정보학연구 제8권 제2호 2005년 6월(pp.43-52)
The Journal of Information Technology, Vol.8, No.2

지능형 홈오토메이션 보안설계에 관한 연구

오주영* · 강순덕**

목 차

Ⅰ. 서론

홈 오토메이션기술은 집안의 조명, 냉난방, 방범, 오락 및 통신 기능을 하나의 시스템으로 통합하여 제어함으로서 생활을 편리하게해주는 기술이다.

최근 인터넷의 급속한 발전으로 홈오토메이션에 대한 관심과 수요가 증가하고있다. 또한 휴대폰과 같은 휴대형 단말기기의 보급으로 언제어디서나 홈 네트워크에 접속하여 홈 오토메이션을위한 단말기로도 활용하기도한다. 하지만 이렇게 편리한 홈오토메이션의 현재의 문제점은, 바로 사이버 공격으로 인해 개인의 정보유출, 재산피해 뿐만 아니라 생명까지 위협을 받을 수 있어서 대응책이 시급하다고 할 수 있다.

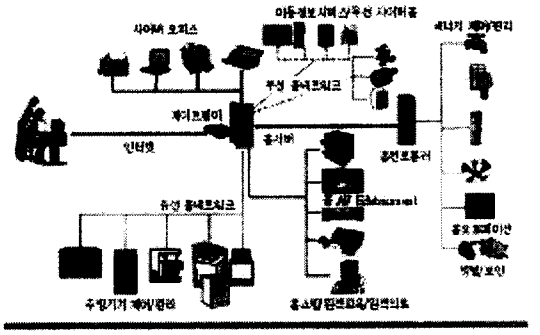
따라서 본 연구에서는 안전한 홈오토메이션 구축을 통한 홈서비스가 활성화 될 수 있도록 홈오토메이션 기술을 분석하고, 보안을 고려한 시스템을 설계를 구현해 지능형 센스 보안까지 사용할 수 있게 했다.

Ⅱ. 본론

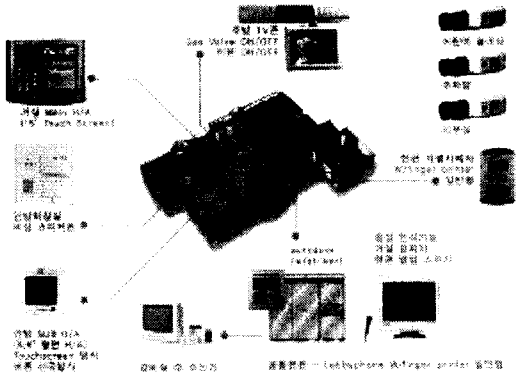
2.1. 홈오토메이션 시스템 설계

홈오토메이션 시스템은 <그림 1>과 같고 최첨단 홈 네트워크 시스템<그림 2>은 기존의 방범/방재, 가정 내 각종 설비의 제어/관리 등 홈오토메이션 기능을 인터넷과 유무선 통신망을 통해 수행하도록 하는 내장형 제어 시스템으로서, 통상 셋톱박스 형태를 사용하며 외부로 이더넷과 내부로 유무선 네트워크에 의한 전기/기계 설비의 인터페이스나 센서/구동기 신호 인터페이스를 가지며 소프트웨어로는 웹 서버에 의한 인터넷과 휴대폰 연결 기능을 제공한다.

* 공주대 컴퓨터공학전공 교수



〈그림 1〉 홈 오토메이션 구성도



〈그림 2〉 최첨단 홈 네트워크 시스템

2.1.1. 네트워킹

가정내에 고정된 기기와의 연계동작에는 CEbus 표준전력선 통신방식을, 이동 단말기와는 Bluetooth나 IEEE802.11b 무선 홈 네트워킹을 지원한다.

2.1.2. 홈 게이트웨이 및 네트워크보안

Firewall, 패킷필더링, NAT(Network Address Translation), 프락시(proxy) 등을 통해외부로부터의 네트워크접근 감시와 내부로부터 유해사이트접근을 차단한다.

