논문 2012-07-07

홈네트워크 상에서 속성정보를 이용한 티켓기반의 인증 프로토콜 (Ticket-Based Authentication Protocol Using Attribute Information over Home Network)

이 원 진, 김 기 원, 김 현 성*

(Won-Jin Lee, Kee-Won Kim, Hyunsung Kim)

Abstract : Recently, LEE et al. proposed an attribute-based authenticated key agreement protocol over home network, which aimed to support authentication and key agreement between user and home server. However, if the home server is attacked in the protocol, the effects are influenced to the overall home network components severely. Thereby, this paper proposes a new ticket-based authentication protocol using user attributes between user and home devices to solve the problem. The proposed protocol supports the various levels of security to user by diversifying the network accessibility depending on user attribute. Thereby, the protocol could support more secure home network services.

Keywords : Home Network, User Authentication, Ticket-based, ABE(Attribute based Encryption)

1. 서 론

홈네트워크 기술은 가정 내의 모든 정보가 전 기기가 유무선 네트워크로 연결되어 기기, 시간, 장소의 제약없이 다양한 고품질의 홈서비스를 제공할 수 있도록 하는 미래지향적 가정환경을 제공하는 기술이다[1]. 이러한 홈네트워크는 다양한 사이버 공격의 대상이 될 수 있으므로 정보보안 문제는 홈네트워크 활성화를 위해서 필수적으로 해결해야 할 중요한 문제이다. 특히 다양한 보안 취약성으로 인해 개인의 프라이버시 침해 뿐 아니라 개인의 생명 및 자산의 피해 사건을 포함한 다양한 문제들이 발생하고 있다. 그러므로 보다 안전하고 신뢰성 있는 홈네트워크 서비스를 제공하기 위해서는 인증

및 키교환, 접근제어, 그리고 침입차단 및 침입탐지 등의 고려해야 할 보안요소들이 많이 존재한다. 그 중에서도 홈네트워크를 위한 사용자 인증 문제는 홈네트워크 보안에 있어서 가장 중요한 요소이며, 필수적으로 선행되어야 할 문제이다[2-4].

홈네트워크 인증을 위한 국내표준은 한국정보통신기술협회(TTA)에 의해 EEAP-PW가 채택되었으며, 국제 표준화 작업은 ITU-T Study Group 17, Question 9에서 TTA 표준을 토대로 X-homesec-3란 이름으로 표준화 작업을 진행하고 있다[5-6]. 특히, 홈네트워크에서의 사용자 인증은 안전한 홈네트워크 서비스를 제공하기 위한 필수 선행 기술이다[2-3]. 홈네트워크 인증을 위해 가장 많이 사용되고 있는 기법은 EAP-MD5(Extensible Authentication Protocol -MD5)이다[7]. 하지만, EAP-MD5는 인증서버만 사용자를 인증하는 단방향 인증을 제공하고 키 생성 기능을 제공하지 못하기 때문에 중간자공격(Man-In-The-Middle attack)과 서비스거부(Denial of Service)에 취약한 문제점이 존재한다. 2006년 TTA는 EAP-MD5의 취약점들을 개선하기 위해서 EEAP-PW(Encrypted Extensible Authentication Protocol-PW)를 표준화하였다[8]. 하지만, EEAP-PW 또한 키 전송과정에서 전방향안전성(Forward

* 교신저자(Corresponding Author)

논문접수 : 2011. 09. 08., 수정일: 2011. 10. 25.,

채택확정 : 2011. 11. 02.

이원진 : 단국대학교, 김기원 : 우석대학교

김현성 : 경일대학교 컴퓨터공학부

※ 본 연구는 2010년 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 연구임(한국연구재단2010-0021575)

Secrecy)을 제공하지 못하는 것을 포함한 몇 가지 보안 취약점들이 여전히 존재한다. 이러한 문제들을 해결하기 위하여 논문[9]에서는 EEAP-PW 프로토콜의 문제점들을 분석하고 이를 효율적으로 해결할 수 있는 속성기반 인증된 키교환 프로토콜을 제안하였다.

