The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 4, pp.43-53, Aug. 31, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.4.43
JIIBC 2015-4-6

C/S 시스템에 적합한 보안성이 강화된 생체정보 기반의 사용자 인증 스킴

User Authentication Scheme based on Security-enhanced Biometric Information for C/S System

양형규*

Hyung-Kyu Yang*

요 약 서버-클라이언트 시스템에서 패스워드를 기반으로 하는 인증 스킴은 사용이 편리하지만, 사전 공격 및 무작위 공격에 취약하다는 단점이 있다. 이를 해결하기 위한 방법으로 암호학적으로 안전한 장문의 키를 사용할 수도 있지만, 기억하기가 어렵다는 단점이 있다. 그래서 생체정보를 이용한 인증 스킴을 Das가 처음으로 제안하여 이러한 문제를 해결하고자 했다. 하지만 Das의 인증 기법은 다양한 보안 보안취약점이 있어 이를 해결하고자 Jiping 등이 Das의 스킴을 개선하였지만 여전히 다양한 문제점이 있다. 그래서 본 논문에서 분석한 문제점을 해결한 보다 안전한 생체정보 기반의 사용자 인증 스킴을 제안한다. 그리고 보안성 분석을 통해 안전성을 검증하고 다른 스킴과 비교한다.

Abstract Password-based authentication schemes for server-client system are convenient to use, but vulnerable to dictionary attack or brute-force attack. To solve this vulnerability, Cryptographic secret key is used for security, but difficult to memorize. So, for the first time, Das proposed a biometric-based authentication scheme to solve various problems but it has various vulnerabilities. Afterwards, Jiping et al. improved Das's scheme, but some vulnerabilities remain. In this paper, we analyze the cryptanalysis of Jiping et al.'s authentication scheme and then propose improved biometric based user authentication scheme to resolve the analyzed problem. Moreover, we conduct a security analysis for the proposed scheme and make a comparison between the proposed scheme and other biometric based user authentications.

Key Words : User authentication scheme, Biometrics, Security analysis

Ⅰ. 서 론

원격 ID 기반 인증 스킴은 기본적으로는 사용자의 ID와 패스워드만을 이용하여 사용자를 인증하는 방식이다. 이렇게 ID와 패스워드만을 이용한 사용자 인증 스킴은 효율적이고 사용이 간편한 장점을 가지고 있어 일반적인 통신에서 많이 사용되고 있다. 하지만 패스워드만을 비밀정보로 사용하는 경우에는 간단한 사전 공격 혹은 무작위 입력 공격에 쉽게 패스워드가 노출될 가능성이 높다[1]. 이러한 문제를 해결하기 위해서 사용자 인증 스킴

*정회원, 강남대학교 컴퓨터미디어정보공학부
접수일자 2015년 7월 28일, 수정완료 2015년 8월 7일
게재확정일자 2015년 8월 7일

Received: 28 July, 2015 / Revised: 7 August, 2015 / Accepted: 7 August, 2015
*Corresponding Author: hkyang@kangnam.ac.kr
Division of Computer&Media-Information engineering, Kangnam University, Korea

에 암호학적으로 안전한 비밀정보를 패스워드와 함께 사용하는 방식이 사용되기도 하였다. 하지만 이 방식도 암호학적으로 안전한 비밀정보를 사용자가 기억하는 것은 어려운 일이고, 그 값을 저장하여 사용한다면 공격자는 이 부분을 취약점으로 이용할 수 있으므로 문제가 된다. 이러한 문제를 해결하기 위해서 다양한 생체정보 기반의 인증 스킴이 제안되었다[2,3]. Das 가 새로운 생체정보 기반의 사용자 인증 스킴을 제안하였으나, 제안한 스킴이 Denial-of-Service, user impersonation attack, replay attack에 취약하고 패스워드 변경이 자유롭지 못하다는 문제점이 있었다. 이러한 문제를 해결하기 위해, Jiping 등은 서버 클라어언트 구조에서 사용이 가능하고 Das의 스킴보다 안전성이 개선된 생체정보 기반의 원격 사용자 인증 스킴을 제안하였다[4].

하지만 Jiping 등이 제안한 스킴은 여전히 Server Masquerading Attack, Stolen Smart Card Attack에 취약하고 Authentication without Login Phase 라는 문제를 가지고 있었다. 그래서 본 논문에서는 Jiping 등이 제안한 스킴에 대한 취약점 분석을 통해 발견된 문제점을 해결한 스킴을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서 본 논문을 이해하는데 필요한 관련연구를 살펴본 후, 3장에서 Jiping 등이 제안한 스킴에 대해서 간략히 알아본다. 그리고 4장에서 Jiping 등이 제안한 스킴의 취약점을 분석하고 5장에서 이러한 취약점을 해결한 서버-클라이언트 구조에 적합한 보안성이 강화된 생체정보 기반의 사용자 인증 스킴을 제안한다. 그리고 6장에서 제안한 스킴에 대한 취약점 분석을 통해 안정성을 검증한다. 그리고 7장에서 본 논문의 결론을 짓는다.

II. 관련 연구

1. Smart card 공격

그 동안 진행된 다양한 스마트 카드의 분석기술 연구에서 밝혀진 것처럼 SPA (Simple power analysis)나 DPA (Differential power analysis)와 같은 스마트 카드에 소비되는 전력량을 모니터링하는 기술에 의해서, 스마트 카드에 저장되어 있는 기밀 정보를 포함한 모든 데이터가 공격자에 의해 추출될 수 있다. 그래서 사용자가 자신의 스마트 카드를 분실하였을 때, 공격자는 그 스마트를 카드를 분석하여 다양한 정보를 추출해 낼 수 있고, 이를 이용하여 사용자의 기밀 정보도 계산할 수 도 있다. 특히 공격자가 off-line password attack 등을 이용하여 사용자의 패스워드를 계산할 수 있게 된다면, 공격자는 이를 이용하여 사용자로 위장하여 활동할 수 있게 된다.

2. 생체정보 기반의 인증 기법

생체정보를 이용한 인증기법에서는 사람의 특성을 이용하여 정량화된 데이터 정보를 이용하게 된다. 즉, 지문정보, 얼굴, DNA 정보, 손바닥, 각막, 홍채, 목소리 등의 사람을 구별할 수 있을 특징을 컴퓨터가 인식할 수 있는 데이터로 만들어서 사용하게 된다. 이러한 정량 데이터는 생체정보 기반의 인증 기법에서 사용자에 대한 접근 제어 혹은 식별에 사용된다. 사용자의생체정보는 분실하거나 잊어버릴 수 없을 뿐만 아니라, 복사하거나 공유하거나 위조하기가 어렵다. 또한 자신의 생체정보를 알더라도 다른 사람의 생체정보를 유추할 수 없으므로 인증 기법에 적용하기 용이하다.