2.1.3. 무인경비 기능

가스누출, 화재발생, 외부인 침입등 비상시경보를 발생시키고 이를 관리실이나 세대주에게 신속히 알려 안전사고를 미연에 방지하고 신속히 대처 할 수 있게 한다.[1]

2.1.4. 휴대폰원격제어 및 메시지서비스

휴대폰을 통해 어디서든지 세대내 정보가전기기들의 동작상태를 모니터링 하고 제어할 수 있도록하며, 이상상황 발생시 SMS(Short Message Service)를 통보한다.

이때 보안을 위해 홈 게이트웨이에 방화벽을 설치한다.[10]

2.1.5. 전력선통신을 이용한 홈오토메이션제어

세대내조명제어기, 디지털온도조절기, 자동가스차단기, 백색가전을 CEbus 전력선통신을 통해 모니터링 하고 제어한다.

2.1.6. 7" 컬러 LCD, 터치스크린, 스피커폰을 통한사용자인터페이스

방문자영상/음성확인기능뿐만아니라각종보안장치의설정, 정보가전기기의제어, 전화다이얼링과 통화, 경보발생, 방문자영상기록등에있어서사용자가조작하기편리한환경을제공하도록 한다.

1) 미들웨어

① UPnP

UPnP는 마이크로소프트사가 제안한 미들웨어로서 기존의 IP 네트워크와 HTTP 프로토콜을 사용하여 간단한 방법으로 홈 네트워크 기기의 제어를 구현하자는 목적으로 가지고 있다. HAVi처럼 Java Bytecode를 불러와 실행하는 일이 없으며, DHCP와 SSDP(Simple Service Deiscovery Protocol), GENA(General Event Notification Architecture), 그리고 SOAP(Simple Object Access Protocol) 등을 이용한다. UPnP의 가장 큰 장점은 이미 검증된 웹 기술을 기반으로 홈 네트

워크 기기간의 제어 모델을 구현하였다는 것이다. 따라서 하드웨어, 소프트웨어, 그리고 운영체제에 무관하게 동작이 가능하고, UPnP 포럼에 의해 기기와 서비스 타입이 잘 맞추어져 있다. 그리고 HTML을 이용하여 간단하게 사용자 인터페이스를 제공하고 있다.

② Jini

Jini는 Sun Microsystems사가 창안하여 새로운 제어 모델을 개발하고 이를 홈 네트워크의 대표적인 미들웨어로 발전시킬 목적으로 시작되었다. Jini의 강점은 Plug and Play 기능에 의한 간단한 시스템 구성과 실행 코드의 이동성에 의한 가변성, 그리고 기존의 IP를 기반으로 하는 네트워크에 대한 자연스러운 확장성 및 Java 연관 제품 및 시스템과의 호환성 확보 등이다. 단점으로는 Jini 시스템에 JVM을 도입함으로 인하여 수행 속도가 느리고 많은 양의 메모리를 차지하므로 시스템의 단가가 높아진다. 또한 Lookup Server에의 의존도가 높아 홈 네트워크 시스템에 종종 발생할 수 있는 기기의 착탈 시 Lookup Server가 이탈할 경우 전체 네트워크가 동작을 하지 않을 위험성도 있다.

③ HAVi

HAVi는 IEEE1394 기술을 채택한 오디오 비디오 기기간의 실시간 데이터 전송은 물론 상호 호환성을 위해Sony가 처음 제안한 홈 네트워크용 미들웨어이다. 처음에는 Grundig, Hitachi, MEI, Philips, Sharp, Sony, Thomson, Toshiba 등을 포함하는 8개 회원사로 출발하였으나, 지금은 42개의 회원사를 두고 이 표준에 의해 오디오/비디오 제품을 개발하고 있다.

