홈네트워크 환경에서 공개키 기반의 홈디바이스 인증

이윤경* · 이덕규*· 한종욱*

*한국전자통신연구원

PKI Based Home Device Authentication in Home Network

Yun-kyung Lee* · Deok Gyu Lee*· Jong-wook Han*

*Electronics and Telecommunications Research Institute

E-mail : neohappy@etri.re.kr

요 약

홈네트워킹이 댁내의 기기들 간의 연동뿐만 아니라, 이동성에 따른 여러 가지 시나리오가 발생할 수 있다. 이런 경우, 사용자 인증 기능으로 어느 정도의 홈네트워크 보안을 해결할 수는 있지만 한계가 있을 수 있다. 또한 사용자의 개입이 필요한 사용자 인증이 아니라, 사용자가 의식하지 못하는 사이에 홈디바이스에 대한 인증만으로 접근할 수 있는 서비스도 존재하므로 홈디바이스 인증은 더욱 필요하다고 하겠다. 본 논문에서는 공개키 기반의 홈디바이스 인증 체계 및 인증서 프로파일, 그리고 인증 방법에 관하여 기술하고자 한다.

키워드

홈디바이스 인증, 공개키, 디바이스 인증서, 디바이스 인증서 프로파일

Ⅰ. 서 론

유비쿼터스 컴퓨팅은 보안에 있어 특히 취약한 면을 많이 내포하고 있는데, 그 중에서도 분산된 다양한 컴퓨팅 기기들이 도처에 존재함으로 인해 사용자 주변에 있는 기기 중에서 사용자 혹은 서버에 인증된 기기로의 위장공격 등이 가능해진다. 그리고, 홈네트워크 서비스를 이용하는데 있어서 권한이 있는 사용자만이 서비스를 이용할 수 있도록 하기 위해서 사용자 인증/인가 기술을 홈네트워크 서비스에 이용해 왔으나, 사용자의 실수로 인한 사용자 인증정보의 유출, 추측 가능한 인증정보의 사용 및 기존 인증수단의 새로운 취약성 발견 등과같이 기존 사용자 인증기술에 문제가 있다. 그래서 사용자 인증기능외에 디바이스 인증기능을 추가함으로써 신뢰할 수 있는 디바이스만을 사용해서 홈네트워크 서비스를 받을 수 있도록 할 필요성이 제기되었다. 또한 다양한 유무선 네트워크가 사용되고 있는 홈네트워크의 특성상 주변 홈네트워크의 디바이스를 이용하여 불법적인 접근이 이루어질 가능성이 높으므로 자신의 홈네트워크에서만 사용할 수 있도록 소유하고 있는 디바이스에 대해 신뢰성을 부여할 필요가 있다. 또한 향후 홈서비스는 사용자 개입을 최소화하고, 디바이스들 간의 협업으로 사용자에게 서비스를 제공하는 형태로 진화할 것이므로 디바이스 상호인증을 통한 안전한 협업관계 구축이 더욱 중요한 필수요소가 될 것이라 본다.

Ⅱ. 홈디바이스 인증

2.1. 홈디바이스 인증 구조

본 논문에서는 홈서버와 홈디바이스간의 디바이스 인증뿐만 아니라, 홈디바이스들 간의 디바이스 인증 및 우리집의 홈디바이스와 친구네 집의 홈디바이스간의 디바이스 인증을 모두 고려할 수 있는 공개키 방법을 이용한 홈디바이스 인증 메커니즘을 제안하고자 한다. 본 논문에서 고려하는 공개키 기반 시스템(PKI)은 personal CA[1,2]가 아닌 public CA를 고려한다. [1,2]에서는 personal area network에 포함된 디바이스들의 인증만을 고려하였기 때문에 personal CA를 이용하는 것이 적절할 수 있지만, 본 논문에서 고려하는 홈디바이스 인증은 우리집 내의 홈디바이스들 간의 인증뿐만 아니라, 우리집 홈디바이스를 다른집에 가져갔을 때에도 홈네트워크 서비스를 이용하기 위한 디바이스 인증까지를 고려하기 때문에 personal CA 보다는 public CA를 고려하는 것이 더욱 적절하다고 본다.

