스마트 홈네트워크에서 경량화된 디바이스 인증/인가 기술에 관한 연구

문종식, 이임영
순천향대학교 컴퓨터학부
e-mail:comnik528@sch.ac.kr

A Study on Lightweight Device Authentication/Authorization Scheme in Smart Home Network

Jong-Sik Moon, Im-Yeong Lee
Division of Computer Science and Engineering, Soonchunhyang University

요 약

홈네트워크 기술은 통신과 방송 융합, 유비쿼터스 사회로의 빠른 이동 등 IT 전반적인 환경에서 빠른 변화와 함께 사용자의 특성을 고려해야함으로, 다양한 분야의 기술들이 융합되어 IT 분야 통합과 같은 성격을 가지고 있다. 최근 들어 디바이스 인증기능을 추가하여 유효한 디바이스를 통해서만 서비스를 제공 받을 수 있게 하는 한 단계 강화된 보안의 필요성이 제기되고 있으나, 이를 위해 먼저 보안 고려사항을 선행하여 점검해야 한다. 또한 유비쿼터스 홈네트워크로의 진화는 다양한 서비스 도메인에서 홈디바이스 이동이 증가될 것이며, 홈디바이스간의 협업에 의한 새로운 홈서비스가 증가할 것이다. 이와 같은 기술의 진화에 따라 유비쿼터스 환경에서 안전한 이동과 seamless한 서비스를 제공할 수 있도록 경량화된 홈디바이스 인증/인가 기술이필요하다. 따라서 홈네트워크 구성 요소들의 여러 가지 사항들을 고려하여, 댁내와 댁외 모두 사용할 수 있도록 안전하고 효율성있는 경량화된 디바이스 인증 및 인가 기술을 제안하였다.

1. 서론

홈네트워크 기술은 통신과 방송 융합, 유비쿼터스 사회로의 빠른 이동 등 IT 전반적인 환경에서 빠른 변화와 함께 사용자의 특성을 고려해야함으로, 다양한 분야의 기술들이 융합되어 IT 분야 통합과 같은 성격을 가지고 있다. 기간통신사업자를 축으로 기간망의 고도화로 시작된 네트워크 인프라는 이제 최후의 실핏줄인 홈네트워크로 발전하고 있으며, 홈네트워크 기술은 유선뿐 아니라 무선 부분에서도 급속한 발전을 이루고 있다. 이러한 홈네트워크가 발전하게 되는 가장 중요한 이유는 인터넷의 급격한 발전으로 이뤄지고 있으며, 현재, 초기에 비해 다양한 서비스는 물론 지능형 서비스를 통해 브로드밴드 서비스가 이뤄지고 있다.

또한 언제 어디서나 컴퓨팅이 가능한 유비쿼터스 컴퓨팅 사회에서는 개인의 컴퓨팅 환경 의존도가 증가함에 따라 사이버공격뿐 아니라 홈네트워크 및 홈 디바이스의 취약성을 이용한 댁내 홈네트워크에 대한 불법적인 접근이 가능함으로 인해, 홈디바이스에 대한 안전성 확인을 통해 유효한 홈디바이스만 홈네트워크에 접근할 수 있어야 한다. 또한 불법적인 서비스의 접근을 차단하기 위해 사용자 인증기술이 사용되고 있으나, 최근 들어 디바이스 인증기능을 추가하여 유효한 디바이스를 통해서만 서비스를 제공 받을 수 있게 하는 한 단계 강화된 보안의 필요성이 제기되고 있으나, 이를 위해 먼저 보안 고려사항을 선행하여 점검해야 한다. 또한 유비쿼터스 홈네트워크로의 진화는 다양한 서비스 도메인에서 홈디바이스 이동이 증가될 것이며, 홈디바이스간의 협업에 의한 새로운 홈서비스가 증가할 것이다. 이와 같은 기술의 진화에 따라 유비쿼터스 환경에서 안전한 이동과 seamless한 서비스를 제공할 수 있도록 경량화된 홈디바이스 인증/인가 기술이필요하다. 유비쿼터스 홈네트워크 환경에서는 단순한 네트워크 인증이나 미들웨어레벨의 인증만으로 안전하게 홈네트워크가 보호될 수 없기 때문에 유비쿼터스 홈네트워크 디바이스 인증기술 개발이 필요하다[6][7][8]. 따라서 홈네트워크 구성 요소들의 여러 가지 사항들을 고려하여, 댁내와 댁외 모두 사용할 수 있도록 인증 및 인가서로써 디바이스 인증 및 인가 기능을 제공하여야 한다. 본 논문의 구성은 다음과 같다. 2장에서는 홈 네트워크 인증/인가 보안 요구사항에 대하여 기술하고, 3장에서는 홈디바이스 인증/인가 기존 연구에 대하여 알아본다. 4장에서는 경량화된 디바이스 인증/인가 기술을 제안하고, 5장에서는 2장의 보안 요구 사항으로 제안 방식을 분석한다. 마지막으로 6장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