사용자 인증 기법은 Lamport에 의해 처음 제안되었고, 패스워드를 이용한 안전한 원격 패스워드 인증 기법과 TTP(Trusted Third Party)기반 기법을 포함한 다양한 기법 형태로 발전하였으나 이들 기법들은 대부분 패스워드 테이블에 대한 공격에 취약하였다[10-11]. 2006년 Mangipudi와 Katti는 사용자 익명성을 제공하는 서비스 거부 공격에 강한 프로토콜을 제안하였다[12]. 인터넷이 보편화 되고, 다양한 유무선 응용프로그램이 개발됨에 따라 다양한 형태의 사용자 접근제어에 대한 요구사항이 도출되었다. 이러한 요구사항에 따라서 인증의 다양성을 제공하는 속성 기반 암호(Attribute based Encryption, ABE)기법이 Waters에 의해 제안되었다[13-14]. ABE는 속성 값을 암호 인자로 사용하여 동일한 속성을 가진 사용자만이 암호화된 데이터를 복호할 수 있는 암호 기법이다. 특히, 홈네트워크 서비스는 가족 구성원들(관리자, 성인, 어린이, 노인 등)과 원격 관리자들(수도, 전기, 가스 점검 등) 등을 포함한 다양한 목적을 지원할 수 있는 효율적인 접근제어 기법을 제공할 필요성이 있다. 만약 어린이나 노인들에게 화재발생을 야기할 수 있는 홈장비 서비스의 접근을 허용하게 되면 치명적 사고가 발생할 수도 있다. 또한, 원격 관리자들에게 가족 구성원들의 민감한 정보에 대한 접근성을 허용해서도 안된다. 그러므로 홈네트워크 서비스를 이용하는 사용자에 따른 서비스의 차별화된 접근성을 제시할 수 있는 인증프로토콜의 개발이 필요하다.

논문[9]는 속성 기반 암호 시스템을 이용한 다양한 레벨의 보안을 제공할 수 있는 속성 기반 사용자 인증 프로토콜을 제안하였다. 이 프로토콜은 사용자의 속성에 따라 차별화된 홈네트워크 접근 서비스를 제공한다. 이 프로토콜은 사용자 등록 단계와 인증 단계로 구성되는데, 등록단계에서는 사용자 정보와 패스워드 및 속성 관련 정보를 서버에 등록한다. 인증 단계에서는 등록된 정보의 소유 여부를 통해서 사용자와 홈서버 간에 양방향 인증을 수행한다. 하지만, 논문[9]에서 제안한 프로토콜의 사용자 인증은 홈서버의 안전성에 기반하고 있다. 만약 홈서버의 안전성에 문제가 발생한다면, 이는 홈네트워크 전반에 걸친 문제로 확대될 수 있다.

본 논문에서는 논문[9]의 문제 및 기존의 홈네트워크 인증 프로토콜들의 문제를 해결하기 위한 사용자, 홈서버, 홈 장비간의 상호인증을 제공하는 새로운 속성정보를 이용한 티켓기반 인증 프로토콜을 제안한다. 특히, 속성 기반 암호 시스템의 속성을 활용하여, 사용자의 속성에 따른 다양한 레벨의 보안을 제공할 수 있다.

본 논문의 구성은 2장에서는 제안한 프로토콜에 대하여 상세히 설명하고 3장에서는 제안된 프로토콜의 안전성 분석을 제시하며 마지막으로 4장에서는 결론을 맺는다.

II. 제안한 속성기반 인증 프로토콜

본 장에서는 사용자, 홈서버, 홈장비간의 상호인증을 제공하고, 사용자의 속성 값을 이용하여 차별화된 홈네트워크 서비스를 제공하는 속성기반 인증 프로토콜을 제안한다. 초기 사용자 인증과정에서 홈서버가 사용자에게 티켓을 발급함으로써 여러번 인증이 필요한 응용에서 인증 시 발생하는 통신 및 연산의 오버헤드를 줄일 수 있다.

2.1 표기법

본 절에서는 프로토콜에서 이용할 표기법을 표 1과 같이 정의한다.