본 논문에서 제안하는 홈디바이스 인증 체계는 CA(Certificate Authority)들을 관리하는 Root CA가 있고, 일부 RA(Registration Authority)의 기능을 하면서, 홈에 존재하는 HRA(Home RA)로 구성된 PKI 구조를 따른다. 구현에 따라서 루트CA가 디바이스를 직접 관리하면 중간CA가 생략될 수 있고, 위 그림처럼 루트CA는 CA들의 관리 기능만을 하고, CA들이 디바이스들을 관리하는 구조가 될 수도 있다. HRA는 홈에 존재하는 하나의 디바이스로써, 다른 홈디바이스보다 약간의 권한을 더 많이 갖는다. 즉, 일반 디바이스에 비해 조금 더 많은 공신력을 가진다. HRA는 댁내의 디바이스들 중 편리한 사용자 인터페이스를 갖고 있고, 홈디바이스들과 통신할 수 있는 통신수단을 갖고 있어야 한다. 또한 다른 홈디바이스들과 관련된 정보들을 저장하고 있어야 하므로 외부 공격으로부터 이들 데이터를 안전하게 보관할 수 있어야 한다. 그리고 HRA는 홈디바이스의 등록 및 관리의 책임을 진다. 또한, 디바이스 인증 경로에 있어서, HRA는 device보다 상위의 개념이 될 수 없고, 다만, HRA는 디바이스를 등록하는 과정에 있어서 중요한 역할을 수행하는 하나의 디바이스일 뿐이다.

2.2. 홈디바이스 등록 및 인증서 발급과정

본 절에서는 홈디바이스 등록 및 디바이스 인증서 발급 과정에 관하여 기술하고자 한다. 디바이스 등록 및 인증서 발행 과정에는 사용자의 개입이 필요한데, 특히 몇몇 과정은 사용자를 통해서 off-line 방법으로 이루어져야 한다. 디바이스 등록 및 인증서 발행 과정은 다음의 순서를 따른다.

(0) 홈네트워킹이 가능한 디바이스를 구입하여 집에 가져온다.

(1) 집에 있는 HRA에 디바이스를 등록한다. 이때 디바이스 identity 정보와 디바이스 인증서 발급에 필요한 여러 정보들을 입력할 필요가 있을 것이다.

$$Device \rightarrow HRA : [ID_D, AP]$$

(2) HRA와 device manufacturer portal 사이에 TLS 터널을 형성하고, 이를 이용해서 HRA는 디바이스 생산자가 운영하는 서버에 해당 디바이스의 ID정보를 전송해서 디바이스의 유효성을 확인한다.

$$HRA \rightarrow Manufacturer : [ID_D, ID_{HRA}, AP]$$

(3) 디바이스 생산자는 디바이스 identity 정보를 확인해서 자신이 생산한 디바이스가 맞는지 여부를 확인하고, 그 결과를 TLS 터널을 통해서 HRA와 CA로 전송한다.

(4) 디바이스 제조사 포탈로부터 디바이스 확인 성공메시지를 받으면 HRA는 해당 device를 대신해서 키쌍을 생성한다.

(5) HRA는 CA에게 해당 디바이스의 디바이스 인증서 발급 요청 메시지를 전송한다.

$$HRA \rightarrow CA : [ID_D, ID_{HRA}, AP]$$

(6) CA는 HRA의 디바이스 인증서 발급 요청 메시지에 해당하는 디바이스의 ID확인 성공 메시지를 디바이스 제조사 포탈로부터 받은 경우 홈디바이스 인증서를 발급하고, 그렇지 않다면 디바이스 인증서 발급요청을 거절한다.

$$CA \rightarrow HRA : Cert_{CA}[ID_D, ID_{HRA}, AP]$$

(7) HRA는 CA에게서 발급받은 홈디바이스 인증서를 해당 디바이스에게 off-line의 방법으로 전송한다. 이 과정에서 사용자의 개입이 필요할 것이다.

$$HRA \rightarrow Device : HRAC = Cert_{HRA}[ID_D, h(Cert_{CA} \| r)] \| AP$$

앞서 언급한 디바이스 ID는 디바이스를 구분할 수 있는 요소를 의미하는데, 완전히 새로운 디바이스ID 체계가 나올 수도 있고, 디바이스의 시리얼넘버 혹은 바코드같은 정보가 될 수도 있을 것이다. 그리고 본 논문에서 기술한 HRA는 일반적인 PKI의 RA처럼 엔터티의 ID와 디바이스 인증서에 기술된 내용들을 확인하는 기능을 한다.

