情報保護學會論文誌
第18卷 第5號, 2008. 10

홈네트워크 상에서 속성기반의 인증된 키교환 프로토콜

이 원 진†, 전 일 수‡
금오공과대학교

Attribute-base Authenticated Key Agreement Protocol over Home Network

Won-Jin Lee†, Il-Soo Jeon‡
Kumoh National Institute of Technology

요 약

안전한 홈네트워크 서비스를 제공하는데 있어서 사용자 인증 및 키교환은 아주 중요한 구성요소이다. TTA는 사용자 인증과 키전송 표준으로 EEAP-PW를 채택하고 있지만 이 프로토콜은 전방향 안전성을 제공하지 못하는 것을 포함한 몇 가지 문제를 가지고 있다. 본 논문에서는 먼저 EEAP-PW 프로토콜의 문제점을 분석하고 이를 효율적으로 해결할 수 있는 속성기반의 인증된 키교환 프로토콜(EEAP-AK)을 제안한다. 제안한 프로토콜은 사용자의 속성에 기반한 인증과 키 교환 후 사용자 속성에 따라 홈 네트워크 서비스의 접근성을 차별화시킴으로 보안의 다양한 레벨을 제공한다. 본 논문에서 제안하는 프로토콜은 EEAP-PW의 문제점을 효율적으로 해결할 수 있어 EEAP-AK를 통한 보다 안전한 홈네트워크 서비스를 제공할 수 있을 것으로 기대된다.

ABSTRACT

User authentication and key agreement are very important components to provide secure home network service. Although the TTA adopted the EEAP-PW protocol as a user authentication and key transmission standard, it has some problems including not to provide forward secrecy. This paper first provides an analysis of the problems in EEAP-PW and then proposes a new attribute-based authenticated key agreement protocol, denoted by EEAP-AK, to solve the problems. The proposed protocol supports the different level of security by diversifying network accessibility for the user attribute after the user attribute-based authentication and key agreement protocol steps. It efficiently solves the security problems in the EEAP-PW and we could support more secure home network service than the EEAP-AK.

Keywords : Home network security, EEAP, ABE, User authentication, Key agreement protocol

Ⅰ. 서 론

최근 IT 기술의 급속한 발달과 초고속망을 통한 서비스가 활발해지면서 홈네트워크에 대한 관심이 높아지고 있다. 이러한 홈네트워크의 핵심은 유·무선 네트워크

접수일 : 2008년 8월 27일; 채택일 : 2008년 9월 25일
† 주저자, wjlee@kumoh.ac.kr
‡ 교신저자, isjeon@kumoh.ac.kr

망을 댁내로 연결시켜 원격지에서도 댁내의 정보가전 기기를 제어 할 수 있도록 하여 생활의 편리성을 증진 시키는데 있다. 이처럼 홈네트워크에 대한 관심이 높아지면 서 다양한 보안 취약성으로 인해 개인의 프라이버시 침해 뿐 아니라 개인의 생명 및 자산의 피해 등이 발생하고 있다. 그러므로 보다 안전하고 신뢰성 있는 홈네트워크 서비스를 제공받기 위해서는 정보보호 기술에 대한 표준화가 수행되어야 한다. 홈네트워크의 표준화는 2005년 ISO에서 홈네트워크 보안 요구사항과 댁내 및 댁외 보안에 대한 표준이 나오게 되었고, 국내에서는 HNSF(Home Netowork Security Forum)와 TTA(Telecommunications Technology Assoication)를 중심으로 홈네트워크 보안에 관한 표준이 개발되고 있는데, 2006년과 2007년에는 홈네트워크 보안 기술 프레임워크, 홈네트워크 사용자 인증 메커니즘, 홈네트워크 보안 정책 기술 언어 등의 표준안이 제정되었다. 이들 표준들 중 일부는 ITU-T SG17에서 국제표준으로 채택하기 위해 2006년 12월 제네바 회의에서 표준으로 발표되었으며, 2005년부터 현재까지 ITU-T에서 진행 중인 표준안에는 Xhomesec-1, X-homesec-2, X-homesec-3이 있다[1,2].

