원격인증서버 기반의 홈네트워크 사용자 인증 프로토콜 설계

최훈일, 장영건
청주대학교 컴퓨터정보공학과
e-mail:choihi@stkorea.net

Design of User Authentication Protocol for Home Network based on Remote Authentication Server

Hoon-Il Choi, Young-Gun Jang
Dept of Computer & Information Engineering, Cheongju University

요 약

홈네트워크의 사용자 인증은 사용자가 홈네트워크 서비스를 이용할 때 안전한 홈네트워크 서비스를 제공하기 위해 필요한 과정이다. 사용자를 인증하기 위한 수단은 크게 ID/PW 기반, 인증서 기반, 생체인식 기반으로 분류할 수 있다. 본 논문에서는 다양한 인증 수단을 수용할 수 있도록 EAP와 TLS 프로토콜을 기반으로 원격인증서버를 이용한 홈네트워크 사용자 인증 프로토콜을 설계하였다.

1. 서론

IT기술의 급속한 발당과 초고속망을 통한 인터넷 보급에 힘입어, 네트워크 환경이 댁내의 전자기기로까지 확산되면서 홈네트워크 시장에 대한 관심이 높아지고 있으며, 이러한 홈네트워크의 핵심은 네트워크 망을 댁내로 연결시켜 원격지에서도 댁내의 각종 기기를 제어 및 모니터링을 할 수 있도록 하여 생활의 편리를 도모하도록 하는 것이다[1,2].

홈네트워크는 네트워크를 통해 댁내의 정보가전 제어가 가능하므로, 사용자 인증과 접근제어와 같은 보안 기능은 필수적이다. 홈네트워크 보안을 구현하는 방법은 크게 인증과 접근제어와 같은 보안 서버를 댁내에 위치시키는 홈서버 기반과 댁외에 위치시키는 원격관리서버 기반으로 나눌 수 있는데, 우리나라와 같이 아파트 단지 형태의 주거환경이 발달한 곳에서는 원격관리서버 기반의 보안 구축 방법이 더 효과적이다[3,4].

이에 본 논문에서는 사용자 인증 서버를 댁외에 위치시킨 원격인증서버를 기반으로 EAP(Extensible Authentication Protocol)[5]와 TLS(Transport Layer Security)[7] 프로토콜을 이용하여 인증 절차를 단순화한 사용자 인증 프로토콜을 설계하였으며, EAP-HNUA (Extensible Authentication Protocol for Home Network User Authentication)로 명명하였다. 이 인증 프로토콜은 홈네트워크 사용자 인증 시 다양한 인증수단을 사용할 수 있고, 댁내와 댁외의 사용자 인증 메커니즘이 동일하도록 한 것이 특징이다. EAP는 무선 인터넷 등의 사용자 인증 프로토콜로 현재 널리 사용되고 있으며, TLS 프로토콜은 인터넷 상의 통신 애플리케이션과 그 사용자들 간의 정보보호와 데이터의 무결성을 제공하기 위하여 사용된다.

EAP-HNUA는 사용자 인증 수단으로 가장 일반적으로 사용되고 있는 ID/PW 기반의 EAP-HNUA-PW, 은행이나 증권, 인터넷 쇼핑 등에서 안전한 거래를 위해 사용되는 인증서 기반의 EAP-HNUA-TLS와 지문이나 홍채 등의 생체인식 기반의 EAP-HNUA-X9.84의 세 가지로 구성된다.

2. EAP(Extensible Authentication Protocol)

EAP는 유무선 네트워크 환경에서 사용자 인증을 위해 확장이 용이하도록 고안된 프레임워크이며,

현재 무선 인터넷이나 PPP 환경에서 주로 사용되고 있다. EAP는 공통 기능만을 정의하고, 확장 가능하도록 하여, 특정 인증 메커니즘을 적용할 수 있도록 하여, 현재 EAP-MD5, EAP-TLS, EAP-TTLS, PEAP, LEAP 등의 특정 인증 메커니즘을 적용한 많은 EAP 방식들이 사용되고 있다[5,6]. 본 논문에서도 EAP의 확장성을 이용하여 원격인증서버 기반의 홈네트워크 사용자 인증 프로토콜을 설계하였다.

3. 제안한 원격인증서버 기반의 사용자 인증 프로토콜

본 논문에서 제안한 원격인증서버 기반의 사용자 인증 프로토콜은 EAP와 TLS를 기반으로 하여 설계하였으며, 인증 수단을 크게 ID/PW, 인증서, 생체인식 기반의 세 가지 분류하여 프로토콜을 설계하였다. 각 인증마다 인증 프로토콜의 기본 과정은 유사하나 각 인증 수단마다의 상이한 특성을 수용하여 세 가지의 세부 인증 프로토콜을 설계하였다.

