * X_s * P$ 값은 스마트카드 안에 저장되어 있지 않으며, 사용자가 입력한 값을 이용하여 생성 값이다. g_i 를 생성하기 위해서는 사용자의 ID_i 뿐만 아니라 패스워드 그리고 생체정보가 필요하다. e_i 값에 $h(f_i||RPW_i)$ 을 XOR 연산을 하면 g_i 값이 생성되는데, f_i 값을 생성하기 위해서는 사용자의 ID정보와 생체정보 값이 필요하며, RPW_i 를 생성하기 위해서는 패스워드가 필요하기 때문이다.

⑩ Denial-of-Service : 사용자 C_i 와 서버 S_i 간의 통신 내용을 수집하여 이를 다량으로 S_i 에게 재전송함으로써 S_i가 정상적인 서비스를 제공할 수 없도록 하는 것을 최대한 막기 위해서, 제안하는 스킴에서는 기본적으로 타임스탬프 방식을 제안하였다. 그러므로 기존의 메시지를 그대로 보내면 타임스탬프 검사만으로 바로 인증메시지를 거절할 수 있다. 또한 공격자가 타임스탬프만 최신의 것으로 수정하여 보낼 경우, 악의적 공격자가 보내온 M_3 값과 S_i가 생성한 $h(M_4||M_2||T_1)$ 값이 다르므로, S_i는 이 메시지를 바로 거절할 수 있다. 이러한 방법을 통해서 제안하는 인증 스킴은 서비스 거부 공격에 보다 안전하도록 설계되었다. 아래 표 2에서는 기존에 제안된 다른 스킴과 본 논문이 제안하는 스킴의 안전성을 비교하였다 [2,5,15,16].

본 논문에서 제안하는 스킴은 Li 등이 제안하고 있는 스킴에서 발생하는 취약점뿐만 아니라, An, Das 그리고 Li & Hwang 에서 발생하는 취약점들도 해결할 수 있다. 그러므로 제안하는 스킴은 스마트카드, 패스워드, 그리고 생채정보를 이용하여 사용자를 인증하고 이때 퍼지볼트 기법을 활용하여 보다 안전한 스킴을 완성하였다.

(표 2) 보안성 비교
(Table 2) Security comparison

보안성	An	Das	Li&Hwang	Li et al.	제안스킴
①	O	X	X	O	O
②	X	X	X	O	O
③	X	O	O	O	O
④	X	X	O	O	O
⑤	O	O	O	O	O
⑥	X	O	X	O	O
⑦	X	O	X	X	O
⑧	O	X	O	X	O
⑨	O	X	O	X	O
⑩	X	X	X	X	O

6. 결 론

An이 제안한 사용자 인증 스킴에 대한 보안성을 높이기 위해 Li 등이 제안한 타원암호기술과 퍼지 추출 기술을 기반한 삼요인 사용자 인증 스킴은 효율적이지만, 여전히 off-line password attack, authentication without biometrics, denial-of-service, insider attack 에 취약하다는 문제가 있었다. 본 논문에서는 Li 등의 스킴에서 발견된 문제점을 해결하여 보안성이 향상된 퍼지 추출기술을 활용한 삼요인 원격 사용자 인증 및 키 동의 스킴을 제안하였다. 그리고 다른 인증 스킴과의 비교를 통해 제안하는 스킴의 안전성을 검증하였다.

참 고 문 헌 (Reference)

[1] Lin, Chu-Hsing, and Yi-Yi Lai. "A fingerprint-based user authentication scheme for multimedia systems." Multimedia and Expo, 2004. ICME'04. Vol. 2. IEEE, 2004.
http://dx.doi.org/10.1109/ICME.2004.1394355.

[2] Xiong Li, Jianwei Niu, Muhammad Khurram Khan, Junguo Liao and Xiaoke Zhao, "Robust three factor remote user authentication scheme with key agreement for multimedia systems." Security and Communication Networks (2014).
http://dx.doi.org/10.1002/ sec.961.

[3] Lamport, Leslie. "Password authentication with in-secure communication." Communications of the ACM 24.11 (1981): 770-772.
http://dx.doi.org/10.1145/358790.358797.