HAVi는 IEEE1394 기술을 적용한 디지털 네트워크에 사용되는 기술로 Plug and Play를 지원하며, AVC(Audio Visual Control) 커맨드를 사용하지만 미래에 나타날 기기도 자연스럽게 지원해 주기 위해 DCM(Device Control Module)의 개념을 도입하였다. 즉 각각의 기기는 DCM 이라는 모듈로 자신을 표현하고 RMI(Remote Method Invocation)를 이용하여 이 모듈을 전송함으로써 현재의 제어 커맨드가 제공하지 못하는 명령어를 이해하는 구조를 채택하였다. 또한 어느 기기든 다른 제조회사가 만든 어떤 기지든지 모두 통신할 수 있도록 설계되었으며, 자바 바인딩을 통한 개방형 소프트웨어 API를 지원하고, 제어 신호 및 컨텐츠 등을 전송할 수 있다.[2]

④ VHN

VHN(Versatile Home Networking)은 삼성전자에서 자사가 개발하는 TV 및 Set Top Box에 IEEE1394 기술을 적용하면서 이들간의 상호 제어용 소프트웨어로 개발한 IP를 근간으로 하는 홈 네트워크용 미들웨어이다. 삼성의 VHN은 1996년에 이미 시작된 미들웨어 이지만 VESA Home Network Committee가 1999년 8월에 홈 네트워크의 미들웨어 솔루션을 포함하는 VESA Home Network Spec 1.0이 발표되면서 구체화되었다. VHN은 여러 개의 이기종 네트워크의 인터넷인 셈이다. 따라서 홈 네트워크에 접속되어 있는 모든 기기들 사이의 통신을 가능하게 하기 위해서는 어떤 공통된 인터네트워킹 프로토콜이 필요하다. 이 프로토콜들에는 Network Layer 프로토콜은 물론 네트워크 프로토콜을 사용한 통신용 프로토콜과 기기들을 네트워크 자율적으로 배치하는 데에 필요한 다른 프로토콜 등이 이에 속한다.

홈 게이트웨이는 다양한 홈 네트워크 기술과 초고속 액세스 망 기술을 연결시켜 주는 장치로서 국내외적으로 표준화 활동이 시작되고 있는 분야이다. 국제 표준화 활동으로서, 홈 게이트웨

이의 스펙 및 요구 사항 등을 정의하고 ldT는 ISO/IEC JTC1 SC25 WG1, 미국 내의 건물 자동화와 관련되어 효율적으로 멀티미디어 서비스를 분배하기 위한 홈 게이트웨이 표준을 정의하는 TIA/EIA TR-41.5, 서비스 게이트웨이의 API를 정의하고 있는 OSGi(Open Service Gateway initiative), IEEE1394 기술에 근간을 두고 AV 기기, 셋탑 박스 등으로 이루어진 홈 네트워크 기기를 활용하는 VESA(Video Electronic Standard Associatio- n) 등의 표준 단체들이 활동하고 있다.[11]

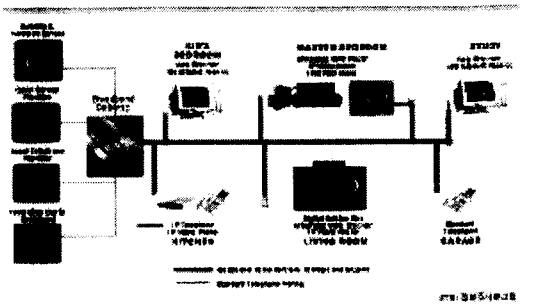
2) 홈 게이트웨이

홈 게이트웨이는 다양한 홈 네트워크 기술과 초고속 액세스 망 기술을 연결시켜 주는 장치로서 국내외적으로 표준화 활동이 시작되고 있는 분야이다. 국제 표준화 활동으로서, 홈 게이트웨이의 스펙 및 요구 사항등을 정의하고 ldT는 ISO/IEC JTC1 SC25 WG1, 미국내의 건물 자동화와 관련되어 효율적으로 멀티미디어 서비스를 분배하기 위한 홈 게이트웨이 표준을 정의하는 TIA/- EIA TR-41.5, 서비스 게이트웨이의 API를 정의하고 있는 OSGi(Open Service Gateway initiative), IEEE1394 기술에 근간을 두고 AV 기기, 셋탑 박스 등으로 이루어진 홈 네트워크 기기를 활용하는VESA(Video Electronic Standard A- ssociation) 등의 표준 단체들이 활동하고 있다.[3]

3) 홈오토메이션 기술

① Phoneline

HomePNA 기술은 전화선로를 이용하는 유선 홈네트워크 기술로서 현재 10Mbps급에서 100M-bps급으로 발전하면서 홈네트워크의 백본 기술로 대두되고 있는 기술이다. HomePNA를 이용한 홈네트워크 구성도는 <그림 3>과 같다.



