情 報 保 護 學 會 誌
第 16 卷 第 6 號, 2006. 12

홈 네트워크 취약점 분석 및 인증 분석

고 훈*

요 약

디지털 홈을 구성하는 HDTV, 디지털 캠코더, Home theater, 인터넷 냉장고 등의 디지털 정보가전기기들의 보급이 활성화 되면서 가정은 단순한 가정에서 탈피하여 하나의 네트워크를 구성하게 되었다. 홈 네트워크 구성하는 기술에는 다양한 응용기술들이 있으며, 새로운 선로의 설치가 없는 여러 신호들을 전송할 수 있는 유·무선 기술이 핵심으로 응용되고 있다. 또한 홈 네트워크를 구성하는 많은 기기들이 있다. 본 논문에서는 다양한 홈 네트워크의 구성기술과 홈 기기들이 취약점 및 인증, 그리고 홈 네트워크 구축에 필요한 보안 기술에 대해서 정리한다.

Ⅰ. 서 론

정보통신의 기술 발전으로 인하여 인간은 좀 더 다양하고, 편리한 서비스에 대한 관심이 높아지고 있다. 홈 네트워크 협의의 개념은 가정에서 2대 이상의 컴퓨터를 LAN 장비를 이용하여 물리적으로 연결한 후 데이터 및 프린터, 인터넷 등을 공유할 수 있도록 가정 내 네트워크를 구성하는 것이다. 홈 네트워크가 추구하는 목적과 서비스는 인터넷을 통해 가정의 정보가전기기들을 외부에서 휴대폰, PDA와 같은 휴대용 무선 단말기를 이용해서 제어할 수 있는 네트워크를 말한다. 현재 상용화 단계에 놓여 있는 홈 네트워크 기술들은 Home RF, HomePNA, IEEE1394, Home Bluetooth, Ethernet 등이 있다. 이로 미루어 볼 때 향후 미래 사회는 하나의 단말기를 활용해 언제 어디서나 끊임없이 다양한 '컨버전스'와 '유비쿼터스'를 충족시키는 기술, 제품, 그리고 서비스가 실현될 것이다. 이러한 홈 네트워크의 요구 조건은 가정 기기간의 상호 운용, 기존 주택에 신규배선의 최소화, 사생활 보호를 위한 보안 및 안전성 확보 등을 들 수 있다. 특히 더 많은 개신정보들이 디지털화되어 인터넷에 노출됨으로써, 홈 네트워크에 접속되어 있는 장치 및 개인 사생활을 보장하는 측면에서 가정 내 시설 및 통신 등에 대한 개인사생활을 보장하는 측면 등의 보안 필요성이 중요한 이슈이다. 물론, KISA, ETRI를 필두로 안전성을 제공해주는 많은 보안모듈들이 개발 및 연구되었고, 현재에도 연구가 진행 중이다[4][5].

이에 본 논문에서는 홈 네트워크 구성요소들의 취약점 및 인증기술 그리고 안전한 홈 네트워크 구축에 필요한 보안기술들을 정리한다.

