홈 네트워크 구축을 위한 보안 프로토콜 설계

이영구*, 이창보*, 이광형**, 전문석*
*숭실대학교 대학원 컴퓨터 학과
**서일대학 인터넷정보과
e-mail: {ad3927, onsmile79}@ssu.ac.kr,
dreamace@seoil.ac.kr,
mjun@computing.ssu.ac.kr

Design of Security Protocol for Home-Network

Young-Gu Lee*, Chang-Bo Lee*, Kwang-Hyoung Lee**,
Moon-seog Jun*
*Dept of Computer Science, Soong-sil University
**Dept of Internet Information, Seoil College.

요 약

본 논문에서는 외부 클라이언트가 PDA와 같은 단말기로 홈 네트워크를 컨트롤 하기위하여 홈 네트워크의 보안요소 중 사용자 인증과 접근제어에 관하여 연구 하였으며 사용자 인증의 인증서는 X.509 v3의 인증서를 기반으로 사용하고 X.509 v3의 확장영역에 사용자의 그룹을 나누어 디바이스를 제어하고 접근이 제한된 디바이스는 ACL(Access Control List)을 추가하여 접근제어를 하는 방법으로 접근이 제한된 사용자와 이를 관리하는 관리자로 나누어 각 디바이스에 대한 접근제안과 외부 공격으로 부터의 안전하게 보호 할 수 있다.

1. 서론

홈 네트워크 환경은 댁내의 가전 기기들을 원격 접속 및 원격 제어가 가능하도록 연결한 네트워크 환경이다. 외부에서 접속하는 이동 디바이스는 홈 네트워크 환경에서 원격 상호작용과 네트워크 부하를 줄일 수 있는 것으로 기대되고 있다. 이동 디바이스의 서비스가 홈 네트워크에서 실현되기 위해서는 이동 디바 이스 인증 기술이 필요하다.

홈 네트워크 기술은 유선방식의 홈 네트워크 기술과 무선 방식의 홈 네트워크 기술로 나눌 수 있다. 현재 다양한 홈 네트워크 기술이 존재하는 데 각 기술마다 장단점을 가지고 있어 각 기술 영역에 따라 독립적으로 발전되고 있다. 따라서 서로 다른 네트워크 기술을 사용하는 디바이스들 간의 통신이 불가능하다. 즉, 홈 네트워크 환경에서 서로 다른 네트워크에 접속된 디지털기기 간에도 상호 통신이 보장되어야 한다. 그리고 현제 홈 네트워크에 접속하는 방법도 여러 가지 방법을 이용하여 접속하고 있다. 기존의 방법에는 아이디와 페스워드를 이용하여 접속하는 방법과 인증서를 이용하는 방법, 바이오 생체를 이용하는 방법 등 각 기술마다 다양한 방법으로 홈 네트워크에 접근하고 있다. 이러한 다양한 접근 방법 또한 서로 상호 호환성이 있어야 하며, 서로 상호 인증이 되어야 한다.

본 논문에서는 외부 클라이언트가 PDA와 같은 단말기로 홈 네트워크를 컨트롤 하기위한 사용자 인증 방법과 각 사용자마다 그룹을 나누어 디바이스를 제어하고 접근을 제한하는 방법을 제안한다.

* 본 연구는 서울시 산학연 협력사업으로 구축된 서울 미래형 콘텐츠 컨버전스 클러스터 지원으로 수행되었습니다.

2. 관련 연구

2.1 홈 네트워크의 구성

홈 네트워크는 (그림 1)과 같이 가정 내의 네트

워크, 외부의 네트워크, 콘텐츠 및 솔루션으로 크게 나눌 수 있다. 외부의 네트워크에서 홈 게이트웨이를 통해 가정 내의 네트워크에 접근할 수 있으며, 가정 내의 네트워크는 유선과 무선으로 나누어 가정 내의 컴퓨터, 통신기기, 각종 가전기기들 간에 통신이 가능하도록 구축된 네트워크를 홈 네트워크라고 말한다.