〈그림 3〉 홈 ePNA를 이용한 홈 네트워크구성

② Powerline

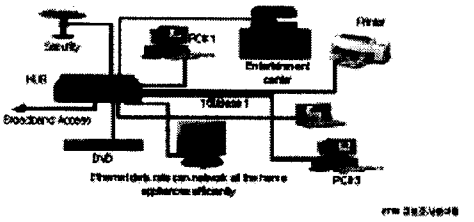
데이터를 전송하기 위해 AC 전력선을 사용한 것은 벌써 20년 가까이 된다. 최초의 홈 네트워크들은 주택 자동화 애플리케이션에 사용되는 저속(60bps) 방식인 X-10 플랫폼을 기초로 형성되었다. 그러나 낮은 속도 때문에 X-10의 초기 구현은 단 방향이었으며, 가정 제어를 넘어선 어떠한 애플리케이션도 제한되었다. 그러나 X-10은 아직까지도 이 기술에 대한 특허를 보유하고 있는 X-10 사를 비롯하여 주택 자동화 및 제어를 전문으로 하는 Leviton과 같은 업체들로부터의 많은 제품에서 여전히 사용되고 있다.

현재 전력선을 통한 가정 제어의 주된 기술로는 세 가지가 있는데, 가장 널리 사용되고 있는 X-10, Echelon사가 개발한 LonWorks, 그리고 CEBUS(Consumer Electronics Bus) 등이다. 이러한 기술들은 자체적으로 네트워크이지만 자동화와 제어 기능을 위해 주로 사용된다. 이 기술은 엔터테인먼트, PC 및 제어 등 다양한 네트워크의 통합이 일어남에 따라 중요해 질 것으로 보인다. 홈 게이트웨이를 통해 이러한 네트워크들을 원격으로 제어할 수 있는 능력은 가정 연결의 자연스런 발전이다.

③ Ethernet

Ethernet은 IEEE 802.3으로 표준화가 되었고 데이터 통신에서 매우 오랫동안 검증된LAN 기술이다. 이 기술은 고속(10Mbps와 100Mbps)으로 안전하며 신뢰할 수 있고 가격 역시 저렴하다. 단말 장치들은 동축케이블 또는 UTP(Unshielded Twisted Pair)에 연결되어 CSMA/CD (Carrier Sense Multiple Access with Collision Dete- ction) 프로토콜을 매체접근제어 프로토콜로 사용하고 있다. 또한, 네트워크의 관리와 셋업 중에 야기되는 문제로 인해 네트워크 관리를 목적으로 허브를 필요로 한다.

현재 UPT를 통해1,000Mbps의 전송속도를 제공하는 IEEE 802.3a가 표준화 완료 상태에 있으며, 이 기술을 이용한 장비가 출시되고 있다.[4]



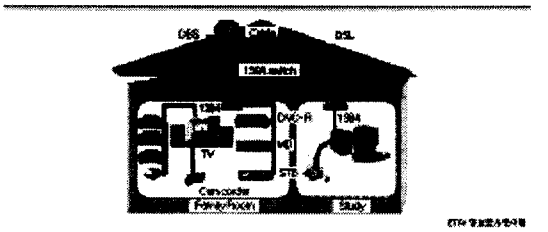
〈그림 4〉 Ethernet 홈 네트워크

④ 1394

IEEE 1394는 처음에 Texas Instruments와 Apple Computer에 의해 개발된 고속 외부버스 구조로 FireWire로 알려져 있다.

