情 報 保 護 學 會 誌
第 15 卷 第 6 號, 2005. 12

홈 네트워크 환경에 적합한 디바이스 인증 프로토콜 요구사항

이 정 환*, 황 유 동**, 박 동 규***, 한 종 욱****

요 약

미래의 홈 네트워크 환경에서는 다양한 홈 디바이스들이 인터넷을 통하여 외부와 직접 또는 간접적으로 연결이 되기 때문에 기존의 인터넷에 존재하는 보안 위협 이외에도 다양한 보안 위협들이 존재한다. 이러한 홈 네트워크 환경에서 디바이스 사이에 안전한 데이터 통신을 위해서는 보안에 대한 필요성이 절실히 요구되며 그중에서도 디바이스 인증은 매우 중요하다. 따라서 본 논문에서는 홈 네트워크 환경에서 기존에 연구되던 방식들을 분석하고 신뢰할 수 있는 홈서비스를 제공하기 위하여 홈 디바이스 특성을 고려한 새로운 디바이스 인증 프로토콜 요구사항을 정리하고자 한다.

Ⅰ. 서 론

초고속 인터넷의 발달과 정보통신 환경의 발전으로 인하여 장소와 시간에 상관없이 가정 내 홈 디바이스의 제어가 가능해지고, 정부에서 2007년 디지털 라이프를 실현하기 위한 디지털 홈 구축 계획을 발표하면서 홈 네트워크에 대한 관심이 높아지고 있다[1]. 홈 네트워크란, 정보처리가 가능한 디바이스를 통하여 가정의 외부에서도 쉬운 방법으로 가정 내의 디바이스를 제어하고 디바이스 간의 상호 연동을 통하여 방범, 방재, 엔터테인먼트 등 사용자의 기호에 맞는 서비스를 제공하는 미래형 홈서비스를 말한다. 이와 같은 서비스는 홈 네트워크의 특성상 다양한 종류의 디바이스가 통합된 네트워크 환경에서 서비스되기 때문에 기존의 인터넷 환경에서 가지고 있던 보안 위협 이외에도 새로운 형태의 보안 위협들이 존재한다. 이러한 보안 위협은 작게는 서비스의 불편을 초래하지만 크게는 인명피해와 재산의 손실과 같은 큰 피해를 가져온다. 따라서 이러한 위협으로부터 안전한 서비스를 보장하기위한 보안요구는 날로 증대 되어 보안 연구의 중요성을 부각시키고 있으며 그 중에서도 사용자의 개입이 최소화된 디바이스간 상호 연동을 통한 서비스를 제공하기 위해서는 홈 네트워크 구성요소인 디바이스 자체에 대한 인증이 필수적이다.[2] 따라서 본 논문에서는 기존의 디바이스 인증 방식들의 특징을 분석하고 이를 바탕으로 홈 네트워크 환경에 적합한 새로운 디바이스 인증 프로토콜 요구사항을 정리하고자 한다.

본 논문의 구성으로는 Ⅱ장과 Ⅲ장에서 홈 네트워크의 보안 구조와 홈 네트워크 환경에서 디바이스 인증에 대하여 알아보고 Ⅳ장과 Ⅴ장에서 미들웨어에서 디바이스 인증 및 보안기능 디지털 콘텐츠 보호를 위한 디바이스 인증 및 보안 기능을 고찰한다. Ⅵ장에서는 기존의 방식들에 문제점과 새로운 디바이스 인증 방식에 대한 요구사항을 정리하고 Ⅶ장에서 결론을 내린다.