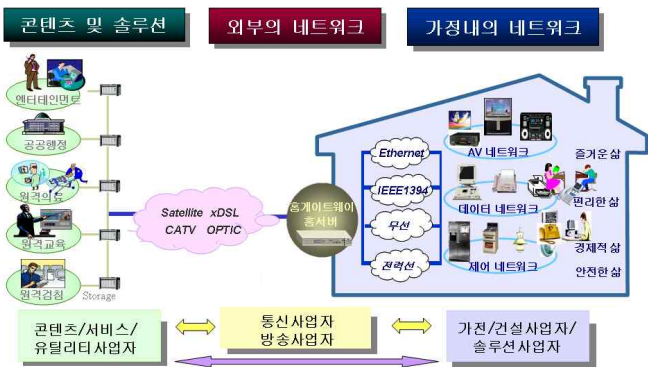

그림 1. 홈 네트워크의 구성

2.2 홈 네트워크 미들웨어

홈 네트워크 미들웨어는 다양한 플랫폼 상에서 동작하는 홈 네트워크 기기들 간에 상호 인증 및 통신을 하고 홈 네트워크 환경에 필요한 서비스들을 제공한다. 홈 네트워크 미들웨어는 보안을 유지하고 사생활을 보호하기 위해서 보안 서비스를 제공한다. 보안 서비스를 제공하는 홈 네트워크의 미들웨어로는 UPnP, Jini, HAVi등이 있다. UPnP는 마이크로소프트에 의해 제안된 홈과 오피스 네트워크를 위한 미들웨어이다. 하지만 IP기반의 네트워크만을 지원하고 있으며 디바이스 자체의 높은 컴퓨팅 파워를 요구한다. Jini의 경우는 홈과 사무실 네트워크를 위해 제안된 미들웨어로서 디바이스를 네트워크에서 찾는 look-up, discovery 서비스를 가지고 있다. 그리고, HAVi는 IEEE1394를 기반으로 하여 A/V 서비스를 제공하기 위해 제안된 미들웨어이다. 하지만 디바이스의 위치에 따른 그룹 제어나 다른 프로토콜들 사이의 상호 운영을 지원하는 것은 고려하지 않았다.

2.3 홈 네트워크 보안기술

홈 네트워크에서는 유무선 네트워크와 다양한 프로토콜 등으로 기존의 인터넷 등에서 발생되던 보안취약성 외에도 추가적으로 고려해야할 보안 취약성이 많이 존재한다.

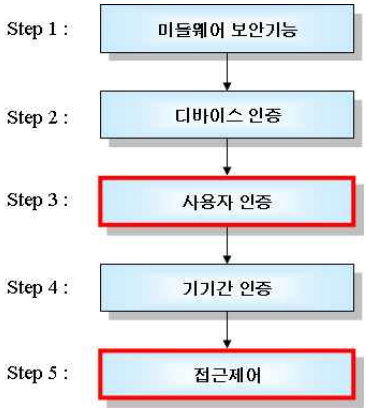

그림 2. 보안 프레임워크

홈 네트워크의 다양한 디바이스들은 인터넷과 서로 연결되어 공격의 대상이 될 수 있으며, 더욱이 홈 네트워크에서 디바이스의 다양성과 기기간 자원의 공유 등으로 보안측면에서 고려해야할 보안요구사항이 더욱 복잡해지고 있다. 홈 네트워크에서 보안해야할 사항에 대하여 (그림 2)와 같이 5가지로 나누어 볼 수 있다.

2.3.1 미들웨어 보안기능

표 1. 미들웨어별 보안기능

미들웨어	제공하는 보안기능
UPnP	Ver 2.0에서 보안기능이 추가될 예정 - 제품 인증기능 제공 - 기기간 인증기능 제공 - 기밀성 제공
Jini	Ver 1.0에서는 Java Security에 의존 - 사용자 인증기능 제공 - 기기간 인증기능 제공 - 메시지 무결성 및 기밀성 제공 - 접근제어기능 제공
HAVi	- HAVi인증서를 이용한 인증기능 제공 - 접근제어 기능 제공

(표 1)과 같이 홈 게이트웨이와 각 디바이스의 제어를 위해 필요한 미들웨어들에도 기본적인 보안기능이 제공되고 있으며, 관련 보안기능에 대한 표준화도 이루어지고 있다.

2.3.2 디바이스 인증

불법 디바이스의 사용을 방지하기 위해서는 홈 네트워크의 구성요소인 디바이스에 대한 인증과정이

필요하다. 현재까지 디바이스의 인증은 미들웨어 레벨에서 제공되고 있다. UPnP의 경우, 디바이스마다 부여된 Security ID로 디바이스의 홈 네트워크 등록 과정에서 디바이스 인증이 이루어지고 있으며, HAVi의 경우 (그림 3)과 같이 디바이스마다 고유한 인증서를 발행하여 디바이스를 인증하고 있다.
디바이스 유효성 확인을 위하여 시리얼 넘버나 인증서 등은 제조업체 등에서 자체적으로 발행하고 있으며 디바이스 인증에 대하여 표준화 연구가 필요하다.