특히, 홈네트워크에서의 사용자 인증과 키교환은 보안에 있어서 중요한 요소이다. 사용자가 안전한 홈네트워크 서비스를 이용할 수 있게 하기 위해서 사용자 인증은 필수적으로 선행되어야 할 문제이다[3,4,5]. 이를 위한 인증 기법으로는 댁내에서 댁내 홈서비스를 위한 사용자 인증, 댁내에서 댁외 서비스를 위한 사용자 인증, 댁외에서 댁내 홈서비스에 대한 세 가지 형태로 크게 나눌 수 있다[6]. 이러한 세 가지 형태의 인증을 제공하기 위해 가장 많이 사용되고 있는 기법은 EAP-MD5 (Extensible Authentication Protocol-MD5) [7,8]이다. 하지만, EAP-MD5에서 인증서버는 사용자를 인증하지만 사용자는 인증 서버를 인증하지 않는 단방향 인증을 사용하고 키 생성을 제시하지 못한다. 그러므로 EAP-MD5는 중간자공격(Man-In-The-Middle attack)과 서비스거부(Denial of Service)에 노출될 수 있다. 이러한 EAP-MD5의 취약점을 개선하기 위해서 2006년 TTA에서 홈네트워크 사용자 인증 메커니즘인 EEAP-PW(Encrypted Extensible Authentication Protocol-PW) [9] 프로토콜을 표준화 하였다.

이처럼 안전한 홈네트워크 서비스를 이용하기 위해서 사용자 인증은 매우 중요한 보안 요소이다. 일반적인 사용자 인증 기술에서는 사용자만이 알고 있는 정보(패스워드)를 입력함으로써 사용자 인증을 수행한다. 이러한 패스워드를 이용한 사용자 인증 방법으로 Lamport에 의해 안전한 원격 패스워드 인증 방법[10]과 TTP 기반 방법[11] 등 제안되었으나, 패스워드 테이블에 대한 공격의 가능성이 존재한다. 2006년 K.Mangipudi와 R.Katti[12]은 사용자의 익명성을 제공하는 서비스 거부 공격에 강한 프로토콜을 제안하였으나, 사용자의 속성(권한)에 따라 정보의 접근성을 차별화하는 인증의 다양성은 제공하지 않는다. 예를 들어 홈네트워크 서비스를 이용하는 가족 구성원들 중에서 어린이나 노인들에게 화재와 관련된 홈장비들에 대한 서비스를 제공한다면 위험한 사고가 발생할 수도 있다. 또한 원격 관리자들(수도, 전기, 가스 검침 및 관리)에게는 가족 구성원들이 가지는 민감한 정보에 대한 접근성을 허용해서도 안된다. 그러므로 홈네트워크 서비스를 이용하는 사용자에 대한 인증 시 사용자들 가지는 속성에 따라 정보의 접근성을 차별화하는 속성 기반의 인증프로토콜이 필요하다.

본 논문에서는 이러한 TTA의 표준인 EEAP-PW의 문제점을 해결하기 위하여 속성기반의 인증된 키교환 프로토콜을 제안한다. 서비스의 차별화를 위하여 제안한 프로토콜은 Sahai와 Waters[13,14]의 속성 기반 암호(Attribute based Encryption) 시스템의 속성을 활용한다. 따라서 사용자의 속성에 따른 다양한 레벨의 보안(접근통제)을 제공할 수 있는 속성 기반의 사용자 인증 프로토콜(EEAP-AK)을 제안한다. 제안한 프로토콜은 기존의 EEAP-PW 프로토콜에서 존재하는 다양한 문제를 효율적으로 해결한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문을 이해하는데 기본이 되는 속성 기반 암호와 홈네트워크의 사용자 인증 및 EEAP-PW 프로토콜에 대해 간략히 살펴보고 EEAP-PW프로토콜의 분석을 제시한다. 3장에서는 제안한 프로토콜에 대하여 상세히 설명하고 4장에서는 제안된 프로토콜의 안전성 분석을 제시하며 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

본 장에서는 먼저 Sahai와 Waters[13,14]의 제안된 속성기반 암호(Attribute based Encryption) 기법에 대해 간략하게 살펴보고, 홈네트워크의 사용자 인증과 EEAP-PW 프로토콜에 대한 설명 및 문제점 분석에 대

하여 살펴본다.

2.1 속성기반 암호

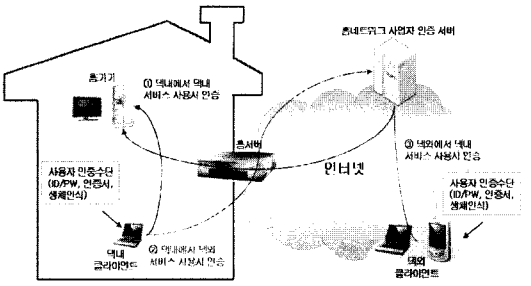
속성 기반 암호 시스템은 Sahai와 Waters에 의해 처음 제안되는데, 속성 값을 암호 인자로 사용하여 속성에 대한 비밀키를 가지고 있는 사용자만이 암호화된 데이터를 복호화 하는 기법이다. 이 기법은 사용자의 속성 값을 이용하여 암호화되며, 속성 값을 소유한 사람만이 메시지를 복호화 할 수 있다. 이러한 속성기반 암호시스템은 먼저 서버가 각 속성 값별로 제공하는 서비스를 정의해야 하며, 사용자는 자신의 개인정보를 서버에 등록한다. 이때 서버는 사용자가 가지는 속성(권한)을 인증하고 사용자에게 제공되는 서비스의 해당되는 특정 속성 값을 제공한다. 사용자는 자신의 속성 값을 사용하여 필요한 서비스를 이용한다.