Ⅱ. 홈 네트워크 보안 구조

홈 네트워크의 보안을 위한 보안 구조에 대한 연구가 다양하게 진행되고 있다. 현재 유럽에서는 디지털 TV와 관련된 멀티미디어 서비스를 위하여 MHP(멀티미디어 홈 플랫폼)이 연구되어 왔으며, 이 MHP위

* 순천향대학교 정보통신공학과 석사과정 (ljhwans@sch.ac.kr)
** 순천향대학교 정보보호학과 박사과정 (coppermilk@sch.ac.kr)
*** 순천향대학교 정보기술공학부 교수 (dgpark@sch.ac.kr)
**** 한국전자통신연구원 홈 네트워크 보안연구팀팀장 (hanjw@etri.re.kr)

에 적용이 가능한 보안구조가 연구되어 왔다. MHP의 사용자는 소비자와 내용을 중계하는 중계자와 서비스를 제공하는 서비스 제공자로 나누어 질수 있으며, 소비자를 위하여 개인의 프라이버시 보호를 위한 서비스를 제공하고, 서비스 제공자를 위하여 정보의 기밀성, 무결성 및 부인 봉쇄 서비스를 제공하며, 중계자를 위하여 신뢰할 수 있는 통신 서비스를 제공하고 있다. 그러나 MHP의 보안 모델은 사용자의 데이터 및 전송 프로그램에 대한 보안을 제공하는 것으로 홈 네트워크 내부의 서로 다른 디바이스들의 대한 인증서비스를 제공하지 못하는 단점을 가지고 있다. 또한 일본에서는 NTT에서 홈 네트워크 서비스를 위한 구조를 제안하고 이 구조에 CSC(통신 서비스 관리기)를 도입하여 외부 홈서비스 제공자들에 대한 보안 서비스를 제공하고 있다. 이 구조는 OSGi에 기반을 둔 자바 기반 미들웨어로서 외부와의 허용되지 않은 통신을 방지하기 위하여 SSL 상호 인증 기법을 사용하고, 의심스러운 프로그램 모듈 실행을 방지하기 위하여 디지털 서명기법을 사용하며, 내부 데이터를 보호하기 위하여 상세한 ACL(Access Control List)을 사용하고 있다. 그리고 홈 네트워크내의 다양한 디바이스들을 결합하여 편리하고 복잡한 서비스들을 제공하는 홈서비스 하모니(Home Service Harmony)기법을 제공하고 있다. 그러나 이 구조역시 홈 네트워크의 디바이스들에 대한 인증 기법을 제공하기 못하는 상황이어서 신뢰할 수 있는 서비스를 제공하지 못하는 단점을 가지고 있다[4][5].

Ⅲ. 홈 네트워크 환경에서 디바이스 인증

홈 네트워크 환경에서 디바이스 인증이란 유일한 식별자를 통하여 자신이 어떠한 기능을 가지고 있고 정당한 디바이스라는 것을 입증 하는 것으로서 디바이스 인증서나 유일한 키를 이용한다[3]. 현재까지 디바이스 인증은 미들웨어 레벨에서 제공이 되고 있고 많은 기업들은 서비스 특성에 맞는 컨소시엄을 구축하여 표준화를 추진하고 있고 이를 바탕으로 시장의 선점을 노리고 있다. 대표적인 미들웨어의 종류로는 UPnP, Jini, HAVi, Lonworks 등이 있다. 하지만 이들 방식들은 각 컨소시엄 마다 독립적인 프로토콜을 사용하기 때문에 상호 연동되는 서비스를 제공하기 위해서는 각 디바이스마다 프로토콜 인터프리터를 가지고 있어야 하거나 변환기를 별도로 설치해야 하는 문제점이 있다. 또한 인터프리터를 이용하여 여러 가지 프로토콜을 연동하여 사용한다고 하여도 서로 다른 보안 서비스로 인하여 신뢰받는 보안 서비스를 제공할 수 없다.

Ⅳ. 미들웨어기반 디바이스 인증기술

홈 네트워크상에서 미들웨어란 물리 계층과 상위계층에서 동작하는 응용프로그램 사이에 중간 매체 역할을 하는 API(Application Programming Interface) 관련 표준이다. 이는 가정 내의 가전 기기와 정보기기를 통합 제어할 수 있는 홈 네트워크에 핵심 기술이며, 이 기술은 홈 서버와 홈 네트워크 구성에 따라서 다르게 연구되어지고 있다. 현재 마이크로소프트사 중심의 UPnP(Universal Plug and Play), 썬마이크로시스템사 중심의 Jini, Sony사 중심의 HAVi (Home Audio/Video interoperability), Echelon사의 Lonworks 등이 홈 네트워크 시장에서 선점을 위하여 연구를 진행 시키고 있다.