[4] Chuang, Ming-Chin, and Meng Chang Chen. "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics." Expert Systems with Applications 2014.
http://dx.doi.org/10.1016/j.eswa.2013.08.040

[5] An, Younghwa. "Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards." BioMed Research International 2012.
http://dx.doi.org/ 10.1155/2012/519723

[6] Xiong Lia, Jian-Wei Niub, Jian Maa, Wen-Dong Wanga, Cheng-Lian Liuc, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards." Journal of Network and Computer Applications 34.1 (2011): 73-79.
http://dx.doi.org/10.1016/j.jnca.2010.09.003

[7] Jongho Moon, Younsung Choi, jaewook Jung, Dongho Won, "An Improvement of Robust Biometrics-Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards." PloS one 10.12 (2015),
http://dx.doi.org/10.1371/journal.pone.0145263

[8] Younsung Choi, Donghoon Lee, Jiye Kim, Jaewook Jung, Junghyun Nam and Dongho Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography." Sensors 14.6, 2014.
http://dx.doi.org/10.3390/s140610081

[9] Dodis, Yevgeniy, Leonid Reyzin, and Adam Smith. "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data." Advances in cryptology-Eurocrypt 2004.
http://dx.doi.org/10.1007/978-3-540-24676-3_31

[10] Choi, Younsung, Youngsook Lee, and Dongho Won. "Security Improvement on Biometric Based Authentication Scheme for Wireless Sensor Networks Using Fuzzy Extraction." International Journal of Distributed Sensor Networks, 2016.
http://dx.doi.org/10.1155/2016/8572410

[11] Lauter, Kristin. "The advantages of elliptic curve cryptography for wireless security." IEEE Wireless communications 11.1 (2004): 62-67.
http://dx.doi.org/10.1109/MWC.2004.1269719

[12] Messerges, T. S.; Dabbish, E. A.; Sloan, R. H, "Examining smart-card security under the threat of power analysis attacks". Computers. IEEE Transactions on Computers, 2002, 51(5).
http://dx.doi.org/10.1109/TC.2002.1004593

[13] Nam, Junghyun, et al. "Dictionary Attacks against Password-Based Authenticated Three-Party Key Exchange Protocols." TIIS 7.12 (2013): 3244-3260.
http://www.dbpia.co.kr/Article/NODE02405172

[14] Younsung Choi, Donghoon Lee, Jiye Kim, Jaewook Jung and Dongho Won.. "Cryptanalysis of Robust Three-Factor Remote User Authentication Scheme with Key Agreement for Multimedia System." The International Conference on Digital Security and Forensics (DigitalSec2014). The Society of Digital Information and Wireless Communication, 2014.
http://sdiwc.net/digital-library/cryptanalysis-of-robust-threefactor-remote-user-authentication-scheme-with-key-agreement-for-multimedia-system.html

[15] Das, Amal K. "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards." Information Security, IET 5.3 (2011): 145-151.
http://dx.doi.org/10.1049/iet-ifs.2010.0125

[16] Li, Chun-Ta, and Min-Shiang Hwang. "An efficient biometrics-based remote user authentication scheme using smart cards." Journal of Network and computer applications 33.1 (2010): 1-5.
http://dx.doi.org/10.1016/j.jnca.2009.08.001

◐ 저 자 소 개 ◑

최 윤 성 (Younsung Choi)
2006년 2월 : 성균관대학교 정보통신공학부 학사
2007년 8월 : 성균관대학교 전자전기컴퓨터공학과 석사
2011년 3월 ~ 현재 : 경북대학교 법학과 형법전공 박사과정
2015년 8월 : 성균관대학교 전자전기컴퓨터공학과 박사
2015년 9월 ~ 2016년 2월 : 성균관대학교 IT융합원 박사후과정
2016년 3월 ~ 현재 : 호원대학교 사이버수사보안학부 조교수
관심분야: 정보보호, 사용자 인증, 디지털 포렌식
E-mail : yschoi@howon.ac.kr

원 동 호 (Dongho Won)
1976년~1988년 : 성균관대학교 전자공학과 (공학사, 공학석사, 공학박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공업대학교 객원연구원
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
1982년~ 현재 : 성균관대학교 컴퓨터공학과 교수
現 성균관대 행단석좌 교수, 한국정보보호학회 명예회장
관심분야: 정보보호, 암호이론, 정보이론
E-mail : dhwon@security.re.kr