2. 보안 요구사항

기존의 유선 네트워크와는 다르게 홈 네트워크에서는 기존의 일반적인 보안 요구 사항 외에 홈 네트워크 특성에 적합한 보안 요구 사항이 필요하며, 자신의 홈 네트워크 내에서 제공하는 서비스 외에 다른 사업자가 제공하는 홈 네트워크로 이동하여 서비스를 제공받을 수 있기 때문에 그에 대한 요구 사항도 고려해야 한다.

- 기밀성(Confidentiality) : 통신에 사용되는 데이터는 정당한 객체만이 확인할 수 있어야 한다. 공격자로부터 불법적인 획득으로 비밀 값을 노출되지 않도록 해야 한다.
- 무결성(Integrity) : 정보 시스템에 저장되어 있거나 네트워크를 통해 전송되는 데이터가 위변조 되거나 삭제되지 않도록 해야 한다.
- 인증(Authentication) : 비스를 이용하고자 접근하는 사용자가 전송한 메시지 또는 전자문서의 출처가 정확히 확인되고, 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다.
- 접근제어(Access Control) : 정보 자원에 대한 읽기나 변경 등의 모든 접근 행위에 대해 그 권한을 명백히 구분해 허가되지 않은 접근 시도를 사전에 차단할 수 있도록 하는 통제가 필요하다.
- 재전송 공격(Replay Attack) :통신 중에 전송되는 데이터를 제 3자가 획득하여 메시지를 재전송함으로써 인증 받는 것을 막을 수 있어야 한다.
- 빠른 로밍 인증 : 자신의 홈 네트워크 환경에서 다른 서비스 제공자가 제공하는 홈 네트워크의 서비스를 이용하고자 이동할 경우, 인증에 소요되는 시간이 오래 걸리게 되면 끊김 없는 서비스를 제공할 수 없다. 따라서 이동 디바이스에게 끊김 없는 서비스를 제공하기 위해서는 인증 소요시간이 짧으며, 경량화된 인증에 대한 고려가 필요하다.
- 홈 인증 서버의 오버헤드 : 다른 사업자가 제공하는 홈 네트워크 서비스를 이용할 경우, 원격지에서 홈 인증 서버로 전송되는 인증 요청이 빈번하게 일어나면 홈 인증 서버의 오버헤드가 발생할 수 있다. 따라서 자신의 홈 네트워크 인증 서버로 요청되는 인증 및 접근을 감소시키거나 분산시켜 오버헤드를 줄이는 방안에 대한 고려가 필요하다.

3. 기존 연구

홈디바이스의 인증/인가에 관한 기존연구는 다음과 같다.