특히 홈네트워크 서비스를 이용하는 가족 구성원들(관리자, 성인, 어린이, 노인 등)과 원격 관리자들(수도, 전기, 가스 검침 및 관리)이 있다. 만약 어린이나 노인들에게 화재와 관련된 홈장비들의 서비스 접근을 허용하게 되면 위험한 사고가 발생할 수도 있다. 또한 원격 관리자들에게 가족 구성원들이 가지는 민감한 정보에 대한 접근성을 허용해서도 안된다. 그러므로 홈네트워크 서비스를 이용하는 사용자에 대한 인증 시 사용자들 가지는 속성에 따라 서비스의 접근성을 차별화시켜 줄 수 있는 인증의 다양성이 제공되는 속성 기반의 인증프로토콜이 필요하다.

2.2 홈네트워크의 사용자 인증 메커니즘

2.2.1 홈네트워크의 사용자 인증

홈네트워크 환경에서 홈서버는 모든 통신을 감시하여 인증서버 역할을 수행한다. 그리고 홈네트워크 서비스를 이용하기 위해서는 서비스의 종류에 따라 사용자 인증을 받아야만 하며, 사용자는 다양한 인증 수단을 사용하여 인증을 받으려 한다. [그림 1]은 홈네트워크 시스템의 구성 및 가능한 인증 시나리오를 보여주고 있다. 홈네트워크 시스템에서 가능한 인증 시나리오는 댁내에서 댁내 홈서비스를 위한 사용자 인증, 댁내에서 댁외 서비스를 위한 사용자 인증, 댁외에서 댁내 홈서비스에 대한 사용자 인증으로 크게 나눌 수 있다[5].



[그림 1] 홈네트워크 시스템 구성 및 사용자 인증 시나리오

2.2.2 EEAP-PW 프로토콜

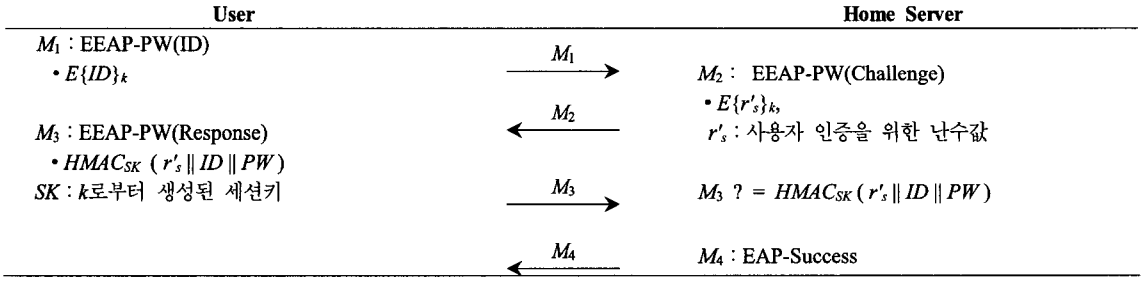
홈네트워크 사용자 인증을 위한 표준안인 EEAP-PW 프로토콜은 기존의 EAP-MD5의 문제점을 해결하기 위해서 상호인증을 제공하고 안전성을 강화한 홈네트워크 인증 프로토콜이다.

(1) 프로토콜 절차

일반적으로 EEAP-PW 프로토콜은 ① 신원 확인, ② 초기 협상 단계, ③ 홈 장치 인증 단계, ④ 사용자 인증 단계로 구성된다. 프로토콜은 사용자의 신원 확인 후, 초기 협상을 위해 사용자 단말기와 홈서버는 버전, 랜덤 값, 세션 *ID* 등이 포함된 헬로우 메시지를 송수신한다. 이때 홈서버는 인증서에 공개키를 포함시켜 보낸다. 그런 다음 사용자 단말에서 대칭키 k를 홈서버의 공개키로 암호화해서 전송하고, 검증 메시지를 통해 홈서버를 인증한다. 마지막 사용자 인증에서는 이전 단계에서 나눠가진 대칭키 k로 사용자의 실제 *ID*를 암호화하여 전송한다. 본 논문은 사용자 인증 및 키교환에 초점을 맞추고 있으므로 이 과정에 대해 상세히 살펴볼 필요가 있다. 먼저, 홈서버는 사용자 인증을 위해 필요한 난수값(challenge)을 k로 암호화하여 보내고, 사용자는 홈서버로부터 받은 난수값과 *ID*, PW를 HMAC 함수에 세션키 *SK*를 사용하여 응답(response) 값을 전송하는데, 이때 *SK*는 대칭키 k로 부터 생성된다. 응답 값을 전송받은 홈서버는 자신이 계산한 응답 값을 통해 검증하고, 유효하면 인증이 성공적으로 끝났음을 사용자에게 알려준다. [그림 2]는 EEAP-PW의 사용자 인증 및 키전송 단계를 보여준다.