표 1. 프로토콜 표기법
Table 1. Notations of Protocol

표기	의 미
ID_U, ID_D, ID_H	사용자, 홈장비, 홈서버의 식별자
PW_U	사용자의 패스워드
x_s	홈서버의 비밀키
k	홈서버와 홈장비간 사전에 공유된 비밀키
AC_{ID_i}	ID_i 홈장비에 대한 접근리스트
a	사용자의 랜덤 값 ($a \in Z_p$)
b	홈장비의 랜덤 값 ($b \in Z_p$)
f_K^l	키 K 를 이용한 MAC(Message Authentication Code) 함수
T_i	i 가 생성한 타임스탬프

2.2. 프로토콜 수행 과정

제안하는 프로토콜은 크게 사용자 등록 단계와 사용자 인증 단계로 구성된다. 먼저 등록단계에서는 사용자 식별자, 패스워드 및 속성 정보를 서버에 등

록한다. 사용자 인증단계에서는 등록된 사용자 정보의 소유 여부를 통해서 사용자와 서버 간에 양방향 인증을 수행하고 티켓을 발급한다. 이후 추가적인 인증 오버헤드를 줄이기 위해서 티켓을 이용한 인증과정을 수행한다.

그림 1. 등록 단계

Fig. 1 Registration Phase

2.2.1 등록단계

등록단계에서 사용자는 그림 1과 같이 자신의 개인 정보와 속성정보를 안전한 채널을 통해 전송하고, 홈서버는 사용자의 정보를 등록한다. 홈서버는 자신과 연결된 모든 홈장치(ID_i)에 대한 접근리

스트(AC_{ID_i})를 유지한다. 이때, 접근리스트는 사용자의 속성정보에 따라 홈장비에 대한 접근가능 여부를 확인할 수 있는 목록이다. 등록단계의 전체적인 처리과정은 다음과 같다.

단계1. 사용자는 홈서버에게 자신의 식별자 ID_U 와 패스워드 PW_U 그리고 속성 값 A_n 을 포함한 메시지 $M_1 = \{ID_u, PW_u, A_n\}$ 을 안전한 채널을 통해 전송한다. 여기서 A_n 은 사용자의 n 개의 속성값으로 $A_n = \{a_1, a_2, \dots, a_n\}$ 이다.

단계2. 메시지 M_1 을 받은 홈서버는 $V_{PW_u} = g^{PW_u} \bmod p$ 를 계산하고 자신의 비밀키 x_s 를 이용하여 사용자 정보 AK 를 계산한다.

$$AK = \bigoplus_{j=1}^n ak_j \quad (1)$$

여기서 ak_j 는 사용자의 속성 값 $A_n = \{a_1, a_2, \dots, a_n\}$ 과 서버의 비밀키 x_s 를 이용하여 다음과 같이 계산한다.

$$ak_j = h(a_j \oplus x_s), 1 \leq j \leq n \quad (2)$$

그림 2. 초기 인증단계

Fig. 2 Initial Authentication Phase

그림 3. 티켓기반의 인증단계

Fig. 3 Ticket-based Authentication Phase

홈서버는 각 장비에 사용자의 접근 허용 여부를 확인한 후 사용자의 AK 값을 그 사용자가 접근 권한을 가진 각 홈장비 접근 리스트(AC_{ID_i})에 포함시킨다.

2.2.2 인증단계

인증 단계에서 홈서버는 사용자 속성에 따른 인증을 수행한다. 특히, 이때 다양한 서비스에 효율적인 접근을 제공하기 위한 티켓을 발급한다. 그림 2는 초기 인증 단계의 전체적인 수행 과정을 보여주며 상세한 수행 과정은 다음과 같다.

단계1. 사용자는 랜덤 값 $a \in Z_p$ 를 선택하고, $A = g^a \bmod p$ 를 계산한 후 $V_{PW_u} = g^{PW_u}$ 와 $EV = V_{PW_u} \oplus T_U$ 를 계산한다. 또한 사용자 속성값 $A_n = \{a_1, a_2, \dots, a_n\}$ 과 타임스탬프 T_U 를 포함한 $MAC_{UH} = f_{EV}^1(A \parallel ID_U \parallel T_U \parallel A_n)$ 를 계산하여 메시지 $M_1 = \{ID_U, ID_H, A, T_U, MAC_{UH}\}$ 을 홈장비에게 전송한다.