1. UPnP(Universal Plug and Play)

UPnP는 마이크로소프트사에서 제안한 미들웨어로 디바이스간 P2P(Peer-to-Peer)를 기반으로 하고 있으며, 널리 사용되고 있는 TCP/IP(인터넷 프로토콜)을 이용하여 그 구조를 정의하고 분산되어있는 디바이스간의 편리한 통신을 지원한다. 또한 디바이스간의 보안을 위하여 검증, 무결성, 인증, 갱신, 권한 할당, 비밀성을 포함하고 PKI구조(공개키 기반 구조)의 공개키를 이용하여 메시지를 암호화 전송함으로써 보안 서비스를 제공하고 소유권을 얻은 사용자가 접근제어 정책을 설정할 수 있다.

UPnP의 특징은 다음과 같다.

- 소규모에서 대규모의 네트워크로 확장이 용이하다.
- 동적으로 홈 네트워크에 연결되어 IP를 자동으로 할당한다.
- PnP(Plug and Paly)를 지원하여 장비의 접속과 분리를 자동으로 인지할 수 있고, 시스템 자원의 점유가 적다.
- 특정 OS(Operating System), 프로그램 언어, 미디어 접근 기술, S/W에 독립적이다.
- P2P 네트워킹이 가능하도록 하는 분산 및 개방 네트워크 구조를 가지고 있다.
- IP 기반이지만 Non-IP 디바이스도 SCP(Service Control Protocol)라는 프로토콜을 통하여 브리지(Bridge: 네트워크 프로토콜 변환기)를 사용해서 수용 가능 하다.

UPnP의 단점은 TCP/IP 기반의 프로토콜을 사용하므로 사용 모듈의 크기와 수행에 따라 CPU의 부담이 크기 때문에 고사양의 컴퓨팅 파워를 요구한다.[6]

2. Jini

Jini는 썬 마이크로시스템즈가 네트워크상에서 원격으로 디바이스를 제어할 수 있도록 제안한 소프트웨어로서 JVM(Java Virtual Machine)기반에서 동작하므로 Jini기술이 지원되는 디바이스는 설치와 부팅 없이 장치 스스로 네트워크에 존재를 알리고 자신의 능력 정보를 제공하며 다른 장치들이 접근 할 수 있도록 지원한다. Jini는 객체 중심적인 구조 기반으로 자발적이며 동적인 분산 네트워크 환경을 구축하고, 정보 디바이스나 소프트웨어를 연계하는 서비스 공유를 목적으로 한다.

Jini의 특징으로는 다음과 같다.

- 네트워크상에서 PnP 기능을 제공하며, 소프트웨어나 하드웨어, 연산능력, 스토리지, 사용자 등 모든 요소를 서비스로 처리하는 "서비스 기반구조"를 활용한다.
- JVM을 사용하므로 하드웨어에 독립적이며, 네트워크의 구성이 단순하고 확장성을 제공한다.
- RMI (Remote Method Invocation) 통신 방법을 기반으로 하고 있다.

제공되는 보안 서비스로는 PKI구조의 공개키를 사용하여 서로의 메시지를 주고받아 디바이스를 식별한 후 메시지는 session key를 사용하여 암호화 되므로 다른 악의 있는 제 삼자에 의해서 악용될 위험으로부터 보호한다.

Jini의 단점은 다음과 같다.