(2) 프로토콜 분석

본 소절에서는 EEAP-PW 프로토콜이 가지는 보안의



〔그림 2〕 EEAP-PW 인증 및 키전송 과정

취약성을 다음의 세가지로 제시한다.

[키전송프로토콜] : EEAP-PW 프로토콜의 인증과 키 전송 과정에서는 홈서버가 향후 통신에 사용할 키를 사용자와 홈서버 간에 미리 알고 있는 정보인 비밀키를 이용하여 전송한다. 하지만 일반적으로 키 생성은 둘 간의 비밀값을 활용하여 생성하는 것이 바람직하다.

[전방향안전성 제시 불가] : EEAP-PW 프로토콜에서는 사용자와 홈서버 간에 밀리 알고 있는 비밀값인 k를 이용하여 서버가 생성한 세션키를 전송한다. 만약 오랫동안 사용되는 키(Long-term secret key)인 k가 노출된다면 현재 세션뿐만 아니라 이전 세션의 모든 세션키가 노출되는 문제가 발생한다.

[티켓기반의 인증이 아님] 일반적으로 홈네트워크에 인증 후 사용자는 다양한 서비스를 사용하고자 할 것이다. 하지만, EEAP-PW 프로토콜은 다양한 서비스에 접근하기 위한 일반적인 방법을 제시하지 못하고 있다. 한번 인증 후 다양한 서비스를 제공받기 위해서는 일반적으로 티켓 기반의 프로토콜을 사용한다.

홈 네트워크에 있어서 보안은 다양한 형태로 사람들에게 직접적인 영향을 미칠 수 있다는 면에서 다른 어떤 다른 응용보다도 더 중요하다. 특히 보안을 제공하는데 있어서 사용자 인증 및 키교환은 선행되어야 할 아주 중요한 문제이다. 본 논문에서는 TTA의 표준인 EEAP-PW에 존재하는 전술한 문제를 해결하기 위한 새로운 프로토콜을 제시하고자 한다.

Ⅲ. 속성기반 인증된 키교환 프로토콜

본 장에서는 EEAP-PW 분석을 통해 나타난 문제점을 해결하기 위한 속성기반의 인증된 키교환 프로토콜(EEAP-AK)를 제안한다. 제안한 기법은 사용자의 속성값을 암호 인자로 사용하여 속성에 대한 비밀키(AK)를 이용하여 사용자 속성(권한)에 따른 차별화된 홈네트워크 서비스를 제공하고자 한다. 또한 매 세션마다 새로운 세션키를 생성하여 상호 교환하는 방법을 이용하고, 세션키 SK와 속성 비밀키를 이용한 보안을 제공함으로서 전방향 안전성을 제공한다. 또한, 첫 사용자 인증과정에서 홈서버가 사용자에게 티켓을 발급함으로서 매번 인증 및 키교환 시 발생하는 연산의 오버헤드를 줄인다.

3.1 표기법

본 절에서는 제안된 프로토콜들에서 사용될 표기법에 대하여 [표 1]과 같이 정의한다.

〔표 1〕 프로토콜 표기법

표기	의 미
ID_R	R의 식별자
PW	사용자의 패스워드
$Sign$	전자서명
x_s	홈서버의 비밀키
V	$g^{PW} \bmod p$
a	사용자의 랜덤 값($a \in Z_p$)
b	홈서버의 랜덤 값($b \in Z_p$)
g	$g < p$이고, p와 서로소인 원시근
p	매우 큰 소수
f_K^1	키 K를 이용한 *MAC(Message Authentication Code)*값과 그에 대응하는 검증 값인 *XMAC* 값을 계산하는 메시지 인증 함수
f_K^2	키 K를 이용한 새로운 세션키(SK)를 생성하는 함수
T_R	R이 생성한 타임스탬프
T	R이 생성한 타임스탬프가 도착 시간
AK	속성기반의 비밀키
SK	*Diffie-Hellman* 기법으로 생성한 세션키