IEEE 1394는 고속 직렬버스 표준으로 버스에 최대 63개의 단말기가 접속될 수 있으며, 4.5m거리에서 최대 전송속도는 IEEE 1394a의 경우 400Mbps로 전송이 가능하며, 현재 CAT5 UTP케이블을 이용하여 보다 먼 거리를 800Mbps~ 1,600Mbps 급의 전송속도로 통신할 수 있는 IEEE 1394b의 표준이 있다. 그리고, IEEE 1394는 Hot-PnP(주소자동 지정기능 지원)를 지원하므로 복잡한 셋업절차 없이 장치의 설치가 가능하다.

네트워크 전송 표준으로서의 IEEE 1394의 주된 장점은 가전 산업과 PC 산업이 모두 이를 차세대 데이터 전송 표준으로 받아들이고 있다는 데 있다. 사실 디지털 카메라, 디지털 VCR, 그리고 고용량 데이터 저장 장치들은 이미 IEEE 1394 인터페이스를 결합하고 있으며, 조만간 소비자용 PC에서도 도입될 것으로 전망된다. (그림 5)는 IEEE 1394에 기반을 두고 있는 홈 네트워크 구성도를 보여준다.[5]



〈그림 5〉 IEEE 1394 홈 네트워크

⑤ USB

USB(Universal Serial Bus)는 HID(Human Interface Device)이며 주변 장치와 편리하게 연결되고 IRQ의 자원이 충분하고 PNP(Plug and play) 기능이 지원되는 장점이 있는 반면 낮은 전력 공급원과 상대적으로 높은 CPU 점유율 등이 단점으로 여겨지고 있다. USB의 규격은 1.1과 2.0으로 나눌 수 있는데, 현재 출시되어 있는 대부분의 USB 제품들은 1.1 규격에 맞춰 제작된 것이다.

⑥ IEEE802.11x

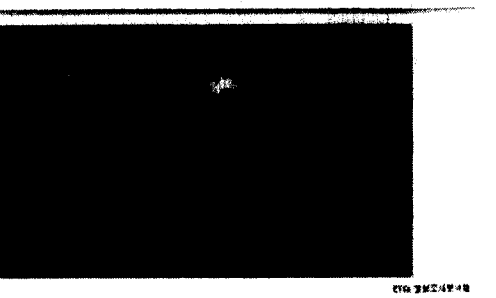
1999년 확정된 무선 LAN IEEE802.11 표준은 케이블 배선이 필요 없고, 이동하면서 기반 LAN에 접속하는 통신 형태로, 신속하게 LAN을 구성

할 수 있으며, 망구조 변경이 용이하다는 장점으로 재해 현장, 전시회, 원서 접수 현장, 유통 창고 등에서 활발하게 이용되고 잇다. 무선 LAN 시스템은 액세스 포인트(Access Point: AP)와 단말의 PCMCIA 카드형의 RF NIC 카드로 구성된다. 액세스 포인트는 유선과 무선의 브리지 역할을 하는 기능으로 최근에는 라우터, 이동관리 및 망 관리 기능 등이 내장되어 있다. 단말의 PCMCIA 카드형의 RF NIC 카드는 노트북 등 휴대용 컴퓨터에 있는 PCMCIA 슬롯에 넣어 사용된다. 핵심 기술은 단말 칩셋 개발 기술과 고성능 프로세서 하드웨어 설계 기술, 실시간 OS 및 고속의 드라이버 처리 기술 등으로 구성된다.[6]

⑦ HomeRF

현재 무선의 네트워킹 기술(RF)에 집중하고 있는 표준 및 워킹 그룹이 있으며, 여기에는 IEEE 802.11, HomeRF, Bluetooth, SWAP(standard wireless access protocol) 등이 포함된다. 무선 기반의 전송 구성요소 기술은 다양한 정보를 가정에 공급(distribute)하기 위해 사용될 수 있는데, 무선의 RF 기술은 유연성과 이동성, 그리고 배선 없이 네트워킹 할 수 있는 능력 등으로 인해 출현하고 있는 네트워크 중심적인 가정에서 선택되는 홈 네트워킹 방식이 될 것으로 예상되고 있다.