3. Das의 생체정보 기반 인증 기법

Das가 제안한 생체정보 기반의 원격 사용자 인증 스킴은 기존의 전통적인 패스워드 기반의 인증 기법 보다 신뢰성과 안전성을 제공하여 준다. 하지만 Das의 인증 기법은 replay attack, denial-of-service attack, user impersonation attack 에 취약하며 패스워드 변경 상의 문제가 발생하였고, 또한 상호인증을 제공하지 못한다는 단점이 있다. Das의 스킴은 이후 다양한 연구가 진행되었으며, Jiping 등도 Das 스킴의 취약점을 분석한 후, 안전성을 개선한 생체정보 기반 인증 스킴을 제안하였다.

III. Jiping 등이 제안한 인증 스킴

Das는 생체정보 기반의 사용자 인증 스킴을 제안하였으나 다양한 보안 취약점을 가지고 있었다. 이를 해결하기 위해 Jiping 등은 보다 안전성을 개선한 스킴을 제안하였다. 이 스킴은 등록, 로그인, 인증, 패스워드 변경 단계로 구성되어 있다. 표 1은 본 논문에서 사용할 용어를 정리하였다.

표 1. 표기
Table 1. Notation

기호	설명
C_i	클라이언트 사용자
S_i	서버
R_i	등록센터
PW_i	사용자 패스워드
ID_i	사용자 ID
B_i	사용자의 생체정보
d(·)	비교함수
τ	비교한계값
h(·)	안전한 해쉬함수
H(·)	바이오 해쉬함수
X_s	서버와 등록센터가 공유한 비밀값
R_c	사용자가 생성한 랜덤값
R_s	서버가 생성한 랜덤값
A ‖ B	연접 연산자
A ⊕ B	배타적 논리합 연산자

1. 등록 과정

그림 1은 등록과정을 보여주고 있으며, 원격 사용자 인증 스킴은 아래와 같은 과정을 실행한다.

(1) 사용자 C_i 는 자신의 생체정보 B_i를 스캔 장치에 입력하여, 자신의 ID와 패스워드를 등록센터 R_i에 전송한다.

(2) 등록센터 R_i는 $f_i = h(B_i)$와 $g_i = h(ID_i)$, $r_i = h(PW_i) \oplus f_i$ 와 $e_i = h(g_i \| X_s) \oplus r_i$ 를 계산한다. X_s는 R_i와 S_i 간에 공유된 정보이다. X_s와 사용자 패스워드는 안전하게 공유되어 다른 사람에게 노출되지 않는다.

(3) 등록센터 R_i는 사용자의 스마트 카드에 ($h(\cdot)$, f_i, g_i, e_i, r_i, τ, $d(\cdot)$)에 저장시키고 사용자 C_i에게 안전한 채널로 전송한다.

2. 로그인 과정

Jiping 등의 스킴의 인증과정에서, 원격 사용자 C_i는 아래와 같이 실행하며 그림 2와 같다.

(1) 먼저 C_i는 자신의 스마트 카드를 리더기에 넣고 자신의 생체정보 B'_i를 입력 받는다. 만약 $d(B_i, B'_i) > \tau$ 이면, 로그인 과정을 중단한다. 그렇지 않으면, C_i는 생체정보의 검증은 완료되었으며, 그 후 사용자 패스워드를 입력한다.

(2) 스마트 카드는 $r'_i = h(PW_i) \oplus f_i$. If $d(r'_i, r_i) > \tau$ 를 계산하여 패스워드를 검증한다. 그 후, $M_1 = e_i \oplus r'$, $M_2 = h(R_c \| T)$, $M_3 = M_1 \oplus M_2$ 을 계산한다. 여기서 M_1은 $h(g_i \| X_s)$와 같으며 R_i는 C_i의 랜덤 넘버이다.

(3) C_i는 $<g_i, M_2, M_3, T>$ 를 S_i에 전송한다.

3. 인증 과정

인증과정에서는 Si를 $<g_i, M_2, M_3, T>$를 전송받은 후 C_i의 적당성을 검증한다. 그림 3은 Jiping 등의 인증과정을 보여준다.

(1) S_i는 $(T^* - T) > \Delta T$ 이면 인증과정을 중단한다. 이때 ΔT 는 시스템이 허용하는 지연 가능한 시간이다. $(T^* - T) \le \Delta T$ 이면 인증과정을 계속 실행한다.

(2) S_i는 $M_4 = h(g_i \| X_s)$와 $M_5 = M_4 \oplus M_3$ 을 계산하고, $M_5 = M_2$ 를 확인한다. 같지 않을 경우 인증과정을 중단한다. 이때 X_s는 서버가 가진 비밀정보이다.

(3) S_i는 $M_6 = h(R_s \| T_s)$ and $M_7 = M_4 \oplus M_6$ 를 생성한 후, $\langle M_4, M_6, M_7, T_s \rangle$ 를 C_i에게 전송한다. T_s 현재 서버의 타임스탬프다.

(4) C_i는 $\langle M_4, M_6, M_7, T_s \rangle$ 를 받은 후, 타임스탬프를 검증한다. 그 후 $M_8 = M_4 \oplus M_7$ 를 계산한 후, M_6과 동일한지 확인한다.

(5) C_i는 $M_9 = M_4 \oplus M_6$를 계산하고 $M_9 = M_7$ 인지 검증한다. 만약 동일하다면, C_i는 $M_{10} = h(R_c \| T')$와 $M_{11} = M_7 \oplus M_{10}$ 를 계산한 후, $\langle M_{11}, R_c, T' \rangle$ 를 S_i에 전송한다.

(6) S_i가 $\langle M_{11}, R_c, T' \rangle$ 를 받은 후, T'의 시간 적정성을 확인한 후, $M_{12} = h(R_c \| T')$ 와 $M_{13} = M_4 \oplus M_6 \oplus M_{12}$를 계산하고 $M_{13} = M_{11}$ 인지를 확인한다. 만약 동일하면 S_i는 C_i의 인증 요청을 받아 들인다.

4. 패스워드 변경 과정

Jiping 등의 스킴에서는 C_i가 자신의 현재 패스워드 $PW_{old\,i}$ 를 변경하고자 할 때, R_c의 도움없이 자유롭게 $PW_{new\,i}$ 로 변경할 수 있다.