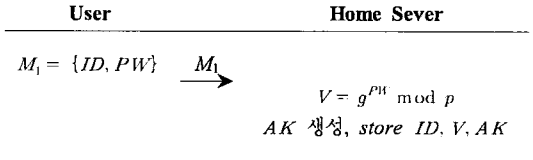
3.2 프로토콜 수행 과정

본 절에서는 제안하는 프로토콜에 대해 설명한다. 제안하는 프로토콜은 크게 사용자 등록 단계와 인증된 키 교환 단계로 구성된다. 먼저 등록단계에서는 사용자 정보와 패스워드 및 속성 관련 정보를 서버에 등록한다. 인증된 키교환 단계에서는 등록단계에 등록한 정보의 소유 여부를 통해서 사용자와 서버 간에 양방향 인증을 수행하고 이후 새로운 서비스에 대한 추가적인 인증의 오버헤드를 줄이기 위해서 티켓을 발급한 후 키 교환을 수행한다.

3.2.1 등록 단계

사용자는 등록 단계에서 [그림 3]과 같이 자신의 개인 정보를 안전한 채널을 통해 전송하고, 홈서버는 사용자의 정보를 이용하여 사용자를 등록한다. 전체적인 처리과정은 다음과 같다.

1. 사용자는 홈서버에 자신의 ID와 PW를 안전한 채널을 통해 전송한다.
2. 홈서버는 $V=g^{PW}$를 계산하고 사용자의 속성값인 AK_i를 생성하여 데이터베이스에 ID, V, AK_i를 저장한다. 특히, 홈서버는 사용자를 위한 n개의 속성값 $a_{i,j} \in UA_i, 1 \le j \le n$ ($UA_i \subseteq G$)와 자신의 비밀키(x_s)를 이용하여 AKi를 계산한다. 여기서, UAi는 사용자 i의 속성 집합이며 G는 홈서버가 정의한 모든 속성 값들의 집합이다.
   $ak_j = h(a_{i,j} \oplus x_s) \oplus h(x_s), 1 \le j \le n$
   그리고, $AK_i = ak_1, \ldots, ak_n$
   등록과정에서 생성된 AK는 홈서버에 안전하게 저장되며, 사용자 인증 및 키교환 과정에서 안전하게 사용자에게 전송된다. AK는 인증의 다양성을 제공하기 위해 사용되는데, 사용자 인증 시 사용자의 속성에 따라 정보접근성에 차별을 주기 위해 사용되는 사용자 속성에 대한 비밀키이다. 즉 속성에 대한 비밀키를 가지고 있는 사용자만이 암호화된 데이터를 복호화하여 메시지를 확인 할 수 있다.



[그림 3] EEAP-AK의 등록 단계

3.2.2 인증된 키교환 단계

EEAP-AK의 초기 인증된 키교환 단계에서 홈서버는 사용자 인증 후 사용자의 속성 비밀키 AK를 분배하고, 다른 서비스의 사용을 용이하게 하기 위해 티켓을 발급한다. 사용자 속성 비밀키와 세션키는 이후 통신의 안전성을 위하여 다양한 목적으로 사용된다. [그림 4]는 초기 인증된 키교환 단계의 전체적인 수행 과정을 보여주며 상세한 수행 과정은 다음과 같다.

1. 사용자는 랜덤 값 $a \in Z_p$를 선택하고, $A = g^a \bmod p$을 계산한 후 $V = g^{PW}$와 $EV = V \oplus T_U$, $MAC_U = f^1_{EV}(A \| ID_U \| T_U)$을 계산하여 다음의 메시지 $M_1 = \{ID_U, ID_H, A, T_U, MAC_U\}$을 홈서버에게 전송한다.
2. 홈서버는 $T - T_U \le \Delta T$ 연산을 통해서 적법한 시간 범위에 메시지가 보내졌는지를 확인한다. 여기서 ΔT는 전송 지연을 고려한 적법한 시간 범위이다. 적법한 시간 범위 ΔT는 네트워크 환경에 따라 다양하게 조정될 수 있다. 홈서버는 V와 EV를 확인하고, MAC_U의 검증을 통해 적법한 사용자 여부를 확인한 뒤, 랜덤 값 $b \in Z_p$를 선택하여, $B = g^b \bmod p$와 $X = V \oplus ID_U$을 계산한 후, 티켓을 서명하여 발급 한다. 그리고 $MAC_H = f^1_{AK}(B \| X \| T_H)$와 $DH_H = A^b \bmod p$, $TAK = AK \oplus DH_H \oplus V$을 계산하여 $M_2 = \{Ticket, B, TAK, MAC_H, T_H\}$을 사용자에 전송한다.
3. 사용자는 $T - T_H \le \Delta T$ 의 적법성을 체크하고, $DH_U = B^a \bmod p$을 계산하여 $TAK \oplus DH_U \oplus V$ 연산을 통해 AK를 유도한다. 그리고 티켓의 유효성 확인과 MAC_H의 검증을 통해 적법한 홈서버 여부를 확인하며, 유도된 AK를 통해 $Y = f^1_{AK}(DH_U - 1)$을 계산하여 $M_3 = \{Y\}$을 홈서버에게 전송한다.
4. M_3을 받은 홈서버는 M_3의 검증을 통해 적법한 사용자를 인증한 후 AK를 사용하여 세션키 SK를 생성한다.