HomeRF(Home Radio Frequency)는 PC, 주변기기, 통신, 소프트웨어, 반도체 등의 산업을 주도하는 기업들을 회원으로 하고 있는 HomeRF WG에서 표준화를 진행하고 있으며, SWAP (Shared Wireless Access Protocol) 1.1 규격에 대한 표준이 완료된 상태에 있다.

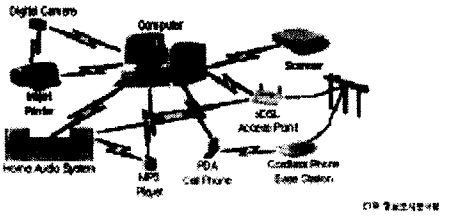


〈그림 6〉 Swap을 이용한 HomeRF 네트워크

⑧ Bluetooth

Bluetooth란 휴대용 장치간의 양방향 근거리통신을 복잡한 케이블 없이 저가격으로 구현하기 위한 근거리 무선통신 기술, 표준, 제품으로 2.4GHz ISM 대역의 라디오 주파수를 사용함으로써 장애물이 있을 경우에도 무선 데이터통신을 구현한다.

Bluetooth는 특히 이동전화 단말기/PDA 등 개인 통신기기, 헤드셋/키보드/주변 기기/프린터와 같은 주변기기, 유선으로 PC에 접속된 기기들과 같은 개인용 네트워크(Personal Area Network: PAN)로써 디자인되었다. Bluetooth의 개발 초기에는 적용범위의 제약을 받았으며, 최근에는 더 넓은 지역의 방대한 네트워크를 향한 Bluetooth의 기능이 요구되고 있다.



〈그림 7〉 Bluetooth를 이용한 홈 네트워크

⑨ UWB

UWB 시장은 주로 군용 레이다나 원격 탐지 등의 특수 목적으로 이용되었고, 통신분야의 응용은 초기 단계인 기술로서 XtremeSpectrum 사에서 VTR 및 DVD 플레이어 등의 무선 동화상 전송을 위한 UWB 칩세트(Trinity)의 평가 샘플을 발표하였다. TimeDomain사에서는 2002년 기기 메이커 대상의 평가용 칩으로서 4-5W의 전력을 사용하며, 통신, 레이더 및 위치 감지 기능 등을 포함하는 PulseON200 칩을 출시할 예정이고, 2003년 이후에는 가정에서의 무선 동화상 전송용으로 UWB 시스템의 용도를 한정한 100Mbps 급 PulseON 300 칩으로 이 칩은 상관기, 타이머, 콘트롤러의 3칩으로 구성되고, 상관기와 타이머는 IBM의 SiGe기술을, 콘트롤러는 ST의 CMOS 기술로 제조할 것으로 예상 되고 있다. 인텔은 향후 USB2.0의 무선화를 수행하기 위해서 100Mbps 급 이상의 UWB 고속 무선기술을 적용하는 것에 관심을 보이고 있으며, 이상적인 환경에서 2-3m 거리내의 100Mbps의 전송 실험을 수행하였다.[7]

2.2. 지능형 홈오토메이션 시스템 보안

2.2.1. 보안기술

1) 보안프레임 워크

홈 네트워크에서는 이종의 유무선 네트워크와 다양한 프로토콜 등의 혼재로 기존 인터넷 등에서 발생되던 보안취약성 외에도 추가적으로 고려해야할 보안취약성이 많이 존재한다. 홈 네트워크의 다양한 정보가전기기들은 인터넷과의 연결로 사이버공격의 대상이 될 수 있는 등 다양한 보안 취약성이 문제가 될 수 있다.

2) 식별 및 인증

현관의 잠금장치는 지문인증을 사용하고 TV 리모콘에 지문 인식 장치가 포함된 경우 TV 기반 서비스에서 지문 인증을 사용할 수 있으며, T-Banking 에서는 공인 인증서기반의 서비스를 사용해야한다. 실 서비스에서는 보안성과 함께 편의성을 함께 고려하여야 하므로 사용자에게 선택을 맡기는 것도 필요하다.