(1) C_i는 자신의 스마트 카드를 리더기에 넣고 생체정보 B'_i 를 입력하고 $f'_i = h(B'_i)$를 생성한 후,

$d(f'_i, f_i) \le \tau$ 를 검증한다. 이 때 $f_i = h(B_i)$ 이며 스마트 카드에 저장되어 있다.

(2) (1)의 검증이 완료되면, Ci는 $PW_{old\,i}$ 와 $PW_{new\,i}$ 를 입력한다.

(3) Ci는 $r'_i = h(PW_{old\,i}) \oplus f'$를 계산하고 $d(r'_i, r_i) \le \tau$ 인지를 확인하여 $PW_{old\,i}$ 를 검증한다.

(4) 그 후, 스마트 카드는 computes $r'_i = h(PW_{new\,i}) \oplus f_i$, $e'_i = e_i \oplus r_i$ (= $h(ID_i \| X_s)$), and $e''_i = e'_i \oplus r_i$ 를 계산한다.

(5) 앞에서의 검증이 모두 완료되면, 스마트 카드는 e_i 와 r_i 을 e" 와 r''_i 로 교체하여 저장한다.

Ⅳ. Jiping 등의 스킴에 대한 보안 분석

Jiping 등의 스킴은 Das의 인증 스킴의 최약점을 개선하여 제안했지만, server masquerading attack와 stolen smart-card attack에 대해서 여전히 취약하고 authentication without login phase 의 문제등이 있다.

1. Stolen Smart Card Attack

Kocher 등과 Messerges 등은 스마트 카드의 전력 소비량을 모니터링함으로써, 현재 사용되고 있는는스마트 카드 안에 저장되어 있는 데이터들을 추출할 수 있다는 것을 밝혀냈다. 그러므로 사용자가 분실한 스마트 카드를 공격자가 획득하게 되면, 스마트 카드 안에 저장되어 있는 사용자 정보들을 공격자가 모두 추출해낼 수 있다. Jiping 등의 스킴에서는 스마트 카드 안에 로그인 및 인증 과정에서 사용되는 다양한 정보가 저장되어 있다. 그러므로 공격자는 사용자 스마트 카드 안에서 저장되어 있는 $(h(\cdot), f_i, g_i, e_i, r_i, \tau, d(\cdot))$ 모두를 추출할 수 있다. 이 중 f_i, g_i, r_i 을 이용하여 사용자의 ID와 패스워드를 획득할 수 있다. 그 이유는 $r_i=h(PW_i)\oplus f_i$이므로, $h(PW_i)=r_i\oplus f_i$로 계산할 수 있다. 그리고 $h(ID_i)=g_i$이다. 이를 통해 $h(ID_i)$와 $h(PW_i)$를 계산할 수 있기 때문이다. ID와 PW_i가 오직 해쉬함수로만 보호되고 있는데, 이 두 값은 대부분 엔트로피가 낮아서, 무차별 대입공격을 이용하면 $h(ID_i)$와 $h(PW_i)$로부터 ID와 PW_i를 계산해낼 수 있다. 이러한 문제를 해결하기 위해서는 ID나 패스워드를 보호하기 위해 랜덤 값과 같은 엔트로피가 높은 값을 추가할 필요가 있다. 그림 1은 Jiping 등의 스킴에서의 Stolen Smart Card Attack에 대해서 설명하고 있다[5,6].

Attacker

gets(steals) user's smart card

obtains information from smart card using SPA and DPA

→ gets $h(\cdot), f_i, g_i, e_i, r_i, \tau$ and $d(\cdot)$

Attacker knows f_i, g_i, r_i

$r_i = h(PW_i) \oplus f_i$

→ $h(ID_i) = g_i$

→ $h(PW_i) = r_i \oplus f_i$

executes off-line password attack

→ figures out user's ID and password ID_i, PW_i

그림 1. Jiping 스킴의 stolen smart card Attack
Fig. 1. Jiping Scheme's stolen smart card Attack

2. Authentication without Login Phase

Jiping 등의 스킴에서는 공격자가 사용자의 스마트 카드를 이용하여, 로그인 절차를 거치지 않고 서버에 인증을 받을 수 있다는 취약점이 있다. 즉, 공격자가 사용자의 스마트 카드를 획득하더라도, 서버와 인증을 하기 위해서는 우선적으로 사용자의 ID와 패스워드, 그리고 생체정보 B_i를 이용한 로그인 과정을 겨쳐야만 하지만 Jiping 등의 스팀에서는 이러한 로그인 과정을 생략할 수 있다. 그림 2에서는 로그인 과정 없이 인증을 받을 수 있는 방법을 설명하고 있다[6, 7].

먼저 공격자는 사용자의 스마트 카들 획득한 후, SPA와 DPA 와 같은 스마트 카드 소비 전력 분석 기법을 이용하여 저장된 데이터를 추출한다. 저장된 e_i,g_i와 r_i를 추출하고 공격자 자신의 랜덤 값 R_c를 생성하여, $M_1 = e_i \oplus r_i$, $M_2 = h(R_c \| T)$, $M_3 = M_1 \oplus M_2$ 를 생성하고, $<g_i, M_2, M_3, T>$ 를 S_i에게 전송한다. 그런 후 S_i가 공격자에게 보내온 〈 M_4, M_6, M_7, T_s 〉 를 이용하여 $M_{10} = h(R_c \| T')$와 $M_{11} = M_7 \oplus M_{10}$ 를 생성하고, 〈 M_{11}, R_c, T' 〉 를 C_i에게 전송한다. C_i는 전송받은 값을 이용하여 사용자를 검증하게 되는데, C_i로써는 전송된 값만으로는 정당한 사용자가 보낸 값인지 공격자가 보낸 값인지를 구별할 수 없다. 이러한 과정을 통해서, 공격자는 사용자의 스마트 카드를 이용하여 로그인 과정을 생략하고, 서버에게 인증을 받을 수 있다[5].