3.1 제안한 사용자 인증 프로토콜 설계 조건

- 사용자 인증 정보는 원격인증서버에 저장되어 있다.
- 사용자가 홈네트워크 서비스를 이용하는 형태는 댁내에서 서비스를 이용하는 경우와 댁외에서 서비스를 이용하는 경우로 나눌 수가 있는데, 사용자 인증 프로토콜은 댁내와 댁외에서 동일하게 적용되도록 단일 프로토콜로 한다.
- 사용자 인증시 클라이언트와 원격인증서버와의 통신은 홈게이트웨이를 통해 이루어지며, 전송되는 보안 정보는 홈게이트웨이에 노출되지 않도록 한다.
- 홈게이트웨이와 원격인증서버는 각각을 인증할 수 있는 인증서를 가지고 있어야 한다.
- 홈게이트웨이와 원격인증서버 간의 상호 인증은 TLS 기반의 인증서를 통하여 수행하고, 보안 통신을 위한 홈게이트웨이와 원격인증서버 간의 세션키를 생성한다.
- 홈게이트웨이와 원격인증서버 간의 인증 과정은 사용자 인증시마다 수행되는 것이 아니라 홈게이트웨이가 실행될 때, 원격인증서버와의 세션 연결이 끊어졌다가 다시 연결될 때 수행되도록 하여, 홈게이트웨이와 원격인증서버 간의 인증으로 인한 로드를 최소화 한다.
- 클라이언트는 원격인증서버의 인증을 TLS 기반의 인증서를 통하여 수행하고, 보안 통신을 위한 클라이언트와 원격인증서버 간의 세션키를 생성한다.
- 클라이언트의 인증 수단은 ID/PW 기반, 인증서 기반, 생체인식 기반의 인증이 가능하도록 한다.

3.2 제안한 사용자 인증 프로토콜 기본 과정

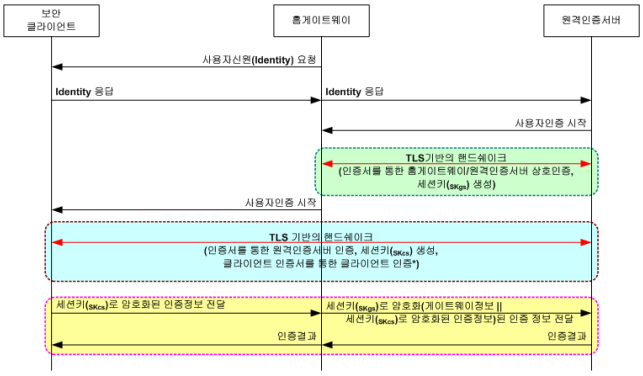

그림 1. 제안한 사용자 인증 프로토콜 기본 과정

본 논문에서 제안한 사용자 인증 프로토콜의 일반적인 인증 과정은 그림 1과 같다.

1) 사용자가 서비스 이용을 위해 홈게이트웨이에 접속하였을 때 사용자의 인증이 이루어지지 않았으면, 홈게이트웨는 사용자에 사용자 신원(Identity)을 요청한다.
2) 신원 요청을 받은 클라이언트는 인증 방식을 결정하여, 홈게이트웨이에 응답으로 전달하고, 홈게이트웨이는 이를 원격인증서버에 전달한다.
3) 원격인증서버는 클라이언트가 전달한 인증 방식으로 사용자 인증의 시작을 홈게이트웨이 알린다.
4) 홈게이트웨이와 원격인증서버는 TLS를 기반으로 서로의 인증서를 통해 상호인증을 수행하고 세션키(SKgs)를 구한다.
5) 홈게이트웨이는 클라이언트에 사용자 인증의 시작을 알린다.
6) 클라이언트는 TLS를 기반으로 원격인증서버의 인증서를 통해 원격인증서버를 인증하고 세션키(SKcs)를 구한다. 클라이언트의 인증서를 통한 클라이언트 인증 방식일 경우 클라이언트 인증을 수행한다.
7) 클라이언트는 인증 정보를 세션키(SKcs)로 암호화하여 원격인증서버에 전달한다. 이때 정보 전달의 중계를 하는 홈게이트웨이는 중계할 정보를 세션키(SKgs)로 암호화하여 원격인증서버에 전달한다. 필요시 홈게이트웨이 정보를 추가할 수 있다.

8) 원격인증서버는 클라이언트의 인증된 결과를 클라이언트에 전달한다.