단계2. M_1 을 받은 홈장비는 자신의 ID_D 정보를 포함하여 $M_2 = \{ID_D, ID_U, ID_H, A, T_U, MAC_{UH}\}$ 메시지를 홈서버에게 전송한다.

단계3. 홈서버는 현재 타임스탬프 T 를 이용하여 $T - T_U \leq \Delta T$ 연산을 통해서 메시지 M_2 가 적법한 시간 범위에 전송되었는지를 확인한다. 여기서 ΔT 는 전송 지연이 고려된 적법한 전송 시간 범위이다. 적법한 전송 지연 ΔT 는 네트워크 환경에 따라 다양하게 조정될 수 있다. 홈서버는

$EV' = V'_{PW_U} \oplus T_U$, $f_{EV'}^1(A \parallel ID_U \parallel T_U \parallel A_n)$ 를 계산한 후 MAC_{UH} 와 비교하여 메시지의 적법성 여부 확인 후, 적법하면 사용자의 속성 정보가 해당 홈장비 접근리스트에 존재하는지 확인한다. 즉

$$ak'_j = h(a_j \oplus x_s), 1 \leq j \leq n \text{ 와 } AK' = \bigoplus_{j=1}^n ak_j \text{ 을 계산하여, 계산한 } AK' \text{ 과 저장된 } AK \text{ 가 같은지 비교한다. 그리고 사용자의 } AK \text{ 가 해당 홈장비 접근리스트 } AC_{ID_D} \text{ 에 포함되어 있는지를 확인한다. 위의 모든 검증과정을 통과하면}$$

$X = V_{PW_U} \oplus ID_U$ 를 계산 하고, 홈서버와 홈장비 사이에 사전에 공유된 키 k 로 $ID_U, LifeTime, h(X)$ 를 암호화하여 티켓을 다음과 같이 발급한다.

$$Ticket = E_k(ID_U, LifeTime, h(X)) \quad (3)$$

그리고 홈서버는 $MAC_{HU} = f_{EV}^1(X \parallel Ticket)$ 와 $MAC_{HD} = f_k^1(ID_D \parallel ID_H \parallel T_H)$ 를 계산한 후, 메시지 $M_3 = \{Ticket, MAC_{HU}, MAC_{HD}, T_H\}$ 을 홈장비에게 전송한다.

단계4. 홈장비는 타임스탬프 T_H 의 적법성을 검사하고, $MAC_{HD} = f_k^1(ID_D \parallel ID_H \parallel T_H)$ 의 검증을 통해 메시지의 적법성을 확인한 뒤 티켓의 유효성을 검증한다. 적법한 메시지인 경우 랜덤 값 $b \in Z_p$ 를 선택하여 $B = g^b \bmod p$, $DH_S = A^b \bmod p$ 와 $SV = h(X) \oplus T_D$ 계산한 후, $MAC_{DU} = f_{SV}^1(B \parallel ID_D \parallel DH_D \parallel T_D)$ 을 계산하며, 메시지 $M_4 = \{Ticket, B, MAC_{HU}, MAC_{DU}, T_D\}$ 를 사용자에게 전송한다.

단계5. 메시지 M_4 를 받은 사용자는 타임스탬프 T_D 의 적법성을 검사하고, $DH_U = B^a \bmod p$, $X = V_{PW_U} \oplus ID_U$ 와 $SV = h(X) \oplus T_D$ 를 계산한다. 그리고 $MAC_{DU} = f_{SV}^1(B \| ID_D \| DH_D \| T_D)$ 와 $MAC_{HU} = f_{EV}^1(X \| Ticket)$ 의 검증을 통해 적법한 메시지 여부를 판단한다.

2.2.3 티켓을 이용한 인증

제안한 인증 프로토콜의 초기 인증 단계를 매 인증시 사용한다면 서버의 연산 및 통신 오버헤드가 커지는 문제점이 있다. 이러한 문제점을 해결하기 위해서 본 논문에서는 초기 인증 후 추가적인 인증이 필요할 경우에 홈서버로부터 발급 받은 티켓을 이용하여 인증을 수행한다. 그림 3은 초기 인증 단계 이후 추가적인 인증이 필요할 때 티켓을 이용한 인증을 수행하고, 처리 과정은 다음과 같다.