Attacker

gets(steals) user's smart card

obtains information from smart card using SPA and DPA

→ gets $h(\cdot), f_i, g_i, e_i, r_i, \tau$ and $d(\cdot)$

computes M_1, M_2, M_3

→ generates random number R_c

→ $M_1 = e_i \oplus r_i$

→ $M_2 = h(R_c \| T)$

→ $M_3 = M_1 \oplus M_2$

sends login and authentication message to S_i

→ $\langle g_i, M_2, M_3, T \rangle$

receives $S_i's$ message

→ $\langle M_4, M_6, M_7, T_s \rangle$

computes M_{11}, R_c, T'

→ generates timestamp T'

→ $M_{10} = h(R_c \| T')$

→ $M_{11} = M_8 \oplus M_{10}$

sends authentication message to S_i

→ $\langle M_{11}, R_c, T' \rangle$

→ attacker can be authenticated with S_i

그림 2. Jiping 스킴에서의 authentication without login phase

Fig. 2. Jiping Scheme's authentication without login phase

3. Server Masquerading Attack

Jiping 등의 스킴에서 공격자는 $h(g_i||X_s)$을 알 수 있기 때문에 적법한 서버로 가장할 수 있다. 그 이유는 서버에서 사용자를 인증할 때 $h(g_i||X_s)$만 을 확인하고 있기 때문이다. 그림 3에서는 Jiping 등의 스킴에서의 Server Masquerading Attack에 대해서 설명하고 있다. 이 공격을 위해 공격자는 우선 사용자가 서버에게 전송하는 메시지 $<g_i, M_2, M_3, T>$를 캡쳐하여 $M_2 \oplus M_3$를 이용하여 $h(g_i||X_s)$를 계산한다. 그것은 $h(g_i||X_s) = e_i \oplus r_i = M_2 \oplus M_3$이기 때문이다. 그러므로 공격자는 정상적인 서버처럼 T_A와 $h(g_i||X_s)$를 이용하여 M_4, M_6, M_7을 계산할 수 있다.

공격자는 이 만들어진 값들을 사용자에게 전달한다. 사용자는 공격자에게 받은 M_4, M_6, M_7을 검증하더라도 정상적인 서버와 구분할 수 없다. 그러므로 사용자는 서버로 인증한 후 M_{11},R_c,andT'를 공격자에게 전송하게 된다. 그러므로 공격자는 사용자에게 정상적인 서버로 인식하게 되며 Server Masquerading Attack 이 성공하게 된다. 이러한 문제를 해결하기 위해서는 서버와 사용자 간의 인증에서 사용되는 비밀값을 추가할 필요가 있다. 이 비밀값은 공격자가 사용자와 서버 간의 통신 내용 상

Client (C_i) — Attacker (A_i)

$M_1 = e_i \oplus r_i'$
$M_2 = h(R_c \| T)$
$M_3 = M_1 \oplus M_2$

(1) A_i intercept client's message $\langle g_i, M_2, M_3, T \rangle$ →

(2) A_i calculates $h(g_i \| X_s) = e_i \oplus r_i' = M_2 \oplus M_3$
(3) A_i masquerades as server
(4) computes $M_4 = h(g_i \| X_s)$
(5) computes $M_6 = h(R_A \| T_A)$
(6) computes $M_7 = M_4 \oplus M_6$

← (7) A_i send message to C_i $\langle M_4, M_6, M_7, T_A \rangle$

(8) when receiving $\langle M_4, M_6, M_7, T_A \rangle$
at T^{**}, C_i checks $(T^{**} - T_A) > \triangle T$?
computes $M_8 = M_4 \oplus M_7$, then verifies $M_8 = M_6$?
(9) computes $M_9 = M_4 \oplus M_6$, then verifies $M_9 = M_7$?
computes $M_{10} = h(R_A \| T')$, and then $M_{11} = M_7 \oplus M_{10}$,

$\langle M_{11}, R_A, T' \rangle$ →

(10) when A_i receives $\langle M_{11}, R_A, T' \rangle$ at, then A_i computes $M_{12} = h(R_A \| T')$
$M_{13} = M_4 \oplus M_6 \oplus M_{12}$, then verifies $M_{13} = M_{11}$?
(11) if it corrects, A_i success to masquerades as server

그림 3. Jiping등 스킴의 Server Masquerading Attack

Fig. 3. Jiping scheme's Server Masquerading Attack

에서 노출되거나 계산되어지지 않은 값이어야 한다[5].

4. 추가적인 보안요구사항

Jiping 등의 스킴에서는 사용자의 생체정보를 사용하는데 일반적인 해쉬함수를 사용한다. 이럴 경우 생체정보가 조금만 다르게 입력되어도 오류가 발생할 확률이 높다. 그러므로 생체정보에는 바이오해쉬함수를 사용하여 오류의 가능성을 낮추고 정확도를 높힐 필요가 있다.

그리고 Jiping 등의 스킴에서는 사용자와 서버간의 세션키를 만들지 않는다. 그래서 인증이 끝난 후에도 안전한 통신을 제공하지 못한다. 그리므로 인증과정에서 세션키 확립 과정을 추가하여 인증후의 안전한 통신을 가능하도록 해야할 것이다.

V. 제안하는 보안성이 향상된 스킴

본 논문에서는 Jiping 등의 스킴에서 발생한 보안취약점 Stolen Smart Card Attack, Authentication without Login Phase, Server Masquerading Attack 을 해결하는 안전한 인증스킴을 제안한다.

그리고 보다 생체정보에는 바이오해쉬를 적용하여 오류의 가능성을 낮추고, 인증과정에서 사용자와 서버간의 세션키를 확립할 수 있도록 하는 과정을 제공한다.

1. 등록 절차

제안하는 스킴에서는 사용자는 R_i에게 등록을 진행하게 되며 그림 4에서 상세히 설명하고 있다.

(1) C_i는 자신의 생체정보 B_i를 스캔 장치에 입력하여, 자신의 ID와 패스워드를 입력한 후, 랜덤넘버 b를 생성하고 $f_i = H_i(B_i)$와 $w_i=h(PW_i||b)$를 계산하여 R_i에게 (ID_i,f_i,w_i)를 전송한다. H()는 생체정보에 사용되는 바이오 해쉬함수이다.

(2) 등록센터 R_i는 $g_i = h(ID_i)$, $r_i = H(g_i||w_i||f_i)$와 $e_i = h(g_i \| X_s) \oplus r_i$ 를 계산한다. X_s는 R_i와 S_i간에 공유된 정보이다. 등록센터 R_i는 사용자의 스마트 카드에 $(h(\cdot), H(\cdot), g_i, r_i, e_i)$에 저장시키고 사용자 C_i에게 안전한 채널로 전송한다

(3) C_i는 R_i에게 스마트카드를 받은 후 랜덤넘버 b를 저장함으로써 과정을 마친다.