- 단독으로 Jini를 사용하기 위해서는 KVM(CLDC를 위한 Java VM)에서 Jini를 지원해야 한다.
- 고성능의 컴퓨팅 파워를 요구하는 디바이스인 경우는 내장 디바이스(Embeded device)에서 사용하는 컴퓨팅 파워로는 사용하기가 힘들다. [7]

3. HAVi(Home Audio/Video interoperability)

HAVi는 UPnP나 Jini와는 달리 가정 내의 문화생활과 오락과 같은 홈 엔터테인먼트(Home Entertainment)를 강조한 미들웨어 이다. 이 미들웨어 기술은 가전제품회사들이 A/V 디바이스나 정보 가전제품과 같은 네트워크를 사용하는 가전제품들이 늘어나면서 여러 회사의 가전제품을 하나의 홈 네트워크 시스템으로 묶어 서비스할 수 있도록 하기 위하여 개발하였다. 이는 UPnP나 Jini와 같이 PC기반의 미들웨어와는 다른 특징을 갖는다.

HAVi의 주요 특징은 다음과 같다.

- **상호운용성** : HAVi를 지원하는 장비의 기능들을 서로 다른 장비에서 제어할 수 있다. 즉, 안방의 TV를 통하여 거실의 VTR을 작동하여 안방 TV화면을 통하여 영화를 감상하는 등의 기능이 안방 TV 조작만으로 가능해 진다.
- **제조사 독립성** : 제조사와 무관하게 HAVi 표준 미들웨어 사용으로 상호운용성을 제공한다. 즉, 소비자는 홈 엔터테인먼트 네트워크를 구축하기 위하여 제조사와 무관하게 제품에 대한 선택 폭을 넓게 가질 수 있다.
- **플러그&플레이** : 제품이 연결되면 자신의 존재와 기능을 자동으로 알려서 네트워크 주소나 장비 드라이버 등의 설치 없이 간편하게 장비를 설치하고 바로 사용할 수 있다.
- **기능 갱신의 용이성** : DCM (Device Control Module) 형태로 개별적인 기능을 처리하는 방식을 지원함으로써 새로운 DCM의 제공을 통해 기능개선이나 추가적인 기능 제공이 가능하다.
- **분산 제어** : 중앙에 서버형태의 기능을 두지 않고 장비간의 직접통신(peer to peer)을 통해 제어하는 분산처리 구조이다.
- **하부 네트워크 모듈이 IEEE 1394로 제한**: IEEE 1394는 A/V정보를 전송하기 위해 제안되었고, 따라서 많은 제품들이 이미 시장에서 유통이 되고 있다.
- **Non-IP기반** : HAVi는 IEEE에서 제공하는 노드 ID를 사용하여 관리하기 때문에 IP를 지원하지 않는다. 광범위한 홈 네트워크 미들웨어로 사용되기 위해서는 UPnP나 Jini와 같은 미들웨어와 혼용되어야 하며, 실제로 HAVi-UPnP 브릿지와 같은 방식으로 미들웨어 간의 호환성을 제공하고 있는 추세이다.

HAVi의 단점으로는 국한 적인 분야에 사용이 되므로 홈 네트워크의 다양한 디바이스에 적용이 불가능하다[8].

4. LonWorks

LonWorks는 전력선을 기반으로 디바이스를 제어하는 미들웨어로써 이미 LonMark, CEBus 등의 관

련 기관을 통하여 1990년대에 표준화가 되었다. 이는 현재 미국의 ANSI 산하 EIA 709.1 표준으로 등록되었고 다양한 제품이 시장에 발표되면서 빌딩 자동화의 산업 표준으로 인정되고 있으며 현재에는 홈 네트워크 환경에 적용 가능한 모델로 발전하고 있다.

LonWorks의 특징은 다음과 같다.

- LonTalk라는 네트워크 프로토콜과 Neuron 칩을 공급함으로써 디바이스 개발자에게 손쉬운 개발환경을 제공한다.
- 윈도우즈 환경 기반의 LNS을 제공하여 강력한 관리 시스템 제공과 자동화 서비스의 생성 및 제어 할 수 있는 환경을 제공한다.
- 99.7%의 높은 신뢰성을 보이며 기존에 선로를 이용한다.
- IP를 지원하므로 인터넷 제어가 가능하고 Lon Works 시스템과의 통합 및 상호 연동이 용이하다.

LonWorks의 단점은 다음과 같다.