단계1. 사용자는 $MAC_{UD} = f_{SV}^1(ID_U \| Ticket \| T_U)$ 를 계산하고, 자신의 ID정보와 티켓 및 타임스탬프 T_U 를 포함한, $M_1 = \{ID_U, MAC_{UD}, Ticket, T_U\}$ 을 홈장비에게 전송한다.

단계2. M_1 을 받은 홈 장비는 타임스탬프 T_U 의 적법성을 검사하고, $MAC_{UD} = f_{SV}^1(ID_U \| Ticket \| T_U)$ 의 검증을 통해 메시지의 적법성을 확인한다. 홈서버와 공유하는 공통키(k)로 티켓을 복호화하여 티켓의 Life Time 유효성을 검증한다.

$$D_k(Ticket) = (ID_U, LifeTime, h(X)) \quad (4)$$

III. 분석

본 장에서는 본 논문에서 제안한 인증 프로토콜의 안전성을 패스워드 추측공격(Password guessing attack), 재전송 공격(Reply attack), 위장공격(Impersonation attack), 중간자공격(Man-in-the-middle attack)측면에서 분석을 하고, 제안한 두 인증기법에 대한 연산과 통신량에 초점을 맞춘 성능분석을 제시한다.

[패스워드 추측 공격] 제안한 인증 프로토콜에서 공격자가 패스워드 정보를 획득할 수 있는 유일한 방법은 주고받는 메시지 M_1, M_2, M_3 를 통해서이

다. 메시지 M_1 에서 사용자의 패스워드 정보는 $MAC_{UH} = f_{EV}^1(A \| ID_U \| T_U \| A_n)$ 에 의존적이고, MAC_{UH} 에서 $EV = V_{PW_U} \oplus T_U$ 의 정보를 통해서 추측할 수 있다. 하지만 공격자가 V_{PW_U} 를 통해서 패스워드를 계산하는 것은 이산대수의 어려움에 근거한다. 또한 M_3 에서 공격자는 티켓에 포함된 해쉬된 $X = V_{PW_U} \oplus ID_U$ 값을 통해 패스워드 추적이 가능 하지만 티켓은 홈서버와 홈장비사이에 사전에 공유된 공통키 k 로 암호화 됨으로 해쉬된 X 를 통해 사용자 패스워드를 추측하는 것 또한 이산대수 문제의 어려움에 근거한다.

[재전송공격] 재전송공격에 대응하기 위해 제안한 기법은 타임스탬프와 도전/응답 기법을 이용하였다. 먼저, 초기 단계에서 홈서버는 사용자의 메시지 송신 시간 T_U 와 메시지 도착 시간 T 에 대하여 $T - T_U \leq \Delta T$ 연산을 통해 재전송 여부를 확인할 수 있다. 따라서 공격자가 M_1, M_2, M_3, M_4 를 캡처한 후 재전송공격을 할 경우, 캡처된 메시지 내의 T_U, T_D, T_H 로 인해 ΔT 의 시간 조건을 제시할 수 없다. 만약, 공격자가 ΔT 조건 내에 재전송 공격을 한다고 하더라도 도전/응답에 이용된 랜덤 값 a, b 에 대한 적절한 변경을 제시할 수 없으므로 재전송 공격에 강하다. 그리고 제안한 인증 프로토콜의 티켓 기반 인증 단계에서도 타임스탬프를 이용한 도전/응답을 이용하기 때문에 재전송공격에 안전하다.

[위장공격과 중간자공격] 제안한 프로토콜에서 위장공격을 분석하기 위해서는 사용자 위장공격, 홈장비 위장 공격 그리고 홈서버 위장공격 관점에서의 분석이 필요하다.

■ 사용자 위장공격 : 첫 단계에서 공격자가 사용자를 위장하기 위해서는 패스워드 관련 정보를 알 수 있어야 한다. 하지만 M_1, M_2, M_3 를 통해서 패스워드 추측 불가능은 패스워드 추측 공격에서 언급한 것처럼 어려운 문제이므로 사용자 위장공격에 안전하다. 또한 티켓을 이용한 인증 단계에서 공격자는 SV 와 티켓에 포함된 정보를 자신의 정보로 수정할 수 없기 때문에 사용자 위장공격에 안전하다.