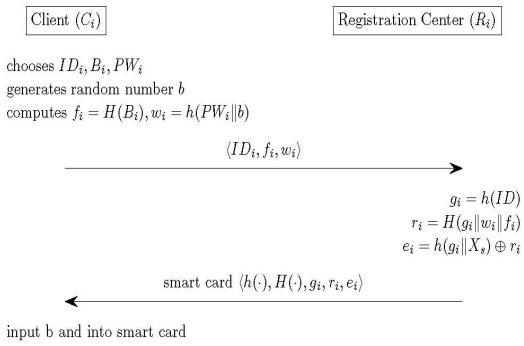

그림 4. 등록절차
Fig. 4. Registration step

2. 로그인절차

제안하는 스킴의 로그인과정에서는 사용자 C_i는 아래와 같이 절차를 실행하며 그림 5와 같다.

(1) 먼저 C_i는 자신의 스마트 카드를 리더기에 넣고 ID_i,PW_i,B_i를 입력한다. 그리고 $g_i = h(ID_i)$, $w_i=h(PW_i||b)$, $f_i=H(B'_i)$계산한 후, 이를 이용하여 r'_i를 계산하고 스마트 카드안에 저장된 r_i와 비교한다. 같이 다르면 로그인 과정을 중단한다. 그렇지 않으면, C_i는 ID, 패스워드 및 생체정보의 검증은 완료되어 다음 절차를 실행한다.

(2) 스마트 카드는 $M_0 = h^2(e_i \oplus r'_i \| T)$, $M_1 = h(M_0)$, $M_2 = h(R_c \| T)$, $M_3 = M_1 \oplus M_2$ 을 계산한다. 여기서 $e_i \oplus r'_i$ 은 $h(g_i \| X_s)$ 와 같으므로 M_0은 $(h(g_i \| X_s)\|T)$ 를 2번, M_1은 3번 해쉬한 값이다. 이값은 $h(g_i \| X_s)$ 의 보호 및 서버를 인증할 때 사용된다.

(3) C_i는 $< g_i, M_2, M_3, T >$ 를 S_i에 전송한다.

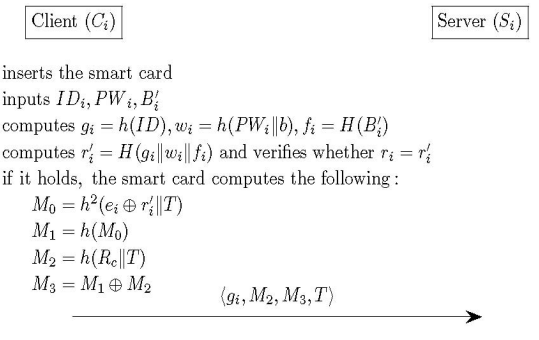

그림 5. 로그인절차
Fig. 5. Login step

3. 인증절차

인증과정에서는 S_i를 $<g_i, M_2, M_3, T>$를 전송받은 후 C_i가 정당한 사용자인지를 확인한다. 그림 7에서는 제안하는 인증과정을 보여준다.

(1) S_i는 $(T^* - T) \le \Delta T$ 인지 확인함으로써, 메시지의 Freshness를 검사합니다. 만약 $(T^* - T) > \Delta T$ 이면 인증과정을 중단한다.

(2) S_i는 C_i가 보내온 T와 g_i그리고 자신이 소유하고 있는 g_i를 이용하여 $M_4 = h^2(h(g_i \| X_s)\|T)$와 $M_5 = h(M_4) \oplus M_3$을 계산하고, M_5와 M_2가 동일한지 확인한다. 이때 X_s는 서버가 가진 비밀정보이다.

(3) S_i 는 $M_6 = h(R_s \| T_s)$ 와 $M_7 = M_4 \oplus M_6$를 계산한 후, $\langle M_4, M_6, M_7, T_s \rangle$를 C_i에게 전달한다. T_s 현재 서버의 타임스탬프다.

(4) C_i는 $\langle M_4, M_6, M_7, T_s \rangle$를 받은 후, 타임스탬프를 T_s를 확인하여 메시지의 Freshness를 검증하고 M_6와 S_i가 보내온 M_4의 동일성을 확인한다.

(5) 그리고 $M_8 = M_4 \oplus M_7$를 계산한 후, M_8와 M_6가 동일한지 확인한다. C_i는 $M_9 = M_4 \oplus M_6$를 계산하고 $M_9 = M_7$ 인지 검증한다. 만약 동일하다면, C_i는 $M_{10} = h(R_c \| T')$와 $M_{11} = M_7 \oplus M_{10}$를 계산한 후, 세션키 $sk = h(R_c\|M_6\|e_i \oplus r'_i)$를 생성한다. 그 후 $\langle M_{11}, R_c, T' \rangle$를 C_i에게 전송한다.

(6) S_i가 $\langle M_{11}, R_c, T' \rangle$ 를 받은 후, T'의 Freshness을 확인한 후, $M_{12} = h(R_c \| T')$ 와 $M_{13} = M_4 \oplus M_6 \oplus M_{12}$ 를 계산한다. 그리고 $M_{13} = M_{11}$ 인지를 확인한다. 만약 동일하면 S_i는 C_i의 인증 요청을 받아들인다. 그리고 세션키 $sk = h(R_c\|M_6\|e_i \oplus r'_i)$를 생성하여 추후에 C_i와의 안전한 통신에 사용한다.

4. 패스워드 변경 절차

본 논문이 제안하는 스킴에서는 C_i가 R_c의 도움을 받지 않아도 자신의 현재 패스워드 $PW_{old\,i}$ 를 새로운 $PW_{new\,i}$ 로 자유롭게 변경할 수 있다.

(1) C_i는 자신의 스마트 카드를 리더기에 넣고 생체정보 ID_i, B'_i, PW_{oldi}를 입력한다. 입력값과 b를 이용하여 g_i, f_i, w_i를 생성한다.

(2) 그 후 $r'_i = H(g_i\|w_i\|f_i)$를 생성하고 저장된 r_i값과 비교하여 동일성을 확인하고 $h(g_i\|X_s) = e_i \oplus r_i \oplus r'_i$를 계산한다.

(3) 그리고 PW_{new} 를 입력하고 랜덤넘버 b'를 생성하고 $w'_i = h(PW_{newi}\|b')$, $r''_i = H(g_i\|w'_i\|f_i)$, $e'_i = h(g_i\|X_s) \oplus r''_i$를 계산하다.

