안전한 홈 네트워크 구축을 위한 인증 프로토콜에 관한 연구

이영구*, 김정재*, 전문석*
*숭실대학교 대학원 컴퓨터 학과
e-mail: {ad3927, argniss}@ssu.ac.kr
mjun@computing.ssu.ac.kr

A Study on Authentication Protocol for Secure Home Network System

Young-Gu Lee*, Jung-Jae Kim*, Moon-seog Jun*
*Dept of Computer Science, Soong-sil University

요 약

본 논문에서는 외부 클라이언트가 홈 네트워크 시스템을 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 보호할 수 있게 제안한 논문이다.

1. 서론

정보통신 기술의 발전으로 인간은 다양하고 편리한 서비스에 대한 관심이 높아지고 있다. 최근 컴퓨터 및 정보통신 기술의 발달과 함께 급속히 발전하는 인터넷 기술은 데이터 서비스는 물론 인터넷 폰, 전자신문, 주문형 비디오, IPTV 등 다양한 멀티미디어 서비스를 가능하게 하였으며, 이러한 인터넷의 발전은 가정 내의 정보화도 가속시키고 있다.

홈 네트워크를 구성하는 HDTV, 디지털캠코더, Home theater, 인터넷 냉장고 등의 디지털 가전기기들의 보급이 활성화 되면서 가정은 단순한 가정에서 하나의 네트워크를 구성하는 가정으로 바뀌게 되었다. 홈 네트워크를 구성하는 기술에는 다양한 응용기술들이 있으며 새로운 선로 없이 여러 신호들을 전송할 수 있는 무선 기술이 핵심으로 응용되고 있다. 과거 '홈오토메이션 시스템'에서 본격적인 '홈네트워킹 시스템'으로 전환이 시작되었고, 최근에 IT의 화두로 떠오르고 있는 홈 네트워크 시스템은 새로운 기술 발전이었으며 거기에 따른 인간의 편리한 생활을 만들어 줄 것이다.

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

2. 관련 연구

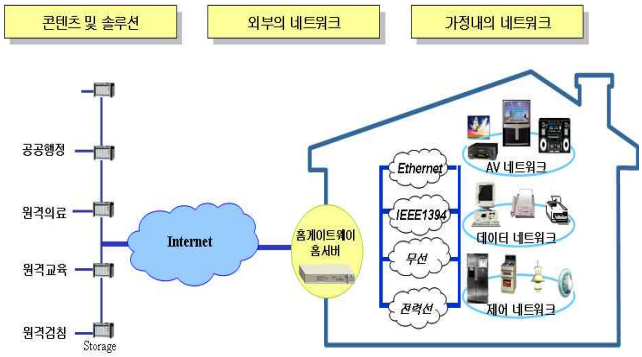
2.1 홈 네트워크의 구성

홈 네트워크 시스템의 구성도는 (그림 1)에서 보여주고 있으며 이러한 홈 네트워크 시스템은 크게 외부네트워크, 홈 게이트웨이, 내부 네트워크, 홈 미들웨어, 각종 디지털 정보 가전기기 그리고 다양한 응용서비스로 구성된다.

홈 네트워크 환경에서의 각종 디바이스들은 인터넷과 직접적으로 연결되어 있어 언제라도 외부 위협요소로부터 공격에 대상이 될 수 있으며, 디바이스의 다양성과 홈 디바이스의 자원 공유 등으로 인해

본 연구는 서울시 산학연협력사업으로 구축된 서울 미래형콘텐츠컨버전스 클러스터 지원으로 수행되었습니다.

고려해야 할 보안요구 사항은 더욱더 복잡해지고 있다.

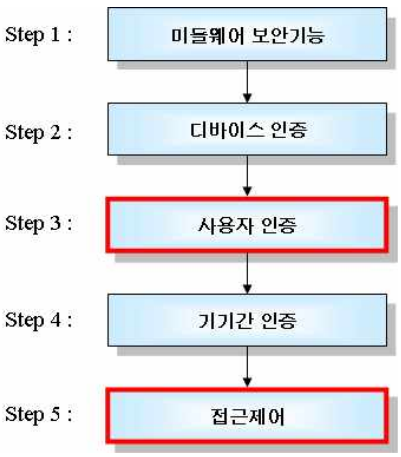


(그림 1) 홈 네트워크 시스템 구성도

2.2 사용자 인증

홈 네트워크에서는 각 디바이스를 사용하는 사람의 신원확인을 위한 사용자 인증과정이 필요하다. 이를 위해 생체인식, 패스워드, 인증서, 스마트카드, RFID 등의 다양한 사용자 인증기술의 활용이 가능하며 사용자 인증기술은 외부에서 홈 네트워크에 대한 원격 접근과 댁내에서 인터넷 뱅킹과 같은 서비스 사업자가 제공하는 서비스를 이용하고자 할 때 해당 사용자가 정당한 사용자임을 증명하는 하기 위한 수단으로 사용된다.