User		Home Sever
$a \in Z_p$, $A = g^a \bmod p$		
$V = g^{PW} \bmod p$		$T - T_U \le \Delta T$ 체크
$EV = V \oplus T_U$		$V = g^{PW} \bmod p$, $EV = V \oplus T_U$
$MAC_U = f^1_{EV}(A \parallel ID_U \parallel T_U)$		$MAC_U ? = XMAC_U$
$M_1 = \{ID_U, ID_H, A, T_U, MAC_U\}$	$M_1 \rightarrow$	$b \in Z_p$, $B = g^b \bmod p$, $X = V \oplus ID_U$
		$Ticket = ID_H, \{Sign_H[ID_U, Life\,Time, T_H, A, h(X)]\}$
		$MAC_H = f^1_{AK}(B \parallel X \parallel T_H)$
$T - T_H \le \Delta T$ 체크	$\leftarrow M_2$	$DH_H = A^b \bmod p$
$DH_U = B^a \bmod p$		$TAK = AK \oplus DH_H \oplus V$
$AK = TAK \oplus DH_U \oplus V$		$M_2 = \{Ticket, B, TAK, MAC_H, T_H\}$
$X = V \oplus ID_U$, $Ticket$의 유효성 확인		
$MAC_H ? = XMAC_H$		
$Y = f^1_{AK}(DH_U - 1)$		
$M_3 = \{Y\}$	$M_3 \rightarrow$	
$SK = f^2_{AK}(DH_U)$		$Y ? = f^1_{AK}(DH_H - 1)$
		$SK = f^2_{AK}(DH_H)$

〔그림 4〕 EEAP-AK의 초기 사용자 인증된 키교환 단계

EEAP-AK의 초기 인증된 키교환 단계를 매 인증마다 사용한다면 연산의 오버헤드가 커지는 문제점이 있다. 이러한 문제점을 해결하기 위해서 본 논문에서는 초기 인증 후 추가적인 인증이 필요할 경우엔 홈서버로부터 발급 받은 티켓을 이용하여 인증과 키 교환을 수행하고자 한다. [그림 5]는 초기 인증된 키교환 단계 이후 추가적인 인증이 필요할 때마다 티켓을 이용한 인증된 키교환을 수행하기 위한 전체과정을 보여주고 있고, 상세한 처리 과정은 다음과 같다.

1. 사용자는 $MAC_U = f^1_{AK}(T_U)$을 계산하고, 티켓과 타임스탬프 TU를 포함한 $M_1 = \{Ticket, T_U, MAC_U\}$을 홈서버에게 전송한다.
2. 홈서버는 $T - T_U \le \Delta T$ 체크하고 티켓의 유효성을 확인한다. MAC_U의 검증을 통해 적법한 사용자 여부를 확인하고, 새로운 랜덤 값 $b \in Z_p$를 선택하여, $B = g^b \bmod p$을 계산한다. 그리고 $MAC_H = f^1_{AK}(B \parallel DH_H \parallel T_H)$과 $DH_H = A^b \bmod p$을 계산하여 $M_2 = \{B, MAC_H, T_H\}$을 사용자에 전송한다.
3. 사용자는 $T - T_H \le \Delta T$ 체크하고, MAC_H의 검증을 통해 적법한 홈서버 여부를 확인하며, AK를 통해 $Y = f^1_{AK}(DH_U - 1)$을 계산하여 M_3을 홈서버에게 전송한다.
4. M_3을 받은 홈서버는 M_3의 검증을 통해 적법한 사용자를 인증한 후 새로운 세션키 SK를 생성한다.