(4) 앞에서의 검증이 모두 완료되면, 스마트 카드는 b, e_i 와 r_i 을 b', e''와 r''_i 로 교체하여 저장함으로써 패스워드 교체를 마친다.

Client (C_i)

inputs ID_i, B_i, PW_{old}
computes $g_i = h(ID), f_i = H(B_i), w_i = h(PW_{old}\|b)$
computes $r'_i = H(g_i\|w_i\|f_i)$ and verifies whether $r_i = r'_i$
$h(g_i\|X_s) = e_i \oplus r_i \oplus r'_i$
inputs new password PW_{new}
generates random number b'
computes $w'_i = h(PW_{new}\|b')$
$r''_i = H(g_i\|w'_i\|f_i)$
$e'_i = h(g_i\|X_s) \oplus r''_i$
replaces b, r_i, e_i into b', r''_i, e'_i

그림 6. 패스워드 변경 절차
Fig. 6. Password change setp

Ⅵ. 안전성 분석

본 장에서는 제안하는 스킴의 안전성을 분석하기 위해서 일반적인 보안 요구사항을 만족하는 지와 스킴에 대한 공격에 안전한 지를 분석한다.

- (01) Mutual authentication: Ci 와 Si 는 $h(h(g_i||X_s)||T), M_0=M_4=h^2(h(g_i||X_s)||T), M1=h^3(h(gi||Xs)T)$을 이용하여, 상호 인증을 확인한다. 즉 위의 값들을 이용해서 C_i는 $h(g_i||X_s)$을 소유하고 있는지, S_i는 X_s을 소유하고 있는지를 확인하는 것이다[8,9].
- (02) Denial of Service : 제안하는 스킴에서는 C_i와 S_i간의 통신에 사용하는 메시지에 타임스탬프를 사용하여 DoS 공격을 방지한다. 즉 M_2, M_6, M_{11}에 각각 T, T_s,T'가 포함되어 있어 다량의 예전 메시지를 재전송을 하는 DoS 공격은 막을 수 있다. 또한 $r' = H(g_i||w_i||f_i)$를 검증하게 되는데, 공격자는 사용자의

ID, 패스워드 및 생체정보 중 하나라도 없으면, 처음 검증과정을 통과하지 못하므로 로그인 값을 계속 입력하는 DoS 공격을 효율적으로 방지할 수 있다.

- (03) Stolen-Verifier Attack : 제안하는 스킴은 ID, $f_i = H_i(B_i)$와 $w_i=h(PW_i||b)$만을 R_i에게 전송하므로R_i는 B_i와 PW_i를 알아낼 수 없다. 또한 Si도 Ci와의 통신과정에서 $g_i=h(ID)$밖에 알 수 없다. 그러므로 R_i및 S_i모두 패스워드 테이블 및 생체정보 테이블과 같은 Verifier를 소유할 수 없다. 그러므로 Stolen-Verifier Attack 에 안전하다.
- (04) Many Logged-In Users Attack : 제안하는 스킴에서는 스마트 카드가 없으면, 로그인 및 인증과정을 진행할 수 없다. 그건 사용자의 ID, 패스워드, 생체정보를 완벽히 입력해야 로그인을 통과할 수 있으며, 입력값을 이용하여야만 계산할 수 있는 $h(g||X_s)$이 스마트 카드 안에 저장되어 있고 $h(g_i||X_s)$이 있어야만 인증과정을 통과할 수 있다. 스마트 카드가 없는 다른 사용자들이 자유롭게 로그인 및 인증이 가능하지 못하므로 Many Logged-In Users Attack에 안전하다.
- (05) Guessing attack : 제안하는 스킴에서는 생체정보 및 패스워드를 함께 사용하므로써, 패스워드만 사용하였을 발생할 수 있는 Guessing attack에 안전하다. 다시 말해, 스마트 카드 안에 패스워드를 포함하고 있는 값은 $r_i = H(g_i||w_i||f_i)$뿐인데, 이 값에는 사용자의 ID 및 생체정보, b 값까지 알아야만 생성할 수 있는 값이므로, 패스워드 추측 공격이 매우 어렵다[5].
- (06) Replay Attack : 제안하는 스킴에서는 공격자가 사전에 획득한 메시지를 사용자에게 다시 전송하는 공격에 안전하다. 그 이유는 모든 메시지 타임스탬프를 추가하여 항상 메시지의 Freshness를 체크하기 때문이다. 예를 들어 예전에 확보한 메시지 $< g_{ip}, M_{2p}, M_{3p}, T_p >$를 사용자에게 그대로 전송하게 되면 보내온 타임스탬프 T_p가 ΔT 를 만족하기 못하게 된다. 이를 피하기 위해서 현재의 타임스탬프 T만 바꾸어 $< g_{ip}, M_{2p}, M_{3p}, T >$를 보내게 되면 ΔT 에는 만족하지만, 보내온 M_{2p}와 계산한 M_5를 비교하는 과정에서 타임스탬프 T가 다르기 때문에 일치성을 만족하지 못하게 된다.