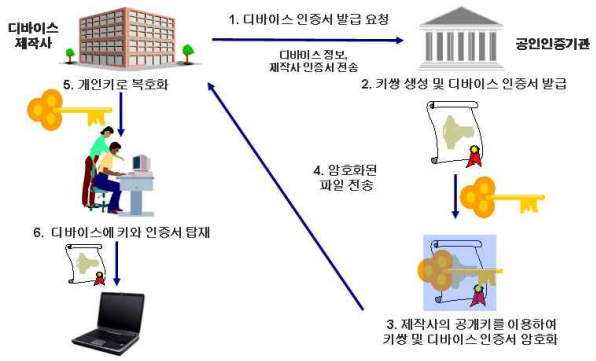

그림 3. HAVi의 디바이스 인증 과정

2.3.3 사용자 인증

홈 네트워크에서는 각 디바이스를 사용하는 사람의 신원확인을 위한 사용자 인증과정이 필요하다. 홈 네트워크에서는 생체인식, 패스워드, 인증서, 스마트카드, RFID 등 다양한 사용자 인증기술의 활용이 가능하다. 사용자 인증기술은 댁내뿐 아니라 댁외에서도 홈 네트워크에 대한 원격 접근을 위해 필요하며, 댁내에서 인터넷 뱅킹과 같은 서비스 사업자가 제공하는 서비스를 사용하기 위해서 사용자 인증 기술이 필요하다. 그르므로, 기존의 다양한 사용자 인증기술을 수용할 수 있는 종합적인 사용자 인증 기술이 개발되어야 한다.

2.3.4 기기간 인증

원활한 홈 네트워크의 서비스 제공을 위해서 기본적으로 홈 네트워크 구성요소간의 자원공유를 위한 신뢰가 확보되어야 한다. 이를 위해서 기기간의 상호인증이 필요하다. 현재 기기간의 인증은 미들웨어 레벨에서 제공하는 보안기능에 의존해 왔다. 하지만, 모든 미들웨어가 보안기능을 제공하지 않으므로 이에 대한 해결방안이 있어야 하며, 기기간 인증은 다양한 홈서비스를 위한 기본적인 보안기능이라고 할 수 있으므로 다양한 홈서비스 제공을 위해서는 기기간의 인증 기술이 개발되어야 한다.

2.3.5 접근제어

홈 네트워크의 각 디바이스에 대한 접근제어 기능이 요구된다. 홈 구성원별로 제공받을 수 있는 서비스의 종류가 다르고 홈 네트워크 구성요소에 대한 제어 범위도 다르므로 이에 대한 접근 제어기능이 필요하다. 또한 인증 정보 유출로 인한 불법적인 접근이 발생할 경우에 이른 능동적으로 대체할 수 있는 보안기능에 대한 연구가 필요하다.

3. 제안한 시스템의 프레임워크

그림 4. 제안하는 시스템의 전체구조

제안하는 시스템의 전체구조는 (그림 4)와 같이 PDA 등과 같은 외부 클라이언트 즉, 댁외 사용자가 인터넷을 통하여 홈 네트워크에 접근할 때 사용자의 인증과 SSL 채널을 통하여 홈 네트워크에 접근할 때 홈 게이트웨이에서 디바이스에 대한 접근제어 한다.

3.1 사용자 인증 과정

사용자인증 과정은 우선 사용자가 홈 네트워크 안에서 인증서버에 직접 USB 케이블을 통해서 인증서를 발급 받는다. 발급 시 인증 서버는 기기에 대한 디바이스 ID와 Key를 생성하여 서버와 클라이언트 모두 저장을 시킨 후에 인증서를 발급하여 준다. 클라이언트는 발급받은 인증서를 가지고 사용자가 외부에서 인터넷을 통하여 홈 네트워크에 접속을 요청한다.

① 클라이언트는 Query와 디바이스 ID를 전송을 한다.
② 홈 게이트웨이는 난수값 (r)을 생하여 클라이언트 디바이스의 키로 난수값 (r)을 대칭키 암호화 방법으로 암호화하여 보낸다.
③ 클라이언트는 자신이 가지고 있는 키로 복호화하여 난수값 (r)을 얻어낸다.

④ 클라이언트는 난수값 (r)으로 자신의 인증서를 암호화하여 다시 서버로 보내게 된다.

⑤ 올바른 인증서이면 홈 네트워크에 접속해 디바이스를 제어할 수 있다.

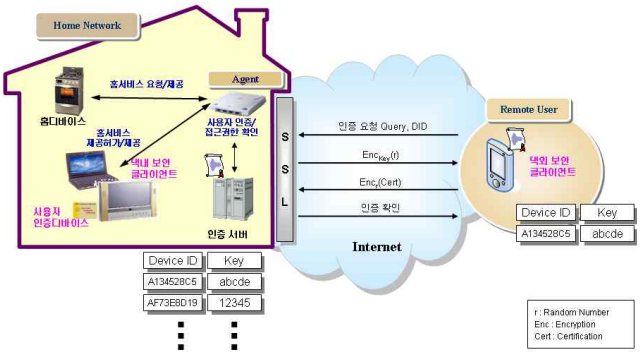

그림 5. 사용자 인증 과정

사용자 인증과정에서 사용되는 인증서에는 기본적으로 사용자 권한에 맞는 기기들을 (그림 6)과 같이 ACL(Access Control List) 그룹으로 묶어 놓고, 각 그룹을 토대로 제어가 가능하도록 하였으며, 또한 해당 그룹에서 제어가 불가능한 기기를 다루기 위해서 AccessList 엘리먼트를 추가 시켰으며, 기본 그룹에서 제어를 막아두기 위해 DenialList 엘리먼트를 추가하여 각 디바이스에 접근에 대한 제어를 하였다.