3.1 Inter-Domain 디바이스 인증/접근제어 방식

Inter-Domain 디바이스 인증/접근제어 방식은 효율적인 통신과 사용자 편의를 위해 two-layer PKI 기반 디바이스 인증과 접근제어 방식을 제안하였다[3][4]. 이 방식에서의 Two-layer는 글로벌 PKI layer과 지역적 PKI layer이며, 글로벌 PKI layer는 기존의 PKI 모델을 사용하였다. Inter 홈네트워크의 디바이스 등록과 인증을 위해서 글로벌 PKI layer를 사용하였으며, 각 종단 디바이스 인증을 위해 지역적 PKI layer를 사용하였다. Inter-Domain 디바이스 인증/접근제어 방식은 안전성과 효율성 그리고 Multi-Domain 디바이스 인증 프로토콜로 사용자의 편의성을 제공하며, Attribute Mapping Certificate를 사용하여 접근제어 방식의 편의성을 제공한다. 그러나 PKI 기반 방식을 사용함으로써 계산량의 효율성이 떨어지며, Root CA와 홈게이트웨이에 오버헤드가 발생한다. 또한 Manufacturer의 추가로 인해 통신량이 증가되는 단점이 있다.

3.1 S/Key 기반 홈디바이스 인증 방식

S/key 기반 홈디바이스 인증 방식은 홈네트워크 보안의 기본적이고 본질적 요소의 홈디바이스 인증을 소개하며[5], 스마트 홈네트워크에서 안전한 무선 접근을 위해 S/Key 기반 외부 홈 인증 방식과 내부 홈 인증 방식을 제안하여, 홈네트워크 서비스 사용자의 편의성 및 안전성을 제공하였다[1]. 그러나 Exclusive OR 연산으로 계산량의 감소는 가져왔으나 통신로 상의 도청으로 인해 비밀정보의 유출 및 재잰송 공격에 취약하며 HDC(Home Device Certificate) 발행단계로 인한 통신량이 증가되는 단점을 가지고 있다.

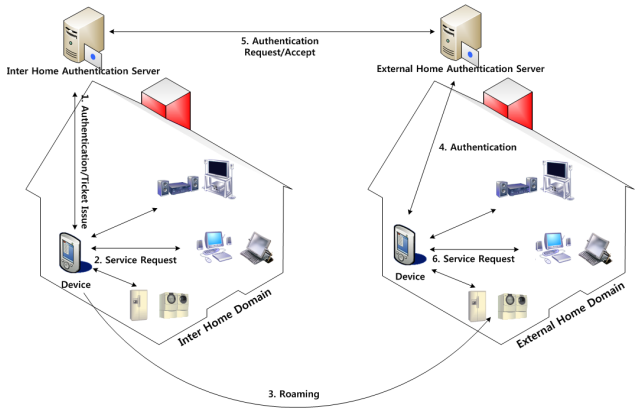
4. 제안 방식

제안 방식은 (그림 1)과 같이 스마트 홈네트워크 환경에서 디바이스가 홈 인증 서버로부터 인증을 받고 인가 티켓을 발급받아 홈네트워크 서비스에게 인가 티켓을 제시하고 서비스를 제공받을 수 있다. 또한 디바이스가 다른 사업자가 제공하는 홈네트워크 서비스를 이용할 경우 외부 홈도메인에 내부 홈도메인에서 발급받은 인가 티켓을 제공하고 인증을 받고 서비스를 제공받을 수 있다.

4.1 시스템 계수

본 제안 방식에서는 다음과 같은 시스템 계수를 이용한다.

- $*$: 각각의 개체 (D : 디바이스, $IHAS$: 내부 홈네트워크 인증 서버, $OHAS$: 외부 홈네트워크 인증 서버, HNS : 홈네트워크 서비스)
  - ID_* : $*$의 아이디
  - OTP : 일회용 패스워드
  - g : 곱셈군 Z_n^*의 생성자
  - $h()$: 충돌성이 없는 안전한 일방향 해쉬 함수
  - CT : OTP 입력 값으로 D와 $IHAS$ 간에 동기화되어 있는 카운터
  - e : $G_1 \times G_1 \rightarrow G_2$ 겹선형 사상