- 장비 및 시스템 개발 비용이 높고 설치시 전문가가 필요하다.
- 다른 미들웨어와의 연동이 어렵다는 단점이 있다[9][10].

5. 미들웨어 보안 기능

현재 대부분의 미들웨어는 독자적인 보안 서비스를 제공하고 있기 때문에 서로간의 호환이 어렵다. 다음 표 1은 각 미들웨어에서는 안전하고 신뢰받는 서비스를 위하여 보안 기능들을 나타내고 있다.

(표 1) 미들웨어 보안 기능

	UPnP	Jini	HAVi	Lonworks
PKI	○	○	×	×
인증서	○	×	○	×
디바이스 인증	○	○	○	○
접근제어	○	○	○	×
기밀성	○	○	×	×

V. 디지털 콘텐츠를 위한 디바이스 인증 프로토콜

지금까지 미들웨어에서 제공되는 디바이스 인증에 관하여 살펴보았다. 그 밖에도 홈서비스 중 디지털 콘텐츠를 보호하기 위한 디바이스 인증 방식이 있다. 대표적인 방식으로는 DTCP(Digital Transmission Content Protection), CableLab, IPCable2Home, DMP(Digital Media Project) 등이 있다.

1. DTCP

DTCP는 Copy Protection Technical Working Group 구성원인 Hitachi, Intel, Matsushita, Sony, Toshiba에 의하여 콘텐츠 제작자들에게 간단하고 저렴하게 복사방지를 제공할 수 있기 위하여 만들어진 표준이다. 이 표준은 IEEE-1394와 같은 고성능 데이터 버스에 오디오/비디오 데이터가 전송될 때 Full/Restricted Authentication 두 가지의 인증 레벨을 이용하여 해당 데이터의 불법 복사와 가로채기 및 내용 변경을 막을 수 있는 암호 프로토콜을 정의하고 있다. 이러한 두 가지 인증 레벨에는 Authentication key, Exchange key, Content key가 쓰인다. 그러나 복사 권한 별로 인증서를 처리하기 때문에 이질적인 네트워크를 통하여 연결되며, 다양한 특성과 제약을 가지고 있는 홈 디바이스의 인증에는 사용하기 어려운 한계를 가지고 있다. DTCP에서는 DTLA(Digital Transmission Protection License Authority)에서 인증서를 발급하며, 제작자들이 인증서 유효성을 검증하고 그 결과를 DTLA에 보고하는 식의 인증서 검증 방법을 사용한다. 그러나 DTCP는 복사 방지를 위해 만들어진 표준으로 다양한 특성과 제약을 가지고 있는 홈 디바이스의 인증에 사용하기 어려운 한계를 가지고 있다.[11]

2. CableLab

CableLab에서는 케이블 서비스 디바이스의 인증을 위하여 인증서를 사용한다. 제조업자들이 디바이스 제조시에 디바이스 내에 인증서를 적재하여, 데이터 기밀성과 내용 무결성 및 하드웨어 디바이스 인증 목적으로 인증서를 사용한다. 예를 들어 케이블 서비스 제공자는 케이블 서비스 디바이스 내에 적재된 인증서를 사용하여 서비스를 요청하는 디바이스를 인증함으로써 불법적인 케이블 서비스의 사용을 방지할 수 있다. CableLabs에서는 CableLabs 인증서의 유효성을 확인하기 위하여 PKI를 운영하고 있으며, 제작자들은 웹기반 CRA(인증서 요청 에이전트)를 통하여 디바이스 인증서들을 받고 이 인증서가 디바이스 제작시에 디바이스 내부에 적재된다. CableLab CRA는 제작자들에게 효율적으로 디바이스 인증서를 제공하며, 제작자들은 웹 브라우저와 스마트카드를 사용하여 호스트CA의 웹에 접속하여 디바이스 인증서를 요청할 수 있다. CRA는 제작자 사이트에 어떤 장치도 필

요로 하지 않으며, 오직 다운 받은 파일의 내용을 해독할 수 있는 적은 용량의 클라이언트 소프트웨어만을 사용한다. 따라서 제작자의 요청과 디바이스 인증서의 전달이 즉시 실현될 수 있게 된다. CableLabs에서는 디바이스 인증서로 X.509 인증서 형식을 사용하며, RSA 암호를 사용하여 인증을 수행한다. 따라서 CableLabs의 디바이스 인증 기법은 케이블 디바이스 인증시에는 효율적이지만 계산 능력에 한계가 있으며 다양한 네트워크로 연결되는 홈 디바이스의 인증시에는 적용하기 어려운 한계를 가지고 있다[12].