3) 암호 알고리즘

기본적으로 사용자의 사생활 보호라는 측면에서 본다면 거의 모든 데이터는 암호화되어 처리되어야 한다. 홈 네트워크는 특성상 많은 가구가 하나의 네트워크에서 분기하여 서비스를 받는다. 그러므로 암호화가 반드시 제공되어야한다.[8]

4) 보안 프로토콜

Silent Tree Walking과 Randomized Tree Walking 등의 정보보호를 위한 보안프로토콜을 이용하여 악의적인 사용자에 의한 정보유출을 방지한다.

5) 네트워크 인프라 공격대응

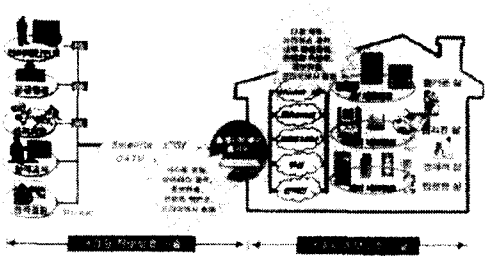
Dos 톨러런트(Tolerant) 정보보호 기술을 이용하여 네트워크 보호 뿐만 아니라, BcN 네트워크에 Dos 공격의 영향을 줄 수 있는 취약성을 원천적으로 차단하여야한다.

6) 전자서명

기기의 모듈을 갱신하거나 추가할 때 기 등록된 인증서로 검증 성공한 모듈만을 설치하도록 하여 불법적인 모듈 또는 바이러스, 스파이웨어 등의 설치를 차단하도록 하다.

7) 플랫폼

홈 네트워크는 기존 서비스와는 달리 매우 다양한 기기를 함께 사용하는 서비스로서 사용되는 플랫폼등 다양하다. 홈 게이트웨이, 셋톱박스 등의 장비는 Embedded Linux 또는 Windows CE 등을 주 OS로 사용하고 있으며 향후 다양한 Embedded OS가 사용될 수 있다.



〈그림 8〉 홈네트워크의 보안 문제점

2.2.2. 정보서버

정보 서버는 코드 관련 데이터를 기업 내부 혹은 기업간에 공유함으로써 네트워크에 유용성을 더해 주기 위한 다른 차원의 애플리케이션이다. 정보 서버가 다루는 영역은 코드 관련 데이터가 수집되고, 서비스 구동과 그에 연관된 데이터 표준을 사용하여 질의된다.[9]

1) 정보 서버 보안

네트워크에서 ID의 정보를 얻어오기 위해 사용한다.

① 해킹사고

<그림 8> 외부에 노출되면 많은 취약점들이 해커들의 주 공격 대상이 되고 있다.

② 호스트 자체의 보안

정보서버가 설치될 운영체제 자체의 보안이 되어야만 한다.

③ 정보 서버의 사용자 계정 생성

개인 사용자에 대한 계정 발급과 같은 것은 금지되어야 하며, 관리자의패스워드는 충분히 복잡해야한다.

④ 디렉터리와 파일의 접근권한

관리자에 의해 실행됨으로써 권한을 이양하거나 획득할 수 있게 하는 가능한 모든 명령어들은 항상 보호되어야 한다.

⑤ SSL/TSL의 사용

전송계층 위에서 동작하는SSL/TSL을 이용하여 보안과 기밀성이 요구되는 경우 통신 데이터를 보호할 수 있다.

⑥ 운영 관리

일반적인 ccess_log 는 서버에서 처리된 모든 요청들의 기록을 가지고 있다.

2.2.3. ODS(Object Directory Service)

질의된 코드에 해당되는 정보서버의 IP주소를 저장하고 있는 NAPTR(Naming Authority Pointer) 레코드를 얻어 오도록 하는 디렉터리 시스템이다.