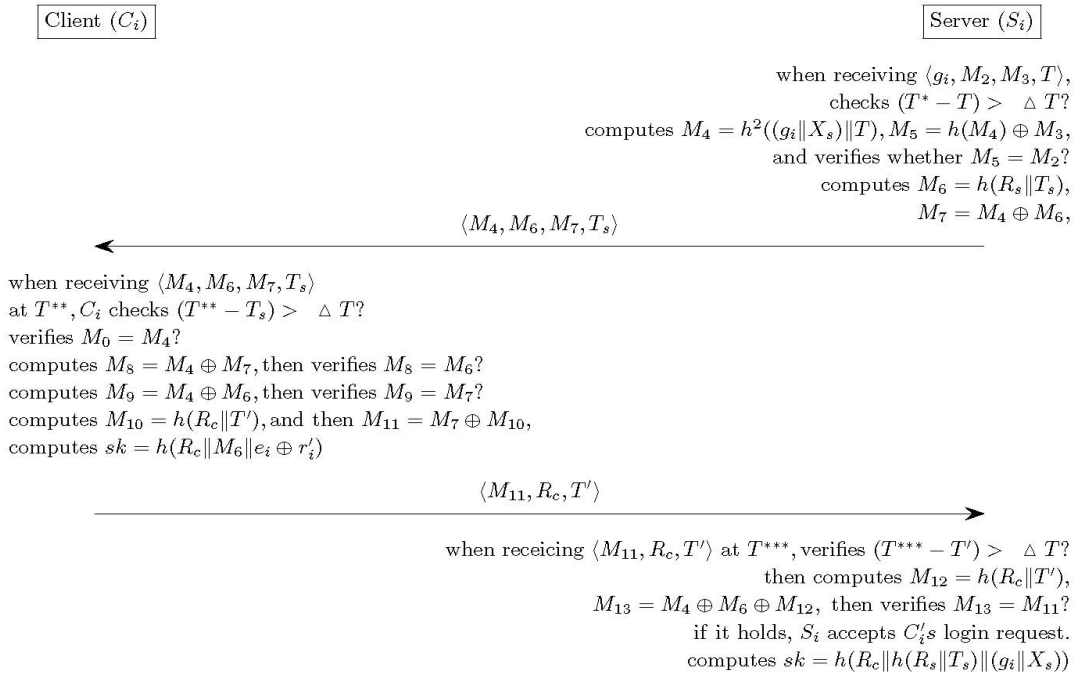

그림 7. 제안하는 인증 과정
Fig. 7. The proposed authentication step

- (07) User Impersonation Attack : 사용자가 로그인 과정에서 사용하는 <g_i,M_2,M_3,T>은 기본적으로 ID 값을 해쉬한 g_i를 사용하기 때문에 공격자는 사용자의 ID를 알 수가 없다. 더욱이 공격자가 사용자의 ID를 알더라도, ID에 해당하는 $h(g_i||X_s)$값을 알 수가 없다. 그것은 사용자도 $h(g_i||X_s)$를 알기 위해서는 자신의 스마트 카드와 ID, 패스워드, 생체정보까지 모두 알고 있어야하는데, 공격자라고 해도 이 모든 것을 알기는 불가능하기 때문이다. 더욱이 공격자가 로그인 과정을 생략 하고 인증과정을 진행하더라도 공격자는 $h(g_i||X_s)$를 알아내지 못하기에, 격자는 서버에게 인증을 받을 수 없다.
- (08) Server Masquerading Attack : 제안하는 스킴에서는 공격자가 정당한 서버로 가정하여 사용자와 통신을 할 수 없다. 그건 사용자는 서버가 $h(g_i||X_s)$, 즉 X_s를 소유하고 있는지 확인함으로써 서버를 인증하기 때문이다. 본 스킴에서 사용자는 서버에게 $h^3(g_i||X_s)$을 전송하고 서버에게 $h^2(gi||Xs)$를 받는 것을 검증하게 된다. $h^3(g_i||X_s)$을 받은 서버라도 $h^2(gi||Xs)$를 생성하기 위해서는 X_s를 알아야만 가능하다. 그러므로 X_s 를 모르는 공격자는 $h^3(g_i||X_s)$를 알더라도 $h^2(g_i||X_s)$를 생성할 수 없으므로 정당한 서버로 가장할 수 없다 [8,9].
- (09) Insider Attack : 본 스킴에서는 등록과정에서 R_i에게 $w_i=h(PW_i||b)$,$f_i=H(B'_i)$만을 전송한다. 즉 패스워드나 생체정보를 평문으로 전달하지 않고 반드시 해쉬함수를 거친 후 전송함으로써, 원래 값들을 알 수 없도록 한다. 그래서 등록센터의 내부자라도 사용자의 PW_i나 B'_i를 알 수가 없다. 또한 사용자와의 인증과정에서는 사용자는 PW_i나 B'_i와 관련된 정보는 인증서버에게 전달하지 않으므로 인증서버도 사용자의 PW_i나 B'_i를 알 수가 없다. 따라서 킴은 내부자 공격에 안전하다.
- (10) Man-in-the-Middle Attack : 중간자 공격이란 정상적인 사용자와 서버 간의 통신내용을 가로챈 공격자가 이를 이용하여 사용자와 서버에게, 정상적인 서버 및 사용자인 척하면 통신을 진행할 수 있는 것을 말한다. 하지만 제안하는 스킴에서는 우선 서버와 사용자 간의 상호인증을 하기 때문에 중간자 공격이 어렵고 더욱이, 각각의 메시지에 타임스탬프를 적용하여 기존의 정상적인 통신내용을 전송하더라도 현재 시간과의 차이 때문에 인증을 받을 수 없다. 그러므로 제안하는 스킴은 중간자 공격에 안전하다.
- (11) Stolen Smart Card Attack : 제안하는 스킴에서 공격자가 사용자의 스마트 카드를 획득하게 되면, 공격자는 SPA나 DPA 기법을 이용하여 ($h(\cdot)$, $H(\cdot)$,b, g_i, r_i, e_i)를 추출해낼 수 있다. 하지만 $g_i = h(ID_i)$, $r_i = H(g_i||w_i||f_i)$, $e_i = h(g_i \| X_s) \oplus r_i$ 를 알더라도 사용자의 패스워드나 생체정보를 계산해 낼 수 없다. 그 이유는 $w_i=h(PW_i||b)$, $f_i = H_i(B_i)$가 $r_i = H(g_i||w_i||f_i)$에 함께 포함되어 있어서 엔트로피가 낮은 패스워드를 추출해내기 위해서는 엔트로피가 높은 생체정보를 알고 있어야 한다. 즉, $a = h(PW_i)$에서 a를 공격자가 알고 있는 계산식이 만들어 지지 않는다. 공격자가 패스워드를 알아내기 위해서는 사용자의 생체정보를 알아야 하지만, 공격자는 생체정보를 알아낼 수 없다.
- (12) Authentication without Login Phase : Jiping 등의 스킴에서는 서버와 사용자간의 인증에서 사용되는 $e_i \oplus r_i$ 즉 $h(g_i \| X_s)$ 가 통신 상에서 노출됨으로써, 공격자가 스마트카드를 이용한 로그인 과정 없이도 사용자인 척 서버에게 인증을 받을 수 있었다. 하지만 제안하는 스킴에서는 인증과정에서 $h(g_i \| X_s)$ 값을 해쉬하는 횟수를 조절함으로써, 공격자가 인증과정에서 $h(g_i \| X_s)$ 값을 알 수 없게 하였다. 즉 사용자가 서버에게 보내는 인증메세지에서는 $h^3(g_i \| X_s)$ 를 사용하고, 그 후 서버가 사용자에게 보내는 메시지에서는 $h^2(g_i \| X_s)$를 사용함으로써, $h(g_i \| X_s)$를 알 수 있는 정당한 사용자와 서버만이 인증과정을 진행할 수 있도록 하였다. 그러므로 $h(g_i \| X_s)$ 를 알 수 없는 공격자는 로그인 절차 없이는 인증을 진행할 수 없다. 더욱이 공격자는 로그인 절차를 수행하더라도 사용자의 ID, 패스워드, 생체정보를 모르면 $h(g_i \| X_s)$를 알 수 없으므로 안전하다.
- (13) Server Masquerading Attack : Jiping 등의 스킴에서는 $h(g_i||X_s)$ 를 사용자와 서버간의 인증과정에서 알아낼 수 있었다. 이 값을 이용하여 공격자는 서버인 척 가장하여, 사용자와 인증절차를 진행할

수 있었다. 하지만 제안하는 스킴에서는 앞에서 설명한 것 처럼, 해쉬함수의 실행 횟수를 변형하는 방식을 통해 $h(g_i||X_s)$ 를 안전하게 보호하므로, 공격자는 서버인척 가장할 수 없다.