3. DMP

DMM(Digital Media Manifesto)은 2003년 비영리 목적으로 e-mail, WWW(World Wide Web)를 사용하는 전문가들의 국제적인 그룹에 의해 발족되었다. 이렇게 발족된 DMM은 디지털 미디어 제작의 표준을 정하고 디지털 콘텐츠의 권한을 부여하기 위하여 DMP를 디자인 하였다. 이러한 DMP에서는 IDP (Interoperable DRM Platform)를 이용하여 디지털 콘텐츠를 보호 한다. DMP는 디바이스를 인증하기 위하여 디바이스 식별 서버에서 X.509인증서를 생성하고 반드시 디바이스에 저장하게 된다. 따라서 DMP의 상호 디바이스 인증 기법은 자신의 디바이스 인증서를 다른 디바이스에게 보내어 인증서의 유효성을 검증하여 상대 디바이스의 공개키를 사용하여 암호화한 메시지를 주고받음으로써 상호 디바이스를 인증하게 된다. 그러나 디바이스에서 인증서를 검증해야 하기 때문에 디바이스마다 높은 컴퓨팅 파워를 요구하게 된다[13].

4. IPCable2Home

IPCable2Home의 목적은 집, 케이블 모뎀, IPCablecom의 하부구조를 보완하여 디바이스에 새로운 케이블 기반의 서비스를 가능케 하는 것과 운영자가 구성 가능한 Residential Gateway 중심의 환경을 만드는 것이다. IPCable2Home 장점은 다음과 같다.

- Residential Gateway 디바이스의 원격관리와 설정이 가능하다.
- IP 기반의 홈 디바이스들을 위한 간단한 Residential Gateway 진단이 가능하다.
- IP 기반의 홈 디바이스들과 관계된 어플리케이션들의 탐색이 가능 하다.
- LAN을 이용한 Residential Gateway 관리가 가능 하다.

IPCable2Home의 보안기능에는 홈 게이트웨이 장치 인증 기능, 암호화된 홈 게이트웨이 관리 메시지 기능, 설정 정보 미 소프트웨어 파일에 대한 암호화된 다운로드 기능, HFC 링크 상의 암호화된 QoS 기능, 원격 홈 게이트웨이 방화벽 관리 기능 등이 정의되어 있다. IPCalbe2Home 의 디바이스 인증서와 디바이스 인증 방식 또한 CableLab과 유사한 형태를 갖고 있다. 따라서 인증서의 계산 능력을 위한 고성능의 컴퓨팅 파워를 가진 디바이스를 요구하게 되며 다른 방식을 사용하는 서비스와 상호 연동하기가 어렵다는 단점을 갖는다[14].

5. 디지털 콘텐츠를 위한 다양한 디바이스 인증 프로토콜의 보안 기능

다음 표 2는 디지털 콘텐츠를 위한 디바이스 인증 프로토콜의 보안 기능을 나타낸다.

(표 2) 디지털 콘텐츠를 위한 디바이스 인증 프로토콜의 보안 기능

	DTCP	CableLab	IPCable2Home	DMP
PKI	×	○	○	×
인증서	○	○	○	○
디바이스 인증	○	○	○	○
접근제어	×	×	×	×
기밀성	○	○	○	×

Ⅵ. 홈 네트워크 환경의 새로운 디바이스 인증 프로토콜의 발전방향

1.기존 연구의 문제점

기존의 미들웨어에서 안전한 서비스를 제공하기 위한 디바이스 인증을 사용하는 방식은 비교적 높은 사양의 컴퓨팅 파워를 요구한다. 그리고 독자적인 기술을 이용하여 특정분야에만 국한되어 있기 때문에 미들웨어를 사용하지 않는 디바이스 또는 서로 다른 미들웨어를 사용하는 타사의 홈 네트워크 디바이스 사이에는 적용이 불가능 하다.