■ 홈장비 위장공격 : 공격자가 홈서버 위장을 통해 M_1 에서 A 값을 얻고, 랜덤 값 생성을 통해

DH_U 을 얻을 수 있다고 하더라도, k 와 SV 을 알 수 없는 공격자는 올바른 MAC_{DU} 을 유도할 수 없으므로 홈장비 위장공격에 안전하다.

■ 홈서버 위장공격 : 공격자는 k, EV 와 V_{PW_U} 를 알 수 없으므로, $MAC_{HU} = f_{EV}^1(X \parallel Ticket)$, $MAC_{HD} = f_k^1(ID_D \parallel ID_H \parallel T_H)$ 값을 유도할 수 없고 적법한 티켓을 생성할 수 없기 때문에 홈서버 위장 공격에 안전하다. 만약 공격자가 중간자공격을 시도하기 위해서 메시지를 캡처한다고 하더라도 관련된 정보에 적합한 MAC 을 생성할 수 있어야 하는데 그러한 연산은 불가능하기 때문에 홈서버와 홈장비, 사용자 측 어느 쪽에서 도 인증에 실패하게 된다.

표 2. 인증 프로토콜들간의 성능분석
Table 2. Performance Analysis between Authentication Protocols

연산	기법	논문[9]에서 제안한 기법		제안한 프로토콜	
		초기 인증	티켓 기반	초기 인증	티켓 기반
XOR		8_{XOR}	·	8_{XOR}	·
MAC		4_{MAC}	4_{MAC}	8_{MAC}	2_{MAC}
지수		6_e	3_e	5_e	·
해쉬		·	·	3_h	·
통신수		3_{MSG}	3_{MSG}	4_{MSG}	1_{MSG}
전체		$8_{XOR} + 4_{MAC} + 6_e + 3_{MSG}$	$4_{MAC} + 3_e + 3_{MSG}$	$8_{XOR} + 8_{MAC} + 5_e + 3_h + 4_{MSG}$	$2_{MAC} + 1_{MSG}$

성능분석을 위해서는 제안한 인증 프로토콜과 논문[9]에서 제안한 기법간의 초기인증과 티켓기반 인증에 대해 비교분석을 제시한다. 표 2는 기존 프로토콜과 제안한 프로토콜간의 성능분석을 보여준다. 본 논문에서 제안한 초기 인증기법은 논문 [9]에서 제시한 기법에 비해 MAC연산, 해쉬연산, 통신횟수에 비해 지수연산의 경우는 1회 감소하지만 MAC연산의 오버헤드는 2배 증가하며, 해쉬연산은 3번의 추가적인 오버헤드가 제시되어야 한다. 또한, 통신오버헤드도 약 13% 정도 증가한다. 이러한 오버헤드를 통해서 본 논문에서 제안한 인증 프로토콜은 논문[9] 기법에 존재하는 사용자 인증이 홈서버의 안전성에 기반하고 있는 보안 문제를 효율적으로 해결할 수 있었다.

하지만, 이러한 연산의 오버헤드도 티켓기반의 인증과정을 이용함으로써 기존의 기법과 비교하여

2번의 MAC연산을 줄일 수 있으며 연산의 오버헤드가 큰 지수연산의 오버헤드를 없앨 수 있다. 또한 통신 오버헤드 측면에서 논문[9] 기법보다 효율적임을 확인할 수 있다.

IV. 결 론

본 논문에서는 기존에 제안된 속성 기반 프로토콜의 문제점인 홈서버의 안전성 문제에 따른 홈네트워크 전반에 걸친 보안 취약성 확대의 문제를 해결하기 위한 새로운 속성정보를 이용한 티켓기반의 인증 프로토콜을 제안하였다. 본 논문에서 제안한 인증 프로토콜은 특히 초기 인증단계에서 발급된 티켓을 이용하여 다양한 서비스에 이용함으로써, 인증에 필요한 연산량과 통신량의 오버헤드를 줄일 수 있었다. 제시된 안전성 분석을 통해 제안한 프로토콜이 다양한 공격에 안전하다는 것을 확인하였다. 본 논문에서 제안한 인증 프로토콜은 사용자의 속성에 따라 홈 네트워크 서비스의 접근성을 차별화시킴으로써 보안의 다양한 레벨을 제공하여 보다 안전한 홈네트워크 서비스를 제공할 수 있다.