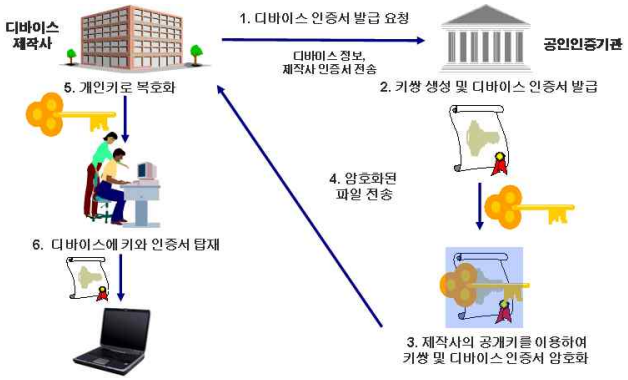
(그림 2)는 홈 네트워크 시스템에서 보안 프레임워크를 보여주고 있다.



(그림 2) 보안 프레임워크

2.3 디바이스 인증

댁내 디바이스에 불법적인 사용을 방지하기 위해서는 홈 네트워크를 구성하고 있는 디바이스에 대한 인증이 선행되어야 한다. 현재 디바이스 인증은 미들웨어 레벨에서 제공되고 있으며 UPnP의 경우, 디바이스마다 부여된 Security ID를 이용하여 디바이스 등록시점에 인증이 이루어지며 HAVi의 경우는 (그림 3)과 같이 디바이스마다 고유한 인증서를 발행하여 디바이스를 인증한다.



(그림 3) HAVi의 디바이스 인증 과정

2.4 홈 게이드웨이 보안

홈 게이트웨이와 서로 상이한 플랫폼을 가진 각각의 디바이스를 제어하기 위해서는 이들을 하나로 제어하고 관리할 수 미들웨어가 필요하다. 이러한 미들웨어 자체에서도 기본적인 보안 기능이 제공되고 있으며, 현재 미들웨어에서의 보안 요소를 표준으로 제정하여 사용하기 위한 연구가 계속적으로 진행되고 있다. [표 1]은 홈 네트워크에 사용되는 미들웨어에 따른 보안 기술들을 보여주고 있다.

(표 1) 홈 게이트웨이 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

2.5 기기간 인증

원활한 홈서비스 제공을 위해서는 기본적으로 홈 네트워크 구성 요소간의 자원공유를 위한 기기간 상

호인증 과정이 이루어져야 한다. 현재 기기간의 상호 인증은 미들웨어 레벨에서 제공하는 보안기능에 의존하고 있다. 하지만 미들웨어 레벨에서의 홈 디바이스의 인증은 가장 기본적인 부분에서의 보안 기능만을 제공하기 때문에 다양한 홈 네트워크 환경에 적용하기 위한 기기간의 인증이 필요하다.

2.6 접근 제어

사용자에 따라 제공받을 수 있는 홈서비스의 종류가 다르고 홈 네트워크 구성요소에 대한 제어 범위도 다르므로 각 사용자에게 부여된 권한에 맞는 기능만을 사용할 수 있게 하는 접근 제어 기술이 요구된다. 현재의 홈 네트워크 시스템의 구조를 고려할 때 접근제어를 위한 접근제어 목록은 각 단말기에 내장하고 있는 것이 효율적이다. 하지만 안정성 측면이나 사용자 측면과 같은 여러 요소들에 대해 일관된 보안정책을 적용해야 한다는 점에서 홈 게이트웨이에서 종합적으로 관리하는 것이 좀 더 효율적이다.

3. 제안한 시스템의 프레임워크

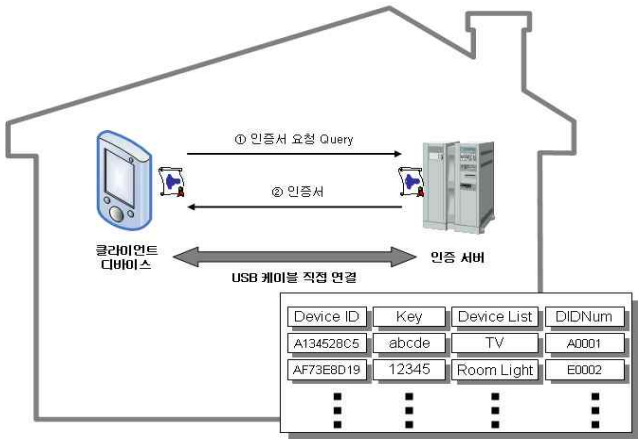
제안하는 시스템의 전체구조는 (그림 4)와 같이 PDA 등과 같은 외부 클라이언트 즉, 댁외 사용자가 인터넷을 통하여 홈 네트워크에 접근할 때 사용자의 인증과 SSL 채널을 통하여 홈 네트워크에 접근할 때 홈 게이트웨이에서 디바이스에 대한 접근제어 한다.

(그림 4) 제안하는 시스템의 전체구조

3.1 인증서 발급 과정

홈 서버에서는 각 사용자의 디바이스에 대한 디바이스 ID와 Key를 생성하여 저장하고 있으며, 사용자 디바이스가 추가/삭제되면 사용자 디바이스는 홈 서버에서 디바이스를 등록하고 디바이스 ID와 Key를 재발급 받는다.