(그림 1) 제안 방식 전체 흐름도

- $E_*[\,]$: $*$의 키로 암호화
- $Sign_*$: $*$의 개인키로 서명
- KS : D와 $IHAS$가 공유한 대칭키
- $service\_key$: $IHAS$와 HNS가 공유한 서비스키
- KU_* : $*$의 ID 기반 공개키
- KR_* : $*$의 ID 기반 개인키

4.2 제안 프로토콜

제안 프로토콜은 내부 홈네트워크에서 홈디바이스 인증 및 인가 티켓 발행 단계, 외부 홈네트워크에서 홈디바이스 인증 단계로 이루어지며, 디바이스와 내부 홈네트워크 인증 서버간 공유한 대칭키는 사전에 분배되었다고 가정한다.

4.2.1. 홈디바이스 인증 및 인가 티켓 발행 단계

디바이스가 자신의 내부 홈네트워크 인증 서버에게 인증을 요청하면 인증 서버는 사용자 권한에 맞는 인가 티켓을 발행하고 홈네트워크 서비스들에게 디바이스의 인가 티켓과 아이디를 브로드캐스팅한다. 디바이스는 홈네트워크 서비스를 이용할 때 인가 티켓을 제시하고 서비스를 제공받는다.

Step 1. 디바이스는 OTP를 생성하고 ID기반 개인키/공개키 쌍을 생성하고 인증을 요청한다.

$OTP = h(PIN \oplus KS \oplus CT)$

$KU_D = ID_D$

$KR_D = ID_D \cdot g^{OTP}$

$ID_D,\ ID_{IHAS},\ E_{KS}[OTP,\ CT]$

Step 2. 내부 홈네트워크 인증 서버는 전송된 값과 데이터베이스에 저장되어 있는 값을 통해 OTP′를 생성하고 디바이스의 OTP와 비교하여 인증한다. 인증이 완료되면 홈네트워크 인증 서버의 ID기반 개인키/공개키 쌍을 생성하고 인가 값과 인가 티켓을 생성한 후, 디바이스의 공개키로 암호화 하여 전송한다.

$h(PIN \oplus KS \oplus CT) = OTP'$

$OTP' \stackrel{?}{=} OTP$

$KU_{IHAS} = ID_{IHAS}$

$KR_{IHAS} = ID_{IHAS} \cdot g^{OTP}$

$Authorization\ \ Value = e(KR_{IHAS},\ KS \cdot ID_D)$

$Authorization\ \ Ticket = ID_D,\ ID_{IHAS},\ Sign_{IHAS}[h(Authorization\ \ Value)]$

$E_{KU_D}[Authorization\ \ Value, Authorization\ \ Ticket]$

Step 3. 디바이스는 자신의 개인키와 내부 홈네트워크 인증 서버의 아이디, 대칭키를 Admissible Bilinear Map을 이용하여 내부 홈네트워크 인증 서버로부터 전송받은 값을 검증한다.

$Authorization\ \ Value' = e(KR_D,\ KS \cdot ID_{IHAS})$

$Authorization\ \ Value' \stackrel{?}{=} Authorization\ \ Value$

Step 4. 내부 홈네트워크 인증 서버는 홈네트워크 서비스들에게 사전에 공유한 서비스키로 디바이스의 아이디와 인가 티켓을 암호화하고 서명하여 브로드캐스팅 한다.

$E_{service\_key_{IHAS-HNS}}[Sign_{IHAS}[ID_D,\ Authorization\ \ Ticket]]$

Step 5. 디바이스는 홈네트워크 서비스에게 티켓을 제시하면 홈네트워크 서비스는 티켓을 검증한 후 디바이스에게 서비스를 제공한다.

4.2.2. 외부 홈네트워크에서 홈디바이스 인증 단계

이 단계에서는 디바이스가 다른 사업자가 제공하는 홈네트워크 서비스를 이용할 경우 외부 홈도메인에 내부 홈도메인에서 발급받은 인가 티켓을 제공하고 인증을 받고 서비스를 제공받을 수 있다.