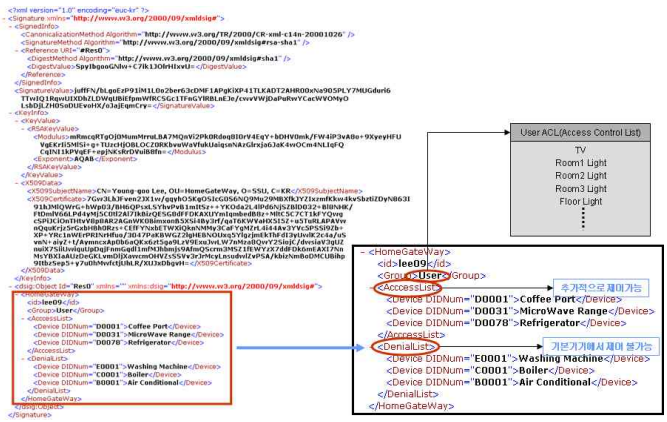

그림 6. 사용자 인증서

3.1.2 디바이스 접근제어

사용자 인증과정이 이루어지면 (그림 7)과 같이 홈 게이트웨이를 통하여 각 디바이스를 접근이 이루어진다.

① 외부 클라이언트가 SOAP Message로 랜덤값 (r)과 자신의 키를 연접한 후 해쉬로 암호화하여 보낸다. 이때 SOAP Message에는 X.509 기반의 애트리뷰트인 DIDnum와 DID 그리고 Control Command를 함께 보낸다.

② 홈 게이트웨이(Agent)는 접근이 가능한지 가능하지 않는지 클라이언트에게 통보하여 준다.

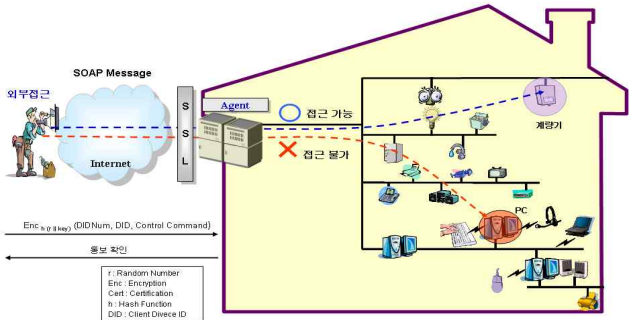

그림 7. 디바이스 접근제어

4. 결론

이 논문에서는 5가지 보안 기능 중 2가지의 보안 기능 사용자 인증과 접근제어에 관하여 연구하였으며 앞으로 미들웨어 보안기능과 디바이스 인증, 기기간의 인증에 대한 연구과 5가지 보안기능에 대하여 표준화 작업이 필요하며 각 보안 기능에 대하여 상호인증이 필요하다. 홈 네트워크 환경에서의 서비스 모델 및 내용이 점차 구체화되어질 경우 보안 인증에 대한 적절한 기술 사항이 보다 구체적이고 안정적인 보안 기술이 연구 되어야 한다. 홈서비스를 활성화하기 위해서 안전성 강화도 중요하지만 우선적으로 사용자의 편리성을 최우선 적으로 고려하여야 한다.

참고문헌

[1] Sungwoo Tak, etc, "An end-to-end home network security framework", Elsevier, pp.412-422

[2] E. Callaway, L. Hester, P. Gorday, "Home networking with IEEE 802.15.4: a developing standard for low-rate wireless personal area networks", IEEE Communications Magazine, VOL. 40 NO. 08 pp. 0070 ~ 0077 2002. 08

[3] Haowen Chan, Perrig A, "Security and privacy in sensor networks", IEEE Computer, VOL. 36 NO. 10 pp. 0103 ~ 0105 2002 . 10

[4] 한종욱, "홈 네트워크 보안 프레임워크 구축을 위한 고려사항", 정보과학회지 22권 9호 통권 제 184호 pp.17-23

[5] 정재학, "홈 네트워크에서의 보안 요구사항 분석", 한국정보보호학회지 제 14권 5호 pp.19-22, 2004