1) ODS 공격 대응 방안

① Data Pivacy

DNS 데이터 보안의 측면에서 데이터 무결성을 보장하기 위한 방법

② TSIG

ODS 보안을 위해 트랜잭션 서명을 이용하여 ODS 메시지를 안전하게 하는 새로운 메커니즘이다.

③ DNSSEC

DNSSEC은 DNS 메시지에 공개키 기반의 전

자서명 기능을 제공한다.

④ SSL 서버인증

SSL서버인증은 ODS 하부구조에 관한 위협을 방지하는 방법이다.

2.2.4. 정보 서버 콘텐츠 보안

1) ESES(ETR)Secure E-commerceService)

디지털 데이터를 보호하기 위해 전자서명, 암호화 등의 보안서비스들과 암호 알고리즘 라이브러리를 통합한 시스템이다.

2) XML Trust Service

Verisign에서는 경량의 PKI를 이용할 수 있게 하기위해 XML 트러스트 서비스를 제공한다.

3) SAML, XACML, 웹서비스보안

OASIS에서는 웹서비스 보안을 위한 표준화가 보안서비스 TC를 중심으로 활발하게 진행되고있다.

2.2.5. 홈서버

홈서버는 유무선 홈 네트워크를 지원하면서 멀티미디어 미들웨어와 제어 미들웨어를 탑재하고 이를 통합하여 외부 망과 홈 네트워크 및 그에 접속된 정보가 전기기간에 서비스를 전달할 수 있는 개방형 서비스 프레임 네트워크를 구성요소로 포함함으로써 다양한 새로운 서비스의 창출이 가능하다.

Ⅲ. 결론

정보통신 인프라의 확대 보급과 함께 주목을 끌고 있는 네트워크 기반 홈오토메이션에 관한 기술 발전과 홈오토메이션 서버를 중심으로 한 보안시스템설계와 기술을 제안해 보았다. 앞으로 홈오토메이션이 아파트를 중심으로 대부분 보급되면, 주택건설업체에는 설치 시 보안 솔루션의 표준화를 통한 비용절감혜택이 주어지고, 입주고객에는 정보통신 인프라이용과 질높은 보안서비스를 받을 수 있게 된다.

따라서 홈오토메이션의 전략적 기술 개발 및 표준화, 고 신뢰성 비즈니스 기반구조 구축, 통신방송 융합성 정보 전달 방식개발, 가정 정보시스템의 안정성과 신뢰성 확보 에 크게 기여할 것이다.

향후에는 홈오토메이션과 함께 인간친화형 및 환경 기술을 지원하는 보안, 지능형 홈 네트워크의 핵심기술인 센서 기술까지 다양한 서비스를 지원하는 보안서비스, 생체인식에 관계되는 지능형 홈오토메이션 기술에 대한 연구가 되어야 할 것이다.

참고문헌

[1] 박대우, "무선 방화벽의 설계 및 구현에 관한 연구", 2003.
[2] http://www.cebus.org
[3] http://www.lonmark.org
[4] http://www.eiba.org
[5] http://www.bluetooth.com
[6] http://www.upnp.org
[7] http://www.osgi.org
[8] http://www.iso.ch/liste/JTC1SC25.htm
[9] http://www.echelon.com/products/ilon/
[10] 하서호, "WCDMA/HSDPA 개발 및 상용화 현황", SK텔레콤, 2005.
[11] 조휘만, "주거의 홈네트워크 복지서비스 전략", 대한주택공사, 2005.

Research about Intelligence Home Automation Security Design

Ju-Young Oh* · Soon-Duk Kang**

Abstract

Home-Automation which it automates as connection home by network gives human beings to many conveniences but there is a problem must solve. Rightly it is an illegal infiltration against the information transmission and a joint ownership of information home appliance machinery and tools. Especially design of Home Automation is necessary for Information Security because the vulnerability is exposed when it is connecting on the mobile communication terminal and the home appliance machinery and tools. In this research, we're going to help to function and efficiency improvement of Korean Home-Automation by Security Design and proposal for a research and development of Korean Home-Automation.

Key Words: Intelligence home automation network, Information transmission

* Professor, Division of Information Engineering, Kongju National University