본 논문에서 언급한 HRA는 일반적인 PKI에서의 RA와는 달리 완벽한 공신력을 갖춘 CA의 개념이 아니라, 홈 디바이스의 일종이다. 그리고 다른 홈 디바이스들 보다 컴퓨팅 파워나 보안측면에서 동등 혹은 그 이상을 갖춘 디바이스 이다. 따라서 컴퓨팅 파워가 많이 사용되는 키쌍 생성을 홈디바이스 대신 하고, HRA가 홈디바이스의 인증서를 받아서 이를 사용자가 off-line으로 홈디바이스에 로딩할 필요가 있다.

III. 홈디바이스 인증서 프로파일

홈디바이스 인증서는 X.509인증서[3,4]의 기본 형식을 따른다. 즉 X.509 v1 인증서를 그대로 따르고, X.509 v3 인증서에서 추가된 부분인 extensions 필드에 홈디바이스 인증에 필요한 항목들을 추가하였고, X.509 v3 인증서의 확장필드에 정의된 항목들 중 홈디바이스 인증과 관계 없는 부분은 디바이스 인증서에 정의하지 않았다. 비록 디바이스 인증서가 X.509 인증서와 인증하고자 하는 대상에서 약간의 차이가 있지만 - 본 논문에서 제안하는 홈디바이스 인증서는 홈 내의 디바이스들을 인증하기 위한 것이고, X.509인증서는 사용자, 서버, 기업체, 라우터 등을 인증하기 위한 것이다.- X.509 인증서가 워낙 널리 퍼져서 사용되고 있으므로 X.509 인증서를 중심으로 디바이스 인증서를 구현하는 것이 효율적이라고 생각한다. 다음은 인증서에서 수정된 부분에 대한 설명이다.

3.1. signature

이 필드는 해당 인증서에 서명하기 위해서 CA가 사용한 알고리듬에 대한 알고리듬 식별자를 담고있다. 이 필드는 기본적으로 X.509 인증서와 동일하지만, X.509인증서에서는 RSA 알고리듬의

사용을 권고하지만, 디바이스 인증서에서는 홈디바이스의 특성을 고려하여 ECDSA(Elliptic Curve Digital Signature Algorithm) 혹은 EC-KCDSA 서명 알고리듬을 주로 사용할 것을 권한다.

3.2. subject

Subject 필드는 subject public key 필드에 저장된 공개키와 연관된 홈디바이스를 식별한다. 이 필드는 X.509 인증서의 subject 필드를 따르지만, 'organization'항목에 디바이스 제조사 정보가 들어가야하고, 'common name' 항목에는 디바이스 인식번호(예를들면, 디바이스 시리얼 넘버 혹은 MAC 주소등)가 들어가야 한다. 그리고, 'organizational unit'항목에 디바이스 제조사 정보가 들어갈 수도 있다.

3.3. extensions

홈디바이스 인증서에 정의된 확장은 기존 X.509인증서에서 정의된 확장 중 5개(Authority Key Identifier, Subject Key Identifier, Key Usage, Basic Constraints, CRL Distribution Points)를 사용하고, 3개의 확장(HRA Information, HRA Ownership, Device Description)이 추가되었다. 이 절에서는 새롭게 추가된 3개의 확장필드에 대해서만 언급한다.

3.3.1. Home RA Information extension

이 확장은 HRA위 위치정보를 기수하기 위한 확장으로 HRA를 포함한 홈디바이스용 인증서에 사용될 수 있으며, non-critical로 설정되어야 한다. 이 확장의 값들은 암호화된 결과값이 인증서에 기록되어야 하고, 암호화에 사용된 키는 인증기관이 관리한다. 이 확장의 ASN.1 표기형식은 다음과 같다.

```
HRAInfo::= SEQUENCE{
        IPAddr iPAddress OPTIONAL,
        PostAddr UTF8String OPTIONAL}
iPAddress ::= OCTET STRING
```