User		Home Sever
$MAC_U = f^1_{AK}(T_U)$		
$M_1 = \{Ticket, T_U, MAC_U\}$	$M_1 \rightarrow$	$T - T_U \le \Delta T$ 체크, $Ticket$의 유효성 확인
		$MAC_U ? = XMAC_U$
		$b \in Z_p$, $B = g^b \bmod p$
$T - T_H \le \Delta T$ 체크		$DH_H = A^b \bmod p$
$DH_U = B^a \bmod p$	$\leftarrow M_2$	$MAC_H = f^1_{AK}(B \parallel DH_H \parallel T_H)$
$MAC_H ? = XMAC_H$		$M_2 = \{B, MAC_H, T_H\}$
$Y = f^1_{AK}(DH_U - 1)$, $M_3 = \{Y\}$		
	$M_3 \rightarrow$	$Y ? = f^1_{AK}(DH_H - 1)$
$SK = f^2_{AK}(DH_U)$		$SK = f^2_{AK}(DH_H)$

〔그림 5〕 EEAP-AK의 티켓을 이용한 인증된 키교환 단계

Ⅳ. 분 석

본 장에서는 EEAP-AK의 안전성을 패스워드 추측(Password guessing attack), 재전송 공격(Reply attack), 전방향 안정성(Forward secrecy), 위장공격(Impersonation attack), 중간자공격(Man-in-the-middle attack)측면에서 안전성 분석한다.

1. 패스워드 추측 공격 : 패스워드는 사용자 인증에 있어서 가장 널리 사용되는 비밀값이다. 그러나 사용자들은 패스워드를 선택할 때 쉽게 기억할 수 있는 패스워드를 선택하는 경향이 있어 패스워드 기반의 프로토콜에 있어서 패스워드 추측 공격의 가능성에 대한 평가는 아주 중요하다. EEAP-AK에서 공격자가 패스워드 정보를 획득할 수 있는 유일한 방법은 주고받는 메시지 M_1과 M_2를 통해서다. M_1에서 사용자의 패스워드 정보는 $MAC_U = f^1_{EV}(A \| ID_U \| T_U)$에 의존적이고, MAC_U에서 $EV = V \oplus T_U$의 정보를 통해서 추측할 수 있다. 하지만 공격자가 V를 통해서 PW를 계산하는 것은 이산대수의 어려움에 근거한다. 또한 M_2에서 공격자는 티켓에 포함된 해쉬된 $X = V \oplus ID_U$ 값을 통해 패스워드 추측이 가능 하지만 티켓은 전자서명 되어 있고, 해쉬된 X를 통해 사용자 패스워드를 추측하기 위해서는 또한 이산대수 문제의 어려움이 따른다.

2. 재전송공격 : 재전송공격에 대응하기 위해 EEAP-AK은 타임스탬프와 도전/응답(challenge/response)을 이용하였다. 먼저, EEAP-AK의 초기 단계에서 홈서버는 사용자의 메시지 송신 시간 TU와 메시지 도착 시간 T에 대하여 $T - T_U \leq \Delta T$ 연산을 통해 재전송 여부를 확인할 수 있다. 따라서 공격자가 M_1, M_2, M_3을 캡처한 후 재전송공격을 할 경우, 캡처된 메시지 내의 TU로 인해 ΔT의 시간 조건을 제시할 수 없다. 만약, 공격자가 ΔT 조건 내에 재전송 공격을 한다고 하더라도 도전/응답에 이용된 랜덤 값 a, b에 대한 적절한 변경을 제시할 수 없으므로 재전송 공격에 강하다. 그리고 EEAP- AK의 티켓 기반 단계에서도 타임스탬프와 랜덤 값을 이용한 도전/응답을 이용하기 때문에 재전송공격에 안전하다.

3. 전방향 안전성 : 전방향 안전성은 공격자가 장기 비밀키(Long-term secret key)를 알고 있다는 가정 하에 이전 세션키를 획득할 수 없을 때 제공된다. EEAP-AK에서 공격자가 비밀키 AK를 알더라도, 현재 및 이전의 모든 세션키 SK를 획득 기 위해서는 메시지 M_2에서 $TAK = AK \oplus DH_H \oplus V$를 통해 세션키 관련 정보를 유추할 수 있어야 한다. 하지만 이 정보에서 세션키 획득에 필요한 $DH_H = A^b \bmod p$값을 알기 위해서 공격자는 V값을 알아야 하고, 이 정보를 확인하기 위해서는 패스워드 추측공격을 수행해야한다. 따라서 EEAP-AK 프로토콜은 전방향 안정성을 제공한다.

4. 위장공격과 중간자공격 : EEAP-AK의 위장공격을 분석하기 위해서 사용자 위장공격과 서버 위장공격 관점에서 분석을 제시한다.
   - 사용자 위장공격 : 첫 단계에서 공격자가 사용자를 위장하기 위해서는 패스워드 관련 정보를 알 수 있어야 한다. 하지만 M_1, M_2를 통해서 패스워드를 추측 불가능 하다는 것은 위에서 언급한 것처럼 불가능하여 사용자 위장공격에 안전하다. 또한 티켓을 이용한 단계에서 공격자는 AK와 티켓에 포함된 정보를 자신의 정보로 수정할 수 있는 방법이 없기 때문에 사용자 위장공격에 안전하다.
   - 서버 위장공격 : 첫 단계에서 공격자는 AK와 V를 알 수 없으므로, $MAC_H = f^1_{AK}(B \| X \| T_H)$ 값을 유도할 수 없고 적법한 티켓을 생성할 수 없다. 그리고 티켓을 이용한 단계에서도 공격자는 서버를 위장하기 위해서 AK를 알 수 있는 방법이 없기 때문에 서버 위장 공격에 안전하다. 만약 공격자가 중간자공격을 시도하기 위해서 메시지를 캡처한다고 하더라도 관련된 정보에 적합한 MAC을 생성할 수 있어야 하는데 그러한 연산은 불가능하기 때문에 서버와 사용자 측 어느 쪽에서도 인증에 실패하게 된다.