그 외의 디지털 콘텐츠를 위한 디바이스 인증 방식에서는 보안성을 높이기 위하여 강력한 암호 알고리즘을 사용하고 서로 다른 프로토콜 사용으로 인하여 디바이스마다 프로토콜 인터프리터를 가지고 있어야 하고 비교적 무거운 인증서를 검증하기위하여 복잡한 연산을 처리할 수 있는 높은 사양의 컴퓨터 파워를 필요로 한다. 따라서 홈 디바이스와 같은 비교적 저사양의

컴퓨팅 파워를 갖는 디바이스에서는 계산에 한계를 가지고 있다. 또한 서로 다른 보안 서비스를 제공하기 때문에 전체 서비스의 보안 수준이 떨어져 안전한 서비스 제공이 불가능해진다. 또한 각 프로토콜에서 요구하는 인증서를 정의하여 사용하거나 기존 X.509 기반에 속성을 새로이 정의하여 사용하기 때문에 통합된 홈 네트워크 환경에 응용은 불가능 하다.

2. 새로운 디바이스 인증 프로토콜개발시의 고려할 요구사항

홈 네트워크 환경은 특성상 다양한 네트워크와 프로토콜을 혼용하여 사용한다. 이러한 특성 때문에 인터넷 등에서 발생되던 보안위협 뿐만 아닌 새로운 보안 위협들이 존재한다. 이러한 문제점을 해결하기 위해서는 다양한 디바이스나 프로토콜의 관계없이 만족할 수 있는 새로운 디바이스 인증 프로토콜이 필요하다. 따라서 새로운 디바이스 인증 프로토콜을 개발하기 위해서는 다음과 같은 요구사항을 반영해야 한다.

1. 모든 디바이스 밴더들이 동의할 수 있어야 한다.
2. 다양한 디바이스의 컴퓨팅 파워를 고려해야 한다.
3. 홈 네트워크 환경의 특성을 반영할 수 있어야 한다.
4. 다양한 IT, CT환경 변화에 쉽게 적응할 수 있어야한다.
5. 디바이스 제작자의 보안 서비스를 위한 추가 사항은 최소화해야 한다.
6. 디바이스 인증을 검증할 수 있는 기반 인프라가 필요하다.
7. 디바이스 인증과 관련된 관계 법령의 수립이 필요하다.
8. 사용자의 프라이버시를 보호하기 위한 디바이스 관련 기관 및 법령 필요하다.
9. 일반적인 디바이스 인증방식 IT389 서비스 상에 필요한 디바이스 인증을 고려하여야 한다.

Ⅷ. 결 론

본 논문에서는 홈 네트워크 환경에 적합한 디바이스 인증 프로토콜 개발을 위하여 다양한 방식의 디바이스 인증 체계를 알아보았다. 홈 네트워크에서 신뢰할 수 있는 홈서비스 제공을 위해서 홈 네트워크 구성요소 간의 자원공유를 위한 신뢰 확보가 필요하며 이를 위하여 홈 네트워크 구성요소간의 디바이스 상호인증이 기본적으로 수행되어야 한다. 또한 홈 네트워크에서 불법 디바이스의 사용을 방지하기 위하여 홈 디바이스 자체의 인증이 필수적으로 수행되어야 한다. 그러나 아직까지 디바이스의 인증에 대한 연구가 미비한 수준이다. 따라서 본 논문에서는 신뢰할 수 있는 홈서비스를 제공하기 위하여 홈 디바이스 특성을 고려한 디바이스 인증 및 디바이스 인증정보에 대한 통일된 발급체계 및 관리체계에 대한 새로운 디바이스 인증 프로토콜 연구 어떻게 진행되어야 하는지 모색해 보았다.