Step 1. 디바이스는 외부 홈네트워크 인증 서버에게 내부 홈네트워크 인증서버로부터 발급받은 인가 티켓을 내부 홈네트워크 인증 서버의 공개키로 암호화하여 아이디와 함께 전송한다.

$ID_D,\ ID_{IHAS},\ E_{KU_{IHAS}}[Authorization\ \ Ticket]$

Step 2. 외부 홈네트워크 인증 서버는 내부 홈네트워크 인증 서버에게 디바이스로부터 전송받은 값을 전달하고, 내부 홈네트워크 인증 서버는 인가 티켓을 검증한 후, 서비스에 접근할 수 있는 인가 티켓을 서명한 후 외부 홈네트워크 인증 서버에게 전송한다. 외부 홈네트워크 인증 서버는 전송받은 티켓을 외부 홈네트워크 서비스에게 브로드캐스팅한다.

$E_{KU_{IHAS}}[Authorization\ \ Ticket]$

$Access\_Accept,\ Sign_{IHAS}[Authorization\ \ Ticket]$

$E_{service\_key_{HNS-OHAS}}[Sign_{OHAS}[ID_D,\ Authorization\ \ Ticket]]$

Step 3. 디바이스는 외부 홈네트워크 서비스에게 티켓을

제시하면 외부 홈네트워크 서비스는 티켓을 검증한 후 디바이스에게 서비스를 제공한다.

5. 제안 방식 분석

제안 방식을 2장에서 언급한 일반적인 보안 요구사항과 홈네트워크에서의 보안 요구사항에 맞추어 분석하면 다음과 같다.

- 기밀성(Confidentiality) : 제안 방식은 디바이스와 내부 홈네트워크 인증 서버간에 공유한 대칭키(*KS*)와 ID기반 개인키/공개키 쌍으로 메시지를 암호화하기 때문에 기밀성을 제공할 수 있다.
- 무결성(Integrity) : 디바이스의 인증 값인 OTP와 인가 값 등을 해쉬하여 무결성이 제공된다.
- 인증(Authentication) : 디바이스가 내부 홈네트워크 인증 서버에게 OTP를 제공하여 인증 받을 수 있으며, 내부 홈네트워크 인증 서버는 디바이스에게 인가 값과 인가 티켓을 제공하여 디바이스는 홈네트워크 인증 서버를 검증할 수 있다.
- 접근제어(Access Control) : 정당하게 인증 받지 못한 디바이스는 인가 티켓을 발행 받을 수 없어 서비스 및 홈네트워크에 접근할 수 없다.
- 재전송 공격(Replay Attack) : 제안 방식은 카운터 기반 OTP를 사용함으로써 매번 패스워드 값이 변경되기 때문에 재전송공격으로부터 안전하며, 인가 티켓에 포함되어 있는 인가 값의 구성요소에 OTP가 있기 때문에 재전송공격에 안전하다.
- 빠른 로밍 인증 : 자신의 홈 네트워크 환경에서 다른 서비스 제공자가 제공하는 홈 네트워크의 서비스를 이용하고자 이동할 경우, 외부 홈네트워에서 다시 인증을 받고 인가 티켓을 발행받지 않고 내부 홈네트워크에서 발행받은 인가 티켓을 제시하여 인증을 제공받음으로써 빠르게 인증을 받고 서비스를 제공받을 수 있다.
- 홈 인증 서버의 오버헤드 : 디바이스가 외부 홈네트워크로 이동하여 인증을 요청하면 내부 홈네트워크 인증 서버는 외부 홈네트워크 인증 서버에게 인가 티켓을 전송하고 홈네트워크 서비스에 브로드캐스팅 해줌으로써 디바이스는 이후 인가 티켓만으로 서비스를 제공받을 수 있어 내부 홈네트워크 인증 서버에 서비스 요청을 하지 않아도 되기 때문에 오버헤드가 줄어든다.