Ⅴ. 결 론

홈네트워크에 대한 관심이 높아지면서 현재 표준의 다양한 보안 취약성으로 인해 개인의 프라이버시 침해뿐 아니라 개인의 생명 및 자산의 피해 등의 홈네트워

크에서의 보안에 대한 관심이 높아지고 있다. 안전한 홈 네트워크 서비스를 이용하기 위해서 사용자 인증 및 키 교환은 매우 중요한 보안 요소이다. 본 논문에서는 EEAP-PW의 문제를 해결하기 위해서 속성 기반의 사용자 인증 프로토콜(EEAP-AK)을 제안하였다. 서비스의 차별화를 위하여 EEAP-AK는 속성 기반 암호(Attribute based Encryption) 시스템의 속성을 활용하였다. 따라서 사용자의 속성에 따른 다양한 레벨의 보안을 제공할 수 있는 속성 기반의 사용자 인증 프로토콜을 제안할 수 있었다.

참고문헌

[1] ITU-T, http://www.itu.int/ITU-T

[2] 이덕규, 김도우, 한종욱, "홈네트워크 보안 기술 및 표준화 동향", *ETRI 전자통신동향 분석*, 제23권 제4호, pp. 89-101, 2008.

[3] Y. K. Lee, H. I. Ju, J. H. Park and J. W. Han, "User Authentication Mechanism Using Authentication Server in Home Network", *Advanced Communication Technology ICACT 2006*, pp. 503-506, 2006.

[4] D. G. Lee, J. W. Han and J. H. Park, "User Authentication for Multi Domain in Home Network Environments", *2007 International Conference on Multimedia and Ubiquitous Engineering(MUE'07)*, pp. 89-96, 2007.

[5] G. W. Kim, D. G. Lee, J. W. Han, S. C. Kim and S. W. Kim, "Security Framework for Home Network : Authentication, Authorization, and Security Policy", *PAKDD 2007 Workshops, LNAI 4819*, pp .621-628, 2007.

[6] 이윤경, 한종욱, 정교일, "홈네트워크 보안 표준 동향," *전자통신동향분석*, 제22권 제1권, pp. 73-82, 2007.

[7] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson. and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, 2004.

[8] P. Funk, "The EAP MD5-Tunneled Authentication Protocol", draft-funk-eap-md5-tunneled-01, 2004.

[9] "홈서버 중심의 홈네트워크 사용자 인증 메커니즘", TTAS.KO-12.0030.

[10] L. Lamport, "Password authentication with insecure communication," *Communication of ACM*, Vol.24, pp. 24-30, 1981

[11] A. Kehne, J. Schonwalder, H. Langenorfer, "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 2006, Vol.25*, pp. 420-425, 2006.

[13] A. Sahai, B. Waters, "Fuzzy identity based encryption", *In Eurocypt 2005*, pp. 457-473, 2005.

[14] M. Pirretti, P. Traynor, P. McDaniel and B. Waters, "Secure attribute-based systems", *ACM Conference on Computer and Communications Security* (CCS'06), pp. 99-112, 2006.

〈著者紹介〉

이 원 진 (Won-Jin Lee) 정회원
2002년 2월 : 경일대학교 컴퓨터공학부 졸업
2004년 8월 : 경북대학교 컴퓨터공학과 석사
2007년 2월 : 금오공과대학교 전자통신공학 박사 수료
2007년~현재 : 경일대학교 컴퓨터공학부 전임강사
<관심분야> 유비쿼터스 컴퓨팅 보안, 홈네트워크 보안, 센서네트워크 보안

전 일 수 (Il-Soo Jeon) 정회원
1984년 2월 : 경북대학교 전자공학과 졸업
1988년 2월 : 경북대학교 전자공학과 석사
1995년 2월 : 경북대학교 전자공학과 박사
1983년~1985년 : 삼성전자
1989년~2004년 경일대학교 컴퓨터공학과 교수
2004년~현재 : 금오공과대학교 전자공학부
<관심분야> 정보보호, 패턴인식