3.3 기호

사용자 인증과정을 나타내는 그림에는 몇 가지의 기호들이 사용되는데, 그 기호들의 종류와 의미는 다음과 같다.

1) ||

"||" 기호는 Concatenation(병합)을 의미한다.

예) "abc" || "def" => "abcdef"

2) /

"/" 기호는 EAP 패킷 안의 구체적인 내용을 의미한다.

3) *

"*" 기호는 선택 사항을 의미한다.

4) $E_{SKcs}()$ 와 $E_{SKgs}()$

$E_{SKcs}()$ 기호는 ( )안의 내용을 인증과정에서 생성된 클라이언트와 관리서버 간의 보안을 위한 세션키로 암호화함을 의미한다.

$E_{SKgs}()$ 기호는 ( )안의 내용을 인증과정에서 생성된 홈게이트웨이와 관리서버 간의 보안을 위한 세션키로 암호화함을 의미한다.

3.4 사용자 인증 데이터 패킷 구조

사용자 인증 과정에서 사용되는 패킷은 크게 기본 데이터 패킷 구조, 서버 인증 과정의 데이터 패킷 구조, 사용자 인증 과정의 데이터 패킷 구조로 나눌 수 있으며, 기본적인 패킷 구조는 EAP 패킷 구조를 따른다.

3.4.1 기본 데이터 패킷 구조

사용자 인증에서 기본 데이터 패킷은 Identity와 Success, Failure 등을 나타낼 때 사용되는 패킷 구조로써, 그림 2와 같은 패킷 구조를 갖는다.

()안의 수는 바이트

Code (1)	Identifier (1)	Length (2)
Type (1)	Type-Data ...	

그림 2. 기본 데이터 패킷 구조

3.4.2 서버 인증 과정의 데이터 패킷 구조

서버 인증 과정의 데이터 패킷은 서버 인증 과정에만 사용되는 것이 아니라 사용자 인증 과정 중에 TLS 기반의 프로토콜에서 사용되는 패킷의 구조로써, EAP 패킷의 Type-Data 부분의 패킷 구성을 다르게 한 것으로, 패킷 구조는 그림 3과 같다.

()안의 수는 바이트

Code(1)	Identifier(1)	Length(2)
Type(1)	Flags(1)	TLS Message Length(2)
TLS Message Length(2)	TLS Data ...	

그림 3. 서버 인증 과정의 데이터 패킷 구조

3.4.3 사용자 인증 과정의 데이터 패킷 구조

사용자 인증 과정의 데이터 패킷은 사용자 인증 과정 중에 인증 정보나 Start 메시지 같은 데이터 전송에서 사용되는 패킷의 구조로써, EAP 패킷의 Type-Data 부분의 패킷 구성을 다르게 한 것으로, 패킷 구조는 그림 4와 같다.

()안의 수는 바이트

Code(1)	Identifier(1)	Length(2)
Type(1)	Flags(1)	Value-Size(2)
Value ...		