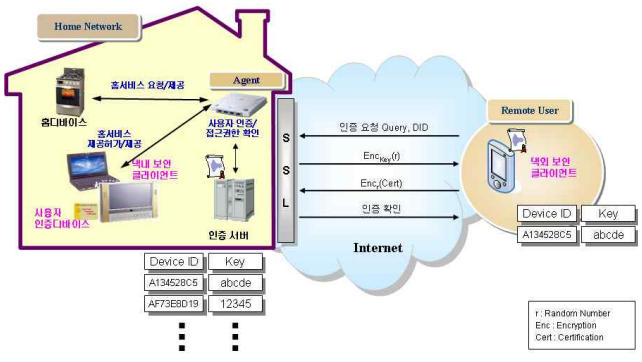
인증서는 사용자가 클라이언트 디바이스를 가지고 홈 네트워크 안에 있는 인증서버에서 직접 USB 케이블을 연결하여 발급 받는다. 발급시 인증서버는 클라이언트 디바이스에 대한 디바이스 ID와 Key를 생성하여 홈 서버에 저장하고 인증서를 발급한다. (그림 5)는 사용자 인증서 발급 과정을 보여주고 있다.



(그림5) 사용자 인증서 발급과정

3.2 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.



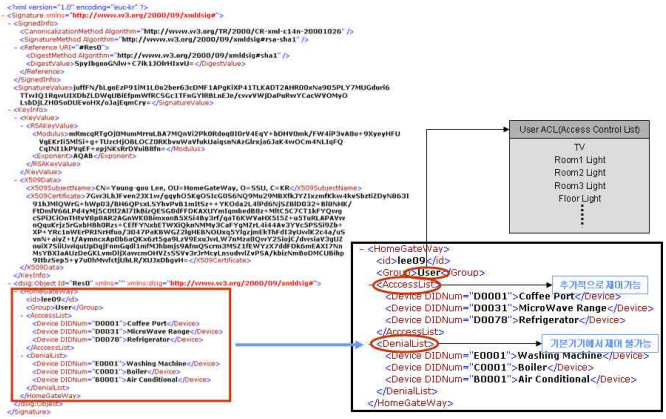
(그림 6) 사용자 인증 과정

① 클라이언트는 Query와 디바이스 ID를 전송을 한다.

② 홈 게이트웨이는 난수값 (r)을 생하여 클라이언트 디바이스의 키로 난수값 (r)을 대칭키 암호화 방

법으로 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.

사용자 인증과정에서 사용되는 인증서에는 기본적으로 사용자 권한에 맞는 기기들을 (그림 7)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.

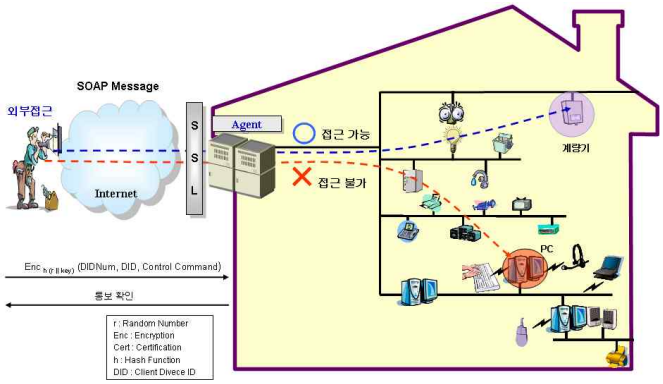


(그림 7) 사용자 인증서

3.3 디바이스 접근제어

사용자 인증과정이 이루어지면 (그림 8)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 8) 디바이스 접근제어

4. 결론

본 논문에서는 사용자가 자신의 클라이언트 디바이스의 인증서를 오프라인에서 홈 서버로부터 직접 발급받아 사용자 인증과 디바이스 접근제어를 수행한다. 또한 사용자 인증 데이터 정보는 항상 암호화 되어 전송되므로 불법적인 장치가 클라이언트의 개인키와 난수 r을 모르면 데이터의 정보가 노출될 위험이 없으며 홈 디바이스 제어정보는 해쉬 한 값을 다시 암호화 하여 전송하기 때문에, 중간에서 메시지를 가로채더라도 메시지의 내용을 유추하는 것은 불가능 하다는 장점이 있다.

참고문헌

[1] P. Thubert, R. Wakikawa, V. Devarapalli, "MEMO Home Network midels", IETF Draft, 2005.
[2] H. Jo, H. Youn, "A Secure User Authentication Protocol Based on One-Time-Password for Home Network", ICCSA 2005, Vol 3480, p.519, May 2005.
[3] Carl M.Ellison, "Interoperable Home Infrastructure Home Network Security", Intel Technology Tournal, Vol 6. pp.37-48, 2002.
[4] 박동준, "홈 네트워크 보안에 관한 연구", 건국대학교, 2005.
[5] TTAS.KO-12.0030, "홈 서버 중심의 홈 네트워크 사용자 인증 메커니즘", 한국정보통신기술협회, 2005.
[6] 정재학, "홈 네트워크에서의 보안 요구사항 분석", 한국정보보호학회지 제 14권 5호 pp.19-22, 2004