참고문헌

- [1] 오연주, 범민준, 김동희, 백희현, “사설IP기반 홈네트워크에서 세션이동성 지원의 적응적인 SIP 응용서버 시스템 구조설계,” 대한임베디드공학회논문지, Vol. 1, No. 2, pp.73-81, 2006.
- [2] D. G. Lee, J. W. Han, J. H. Park, “User Authentication for Multi Domain in Home Network Environments,” Proceedings on 2007 International Conference on Multimedia and Ubiquitous Engineering(MUE'07), pp.89-96, 2007.
- [3] G. W. Kim, D. G. Lee, J. W. Han, S. C. Kim, S. W. Kim, “Security Framework for Home Network : Authentication, Authorization, and Security Policy,” Lecture Notes in Artificial Intelligent, Vol. 4819, pp. 621-628, 2007.
- [4] 서화정, 김호원, “속성기반 제 암호화를 이용한 스마트카드 인증권한 분배스킴,” 대한임베디드공학회논문지, Vol. 5, No. 3, pp.168-174, 2010.
- [5] ITU-T, <http://www.itu.int/ITU-T>
- [6] 이덕규, 김도우, 한종욱, “홈네트워크 보안 기술

및 표준화 동향,” ETRI 전자통신동향 분석, Vol. 23, No. 4, pp.89-101, 2008.

- [7] P. Funk, “The EAP MD5-Tunneled Authentication Protocol,” draft-funk-eap-md5-tunneled- 01, 2004.
- [8] “홈서버 중심의 홈네트워크 사용자 인증 메커니즘,” TTAS.KO-12.0030.
- [9] 이원진, 전일수, “홈네트워크 상에서 속성기반의 인증된 키교환 프로토콜,” 한국정보보호학회논문지, Vol. 18, No. 5, pp.49-57, 2008.
- [10] L. Lamport, “Password authentication with insecure communication,” Communication of ACM, Vol. 24, No. 11, pp.24-30, 1981.
- [11] A. Kehne, J. Schonwalder, H. Langenrfer, “A nonce-based protocol for multiple authentication,” ACM Operating Systems Review, Vol. 26, No. 4, pp.84-89, 1992.
- [12] K. Mangipudi, R. Katti, “A Secure identification and key agreement protocol with user Anonymity(SIKA),” Computers and Security Vol. 25, pp. 420-425, 2006.
- [13] A. Sahai, B. Waters, “Fuzzy identity based encryption,” In Eurocrypt 2005, pp. 457-473, 2005.
- [14] M. Pirretti, P. Traynor, P. McDaniel, B. Waters, “Secure attribute-based systems,” Proceedings on ACM Conference on Computer and Communications Security (CCS'06), pp.99-112, 2006.

저 자 소 개

이 원 진(Won Jin Lee)

2002년 : 경일대학교 컴퓨터공학 학사. 2004년 : 경북대학교 컴퓨터공학 석사. 2009년 : 금오공과대학교 전자통신공학 박사. 2007~2009년 : 경일대 컴퓨터공학부 전임강사. 2011~현재, 단국대학교 소프트웨어학 연구교수.

관심분야: 정보보안, 센서네트워크, 유비쿼터스.

Email: god7300@dankook.ac.kr

김 기 원(Gi Won Kim)

2006년 : 경북대학교 컴퓨터공학 박사. 2007~2009년 : 경일대학교 컴퓨터공학부 전임강사. 2009년~현재, 우석대학교 컴퓨터공학부 겸임교수

관심분야: 정보보안, 보안프로토콜, 암호 H/W

Email: nirk@paran.com

김 현 성(Hyun Sung Kim)

2002년 : 경북대학교 컴퓨터공학 박사. 2002년~현재, 경일대학교 컴퓨터공학부 교수. 2009년~2010년 : 더블린 시티대학교 방문교수. 2010년~현재, 정보융합보안연구소 소장.

관심분야: 정보보안, 정보융합보안.

Email: kim@kiu.ac.kr