3.3.2. Home RA Ownership extension

이 확장은 HRA 소유자 정보를 기술하기위한 확장필드로, 홈의 대표자 정보를 기록한다. 홈디바이스용 인증서에 사용될 수 있으며, non-critical로 설정되어야 한다. 이 확장필드의 값들 중 'RealName' 항목의 값은 암호화된 값이 기록되어야 하고, 암호화에 사용된 키는 인증기관이 관리한다. 이 확장의 ASN.1 구조는 다음과 같다.

```
HRAOwner::= SEQUENCE{
        hRA  BOOLEAN  DEFAULT TRUE,
        RealName  UTF8String OPTIONAL}
```

3.3.3. Device Description extension

이 확장은 디바이스의 간략한 기능을 기술하기 위한 확장이다. 이 확장은 홈디바이스용 인증서에 사용될 수 있으며, non-critical를 설정되어야 한다. 하지만, 인증기관용 인증서에는 존재하지 않아야 한다. 이 확장의 ASN.1 구조는 다음과 같다.

```
deviceDescription::= BIT STRING{
        typeA    [0],
        typeB    [1],
        typeC    [2] }
```

이 확장은 해당되는 비트를 '1'로 세팅하여 홈디바이스의 주요기능을 나타내는데, 홈디바이스에 따라서 복수선택이 가능하다. 'typeA' 디바이스는 다른 디바이스들을 컨트롤 할 수 있는 능력을 갖춘 디바이스를 의미하고, 'typeB' 디바이스는 서로다른 통신수단을 사용하는 디바이스들을 연결하기 위한 브릿지 역할을 하는 디바이스, 'typeC' 디바이스는 홈네트워킹에 참여하여 통신할 수 있는 인터페이스가 없는 디바이스를 의미한다.

Ⅳ. 디바이스 인증 방법

다음은 본 제안 방식에 대한 자세한 흐름을 기술한다. 첫 번째 방식은 사용자가 자신의 스마트 디바이스를 가지고 자신의 도메인으로 이동하여 이동한 공간의 디바이스를 이용하고자 할 때 자신의 인증 정보가 포함된 스마트 디바이스를 통해 인증을 받게 되는 방식이다. 두 번째 방식은 사용자가 자신의 스마트 디바이스를 가지고 단일 도메인이 아닌 멀티 도메인으로 이동하여 그곳의 디바이스를 이용하고자 할 때 자신의 인증 정보가 포함된 스마트 디바이스를 통해 인증을 받게 되는 것이다.

1) 단일 도메인 상에서의 인증

단일 도메인에 홈디바이스가 위치한 경우 HRA에서 사용하고자 할 경우 기존 정보를 그대로 이용하게 된다.

Step 1. 홈디바이스는 단일 도메인에 위치해 있다가 이동이 발생할 경우 이동 신호를 HRA에게 보낸다.

$$Device \rightarrow HRA : Signal(Outgoing)$$

Step 2. HRA는 Single Domain에게 홈디바이스의 이동을 알린다.

$$HRA \rightarrow single-domain : E_{PK_{HRA}}[ID_D, HRAC]$$

Step 3. HRA는 또한 다른 Single-domain에게 홈디바이스 정보를 알린다.

$$HRA \rightarrow other\ single-domain : \left[ID_{D'}, E_{PK_{HRA}}[ID_D, HRAC]\right]$$

Step 4. 다른 single-domain 은 HRA로부터 전송되어온 인증 정보를 Single-domain으로부터 사용한다.

$$other\ single-domain \rightarrow HRA : \left[ID_{D'}, E_{PK_{HRA}}[ID_D, HRAC]\right]$$

Step 5. HRA는 다른 single-domain에서 받은 정보와 single-domain이 받은 정보를 비교한 후, 동일한 정보이면 홈디바이스 인증을 승인한다.

$$HRA : D_{SK_{HRA}}\left[E_{PK_{HRA}}[ID_D, HRAC]\right] = ID_D', HRAC'$$

$ID_D^I, HRAC' ?= ID_D, HRAC$

Step 6. HRA는 홈디바이스가 인증되었음을 확인한다.

$HRA \rightarrow Device : [ID_D, Auth_D]$

Step 7. 홈디바이스가 제시한 값을 비교한 후, 그 디바이스는 다른 single-domain의 사용을 허가받는다.

2) 멀티도메인 상에서의 인증

단일도메인에 있는 홈디바이스가 멀티도메인으로 이동하여 사용자 정보를 이용하고자 할 때, 홈디바이스는 사용자의 정보를 다음과 같이 사용한다.