그림 4. 사용자 인증 과정의 데이터 패킷 구조

3.5 세부 인증 과정

3.5.1 ID/PW 기반 인증 과정

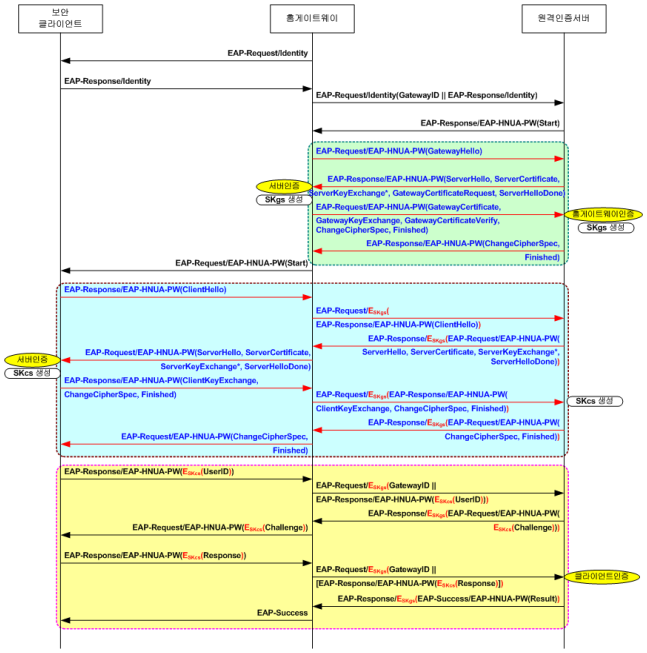

그림 5. ID/PW 기반 인증 과정

3.5.2 인증서 기반 인증 과정

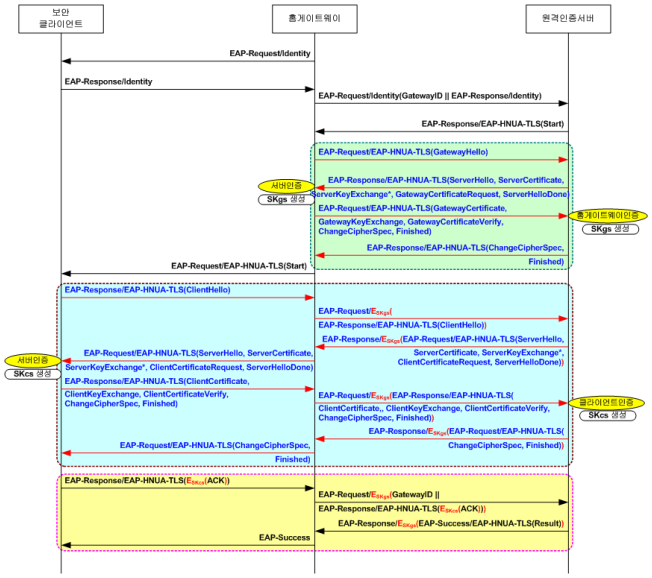

그림 6. 인증서 기반 인증 과정

3.5.3 생체인식 기반 인증 과정

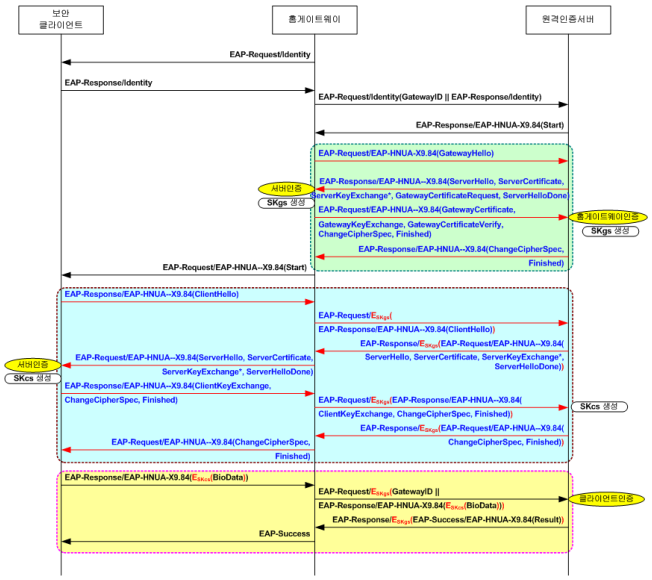

그림 7. 생체인식 기반 인증 과정

4. 결론

본 논문에서는 홈네트워크의 사용자 인증을 위해 다양한 인증 수단을 수용하고, 댁내와 댁외의 사용자 인증 메커니즘이 동일하도록 인증 절차를 단순화한 EAP와 TLS를 기반으로한 원격인증서버 기반의 사용자 인증 프로토콜을 설계하였다.

현재의 인증 방식은 크게 ID/PW 기반, 인증서 기반, 생체인식 기반의 세 분류로 나눌 수가 있어, 본 문에서도 ID/PW 기반, 인증서 기반, 생체인식 기반으로 나누어 세부 인증 프로토콜을 설계하였다.

인증 프로토콜은 새로운 인증 방식이 출현하면 그에 적합한 인증 프로토콜을 설계하여, 다양한 인증 수단을 모두 수용할 수 있는 확장성이 필요하다. 향후 확장성을 고려한 살계 요소를 도입할 예정이다.

참고문헌

[1] 이윤철, “최근의 홈 네트워크 기술동향 및 시장 전망”, 정보통신연구진흥원 주간기술동향 통권 1098호, 2003.6.4

[2] 박천교, “홈네트워크”, 정보통신연구진흥원 주간 기술통향 통권 1138호, 2004.3.24

[3] 최훈일, 장영건, “홈네트워크 시스템의 사용자 인증 및 접근제어 방법”, 한국정보처리학회 2006 년 추계 학술대회, Vol.13 No.02 pp.897~900, 2006.11

[4] Young Gun Jang, Hoon Il Choi, Chan Kon Park, "Implementation of Home Network Security System based on Remote Management Server", IJCSNS, Vol.7 No.2 pp.267~274, February 2007.

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

[6] Extensible Authentication Protocol, http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

[7] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 3546, June 2003