6. 결론

인터넷 및 디바이스의 발전과 유비쿼터스 시대의 도래됨에 따라 스마트 홈네트워크에서 디바이스를 이용하여 서비스를 제공받고자 하는 수요의 빠르게 증가하고 있다. 그러나 디바이스의 다양성과 디바이스간 자원 공유 등으로 보안 측면에서 고려해야 할 요구사항은 더욱 복잡해지고 다양화될 것이며, 스마트 홈네트워크에서 서비스를 제공받는데 있어 기존의 매체나 프로토콜이 갖고 있는 보안 취약성을 그대로 갖고 있으며, 인터넷과의 연결로 기존에 사용되던 네트워크 기반의 사이버공격 기술이 홈네트워크에 그대로 적용될 수 있는 문제점을 갖고 있다. 뿐만 아니라 스마트 홈네트워크 디바이스는 상대적으로 컴퓨팅 능력이 낮아 개발된 보안 기능의 탑재가 어려우므로 단말 해킹, 바이러스 공격, 정보유출 등 다양한 공격이 시도될 가능성이 높다고 할 수 있다.

따라서 본 연구는 스마트 홈네트워크 환경에 적합하고 보안 요구사항을 고려하여 안전한 서비스를 제공할 수 있는 경량화된 디바이스 인증/인가에 관한 연구를 진행하였다. 디바이스를 인증을 위해 OTP를 사용하였으며, 내부 홈네트워크 인증 서버의 인증을 위해 ID 기반 공개키 방식과 Admissible Bilinear Map을 이용하여 인가 값을 검증함으로써 상호인증을 제공할 수 있게 하였다. 또한 발급받은 인가 티켓을 외부 홈네트워크로 이동하여 제시함으로써 인증을 받고 서비스를 제공받아 빠른 로밍 인증 및 내부 홈네트워크 인증 서버의 오버헤드를 줄일 수 있다. 따라서 홈디바이스를 이용하여 서비스를 제공받는데 있어 안전성과 효율성을 제공할 수 있다. 향후 TTA에서 표준화한 외부 인증서 기반 인증/인가 및 댁내 인증서 기반 인증/인가 구조에 적합한 경량화된 디바이스 인증/인가 방식에 대한 연구가 필요할 것으로 사료된다.

참고문헌

[1] Deok-Gyu Lee, Ilsun You, Sang-Choon Kim, Yun-kyung Lee, Jong-wook Han, and Kyo-il Chung, "Intelligent Home Network Authentication SKey-Based Home Device Authentication,"ISPA 2007 Workshops, LNCS 4743, pp. 214-223, 2007.

[2] Hyungkyu Lee, Jongwook Han and Kyoil Chung, "Security Architectrue for Authentication and Authorization in the Intelligent and Ubiquitous Home Network," ICIC 2007, pp. 1110-1118, 2007.

[3] Jin-Bum Hwang, Hyung-Kyu Lee, and Jong-Wook Han, "Efficient and User Friendly Inter-Domain Device Authentication/Access Control for Home Networks,"EUC 2006, LNCS 4096, pp. 131-140, 2006.

[4] Jin-Bum Hwang and Jong-Wook Han, "A Security Model for Home Networks with Authority Delegation,"ICCSA 2006, LNCS 3983, pp. 360-369, 2006.

[5] Yun-kyung Lee, Deok Gyu Lee, Jong-wook Han, "Home Device Authentication Method based on PKI," fgcn 2007, pp. 7-11, 2007.

[6] 김도우, 한종욱, 정교일, "홈디바이스 인증/인가 기술동향," 주간기술동향 통권 1329호, 2008.

[7] 이윤경, 한종욱, 정교일, "홈네트워크 보안 표준화 동향," 전자통신동향분석, 제22권, 제 호, 2007.

[8] 홈네트워크에 적용 가능한 홈 디바이스 인증서 프로파일, TTA, TTAS.KO-12.0052, 2007.