참고문헌

[1] 정보통신부, 차세대 IT 신성장동력 분야별 추진전략 -홈 네트워크편-, 2003

[2] 정보통신부, IT 신성장동력 발전 전략 Broadband IT KOREA 추진전략 공청회 2003

[3] Ralph W. Brown, "Home Network Device Authentication", ITU-T Workshop on Home on Home Networking and Home Services Tokyo, Japan, 17-18 June 2004

[4] Junchun Luo, "Home network application security(MHP)", Residential and Virtual Home Environments - Seminar on Internetworking, Spring 2002

[5] Akihiro Tsutsui, "Management Architecture and Distribution Framework for Home Network Services", NGN Workshop 2005/3

[6] UPnP Forum, http://www.upnp.org.

[7] Jini Overview, http://www.sun.com/jini/faqs/index.html.

[8] HAVi white paper, http://www.havi.org/pdf/white.pdf.

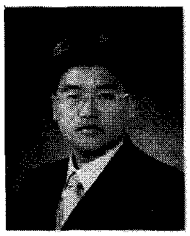
[9] Echelon Co.,"Introduction to the Lonworks System" Version 1.0. http://www.echelon.com

[10] Echelon Co.,"Introduction to the Lonworks System" Version 2.0. http://www.echelon.com

[11] Hitachi, Ltd, Intel Corporation, Matsushita Electric Industrial, Co.,Ltd, Sony Corporation, Toshiba Corporation, "5C Digital Transmission Content Pro-

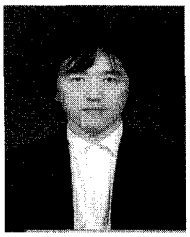
tection White Paper", July 14, 1998
[12] Cable Television Laboratories, Inc, "CableLabs Certificate Issuance Process", 4/13/2004
[13] "INTEROPERABLE DIGITAL RIGHTS MANAGEMENT PLATFORM", http://www.dmpf.org/
[14] AMERICAN NATIONAL STANDARD, ANSI/SCTE 89-1, 2004
[15] AMERICAN NATIONAL STANDARD, ANSI/SCTE 89-2, 2004

〈著者紹介〉



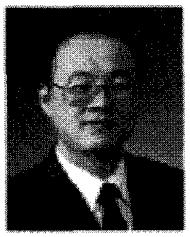
이 정 환 (JungHwan Lee)
정회원

2004년 2월 : 순천향대학교 정보통신공학과 졸업
2004년 3월 ~ 현재 : 순천향대학교 정보통신공학과 석사과정
〈관심분야〉 홈 네트워크, 접근제어, 정보보호



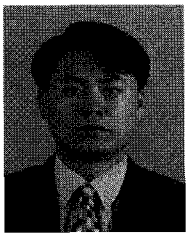
황 유 동 (JungHwan Lee)
정회원

1998년 2월 : 순천향대학교 제어계측공학과 학사 졸업
2000년 2월 : 순천향대학교 정보통신공학과 석사 졸업
2003년 8월 : 순천향대학교 정보보호학과 박사 수료
2005년 1월 ~ 현재 : 순천향대학교 정보통신 프로그램 전공 겸임교수
〈관심분야〉 시스템 보안, 네트워크 보안



박 동 규 (DongGue Park)
정회원

1985년 2월 : 한양대학교 전자공학과 졸업
1988년 2월 : 한양대학교 전자공학과 석사 졸업
1992년 2월 : 한양대학교 전자공학과 박사과정 졸업
1992년 3월 ~ 현재 : 순천향대학교 정보기술공학부 교수
〈관심분야〉 네트워크 보안, 시스템 보안



한 종 욱 (JongYook Han)
정회원

1985년 2월 : 광운대학교 전자공학과 학사 졸업
1991년 광운대학교 전자공학과 공학석사
2001년 광운대학교 전자공학과 공학박사
1991년~현재 한국전자통신연구원 홈네트워크보안연구팀 팀장
〈관심분야〉 홈네트워크보안, 네트워크보안, Optical Security