Step 1. 단일도메인의 HRA로 이동신호를 전송한다. 만약 HRA가 홈디바이스로부터 이동신호를 받으면, HRA는 그 디바이스를 space list에서 삭제한다.

$Home\ device \rightarrow HRA : signal(Outgoing)$

$HRA : HD_{List}[Delete(ID_D)]$

Step 2. HRA는 홈디바이스가 단일도메인에서 나갔음을 CA에게 알린다. 만약 홈디바이스가 다른 CA로 옮겨갔다면 이 사실을 RCA(Root CA)에게도 알린다.

$HRA \rightarrow CA : [ID_D, ID_{HRA}]$

$CA \rightarrow RCA : [ID_D, ID_{HRA}, ID_{CA}]$

Step 3. 홈디바이스가 멀티도메인에 위치했음을 알린후, 홈디바이스는 멀티도메인내의 다른 HRA 에게 인증을 요청한다.

$Home\ device \rightarrow HRA : Signal(Ongoing)$

$Home\ device : E_{SK_{HRA}}[HRAC]$

$Home\ device \rightarrow HRAC : E_{SK_{HRA}}[HRAC]$

Step 4. 인증요청을 받은 HRA는 HRAC로부터 인증정보를 확인한다.

$HRA : D_{PK_{HRA}}\left[E_{SK_{HRA}}[HRAC]\right] = HRAC$

Step 5. HRA 인증정보가 통과되었다면, HRA는 CA로 인증정보를 전송한다.

$HRA \rightarrow CA : (ID_{HRA}, E_{SK_{HRA}}[HRAC])$

Step 6. CA는 멀티도메인 사용자가 생성한 인증정보를 확인한다. 확인 완료후, CA는 홈디바이스에대한 인증을 승인한다.

$CA : D_{PK_{HRA}}\left[E_{SK_{HRA}}[HRAC]\right] ?= HRAC'$

Step 7. 멀티도메인에서, HRA는 홈디바이스가 가져온 인증정보를 받아들이고, 멀티도메인에있는 어플리케이션으로의 접근 허락한다.

V. 결 론

본 논문에서는 홈네트워크의 안전성 및 사용자 편의성을 위해서 홈디바이스 인증의 필요성을 기술하였고, 홈디바이스 인증에 PKI를 사용할 것을 제안하였다. 또한 홈디바이스를 등록하고, 인증서를 발급하는 과정에 관하여 기술하였고, X.509 기반의 홈디바이스 인증서 프로파일을 기술하였다. 또한 사용자가 사용자 주변의 디바이스를 연결하고 사용자에게서 인가된 디바이스는 어느 곳에서도 이용이 가능하여야 하고, 하나의 디바이스가 사용자를 벗어나 다른 사용자의 공간으로 이동되었을 경우, 이동된 공간에서의 사용자 인증이 원활히 수행되어야 한다. 이를 고려한 디바이스 인증 방법을 본 논문에서 제시하였다.

참고문헌

[1] Gehrmann, C., Nyberg, K., and Mitchell, C.J., "The personal CA-PKI for a personal area network,"IST Mobile and Wireless Telecommunications Summit 2002, pp.31-5.

[2] "Intermediatespecification of PKI for heterogeneous roaming and distributed terminals,"IST-2000-25350-SHAMAN, March, 2003.

[3] R. Housley, W. Polk, W. Ford, D. Solo, " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile," RFC 3280, April, 2002.

[4] "Planning for PKI : Best Practices Guide for Developing Public Key Infrastructure," John Wiley & Sons, Inc. 2001.

[5] 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, Aug., 2006.

[6]Deok Gyu Lee, Seo-Il Kang, Dae-Hee Seo, Im-Yeong Lee, "Authentication for Single/Multi Domain in Ubiquitous Computing Using Attribute Certification," International Conference Computational Science and Its Applications (ICCSA 2006), pp. 326-335, 2006. 5 (LNCS 3983)

[7]Yun-kyung Lee, Deok-Gyu Lee, Jong-wook Han, Kyo-il Chung, "Home Network Device Authentication: Device Authentication Framework and Device Certificate Profile", The international workshop on Application and Security Service in Web and pervAsive eNvironments (ASWAN 07), 2007