- (14) Biometric Recognition Error : Jiping 등의 스킴에서는 일반적인 해쉬함수만을 이용하기 때문에, 생체정보를 입력하는 과정에서 입력값이 조금만 달라지면 오류가 발생할 가능성이 매우 높다. 하지만 제안하는 스킴에서는 생체정보값을 처리해야할 때에는 바이오해쉬함수를 이용함으로써, 생체정보의 특성상 입력값이 조금씩 달라지더라도 일정한 결과값을 계산해주어 오류가 발생할 확률이 줄어들었다.
- (15) Session key establishment: Jiping 등이 제안하는 스킴에서는 사용자와 서버간의 인증과정이 완료되더라도, 둘 간의 세션키가 만들어지지 않는다. 그래서 인증 후 둘만의 안전한 통신을 할 수가 없다. 하지만 제안하는 스킴에서는 인증과정에서 사용자와 서버 간의 주고 받은 메시지를 이용하여 세션키 $sk = h(R_c||M_6||e_i \oplus r'_i)$를 생성함으로써, 인증 후의 둘만의 안전한 통신이 가능하도록 하였다. 이 세션키는 사용자와 서버가 인증 과정을 마지막까지 완료하여야만 만들 수 있기 때문에, 공격자는 세션키를 알아낼 수가 없다.

표 2에서는 기존의 스킴들과 제안하는 스킴의 안정성을 비교하고 있다. 표 1에서 알 수 있듯이 Das의 스킴, Li-Hwang의 스킴, Jiping 등의 스킴은 각각 다양한 보안성의 문제점을 가지고 있다. 제안하는 스킴에서는 다른 스킴에서 발생하고 있는 문제점들을 해결하였다.

표 2. 다른 스킴들과의 비교
Table 2. Comparison of the other schemes

보안 요구사항	Das	Li-Hwang	Jiping	제안 스킴
(01)	No	No	Yes	Yes
(02)	No	No	Yes	Yes
(03)	Yes	Yes	Yes	Yes
(04)	Yes	Yes	Yes	Yes
(05)	No	Yes	Yes	Yes
(06)	No	No	Yes	Yes
(07)	No	No	Yes	Yes
(08)	No	No	Yes	Yes
(09)	No	No	Yes	Yes
(10)	Yes	No	Yes	Yes
(11)	Yes	Yes	No	Yes
(12)	Yes	Yes	No	Yes
(13)	Yes	Yes	No	Yes
(14)	No	No	No	Yes
(15)	No	No	No	Yes

Ⅶ. 결론

본 논문에서는 Das의 스킴을 개선한 Jiping 등의 스킴을 분석하였다. 이를 통해, Jiping 등이 제안한 스킴은 여전히 다양한 보안 취약점을 가지고 있다는 것을 밝히고, 이러한 취약점을 해결한 본 논문에서는 Jiping 등이 제안한 스킴에 대한 취약점 분석을 통해 발견된 문제점을 해결하기 위해서 안전성이 개선된 생체정보 기반의 사용자 인증 스킴을 제안하였다. 그리고 제안한 스킴을 보안성 분석을 통해 안전성을 검증하고, 다른 생체정보 기반의 인증 스킴과 비교하였다.

References

[1] M. Kim and C. K. Koc, “Asimple attackon a recently introduced hash-based strong-password authentication scheme,” International Journal of Network Security, vol. 1, no. 2, pp. 77 - 80, 2005.

[2] A. K. Das, “Analysis and improvement on an efficient biometric based remote user authentication scheme using smart cards,” IET Information Security, vol. 5, no. 3, pp. 145 - 151, 2011.

[3] C. T. Li, “An enhanced remote user authentication scheme providing mutual authentication and key agreement with Smart Cards,” in Proceedings of the 5th International IEEE Computer Society Conference on Information Assurance and Security, pp. 517 - 520, Xi’an, China, 2009.

[4] L. Jiping, D. Yaoming, X. Zenggang, and L, Shouyin, “An improved biometric-based user authentication scheme for C/S system,” International Journal of Distributed Sensor

Networks, 2014.
[5] Younsung Choi, et al. “Cryptanalysis of Improved Biometric-Based User Authentication Scheme for C/S System”, International Journal of Information and Education Technology, vol. 5, no.7, 2015
[6] N.Y. Lee and Y.C. Chiu, “Improved remote authentication scheme with smart card,” Computer Standards and Interfaces, pp. 177 - 180, 2005.
[7] P. Kocher, J. Jaffe, B. Jun, “Differential power analysis,” in Proc. The 19th Annual International Cryptology Conference on Advances in Cryptology, 1999, pp. 388-397.
[8] Seung-Cheol Lim, ″ A Real-Time Intrusin Detection based on Monitoring in Network Security″, Journal of the institute of Inernet, Broadcasting and Comm, vol. 13, issue 3, pp.9-15, Jun. 2013.
[9] J. Nam, K. K. R. Choo, M. Kim, J. Paik and D. Won, “Dictionary Attacks against Password-Based Authenticated Three- Party Key exchange protocols,” KSII Transactions on Internet and Information Systems, vol. 7, no. 12, 2013, pp. 3244-3260.

저자 소개

양 형 규(정회원)

- 1985년 2월 : 성균관대학교 석사
- 1995년 2월 : 성균관대학교 정보공학과 공학박사
- 1995년 ~ 현재 : 강남대학교 컴퓨터미디어정보공학부 교수
- 1984년 12월 ~ 1990년 2월 : 삼성전자 컴퓨터부문 선임연구원

<주관심분야 : 정보보안, 네트워크 보안, DRM>

※ 본 연구는 강남대학교 교내연구비 지원 연구임.