Ⅱ. 홈 네트워크 취약점 분석

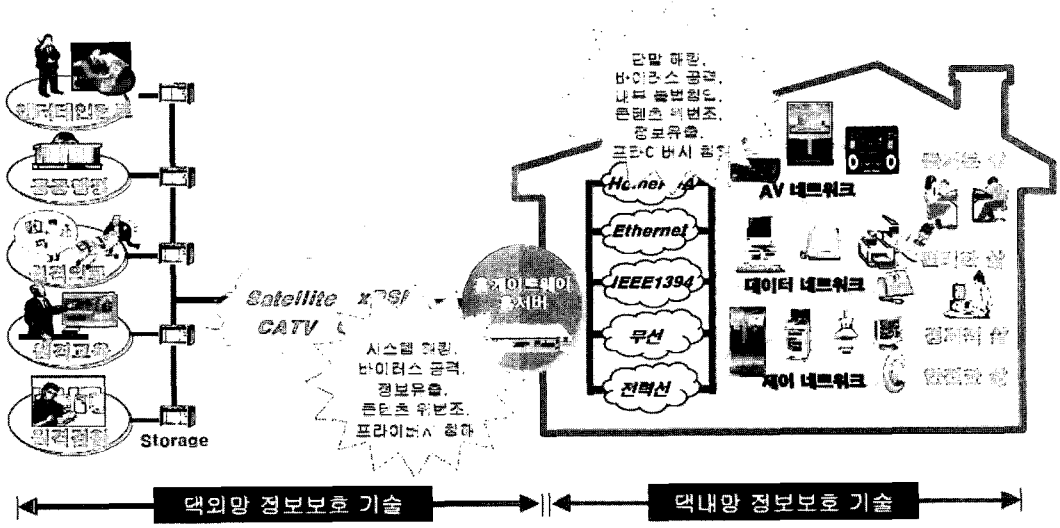
홈 네트워크 구성요소인 외부 서비스 네트워크-홈 게이트웨이-댁내망-정보가전기기간에 전달되는 사용자와 서비스 제공자의 정보에 대한 보안취약성을 분석한다. [그림 1]은 홈 네트워크 보안 취약성을 보여주고 있다. 각각의 외부망과 내부망은 서로 다른 레벨의 서비스를 제공하며 이에 따라 요구되는 차별화된 정보기술을 고려할 수 있다. 내부망, 즉 유비쿼터스 홈 네트워크 환경의 다양한 가전 및 A/V 장치들이 댁외의 서비스를 이용하기 위해서는 중간 매개체인 홈 게이트웨이의 보안 취약성 분석이 우선적으로 요구된다[1][2].

1. 유선 네트워크의 보안 취약점

1.1. HomePNA

HomePNA는 별도의 보안 기능을 제공하고 있지

* 충남대학교 차세대 정보기술 SW인력양성 사업단(skoh21@cnu.ac.kr)



〔그림 1〕 홈 네트워크 보안 취약성

않으므로 물리적으로만 연결되면 통신이 가능하다. HomePNA에서 SNMP 기능이 내장되어 있으므로, Get 및 Set 메시지를 변경하여 정보의 변조가 가능하며 신뢰할 수 있는 개체로 위장이 가능하다. 또한 메시지 순서를 뒤바꿔어 연기될 수 있으며 서비스 거부와 트래픽 분석에 대한 보안취약점을 가지고 있다[3].

1.2. PLC

PLC(Power Line Communication)는 전기가 있는 곳이라면 어디든지 존재한다는 장점이 있다. PLC는 전력선에 전기가 흐를 때 생기는 주위의 자기장을 이용하여 데이터를 전송하는 기술로 가정 곳곳에 위치한 전기콘센트에 꼽기만 하면 네트워크가 가능하여 가장 편리하고 손쉽게 사용할 수 있다는 장점이 있다. 그러나 이 기술은 기밀성이나 무결성 같은 암호 보안 요소들까지 고려하지 않는 것이 보통이다. 따라서 보안을 위해서는 별도의 방법이 강구되어야 한다[3].

1.3. IEEE1394

IEEE1394는 불법복제방지를 위하여 DTCP (Digital Transmission Content Protection) 사양에 기반을 두고 동작한다. DTCP에서는 DVD 플레이어와 디지털 TV 혹은 VCR과 같이 디지털 방식으로 연결되는 기기는 키를 교환한다. 디지털 TV는 암호 알고리즘과 AKE 및 공개키 암호화 기술 기반으로 AKE 방식의 하드웨어 가속기능을 제공하여 사용자 응답 시간을 향상시키고 소프트웨어 오버헤드를 줄인다. 이와 같이 IEEE1394의 보안 기능은 기기간의 접속에 대한 인증만 제공하고 있다. 하지만 파이어 와이어 방식을 이용한 USB 하드드라이브, 아이포드와 같은 휴대형 저장장치 등이 보안에 취약하다는 내용은 네트워크에 악성코드를 전염시켜 데이터를 빼낼 수 있어 보안상에 중대한 위협요소가 될 수 있다[3].

1.4. USB

USB(Universal Serial Bus) 범용 직렬버스로 인텔, 마이크로소프트, 컴팩, DEL, IBM, 캐나다 노던텔레콤, NEC 등 7개사가 공동으로 제안하고 있는 새로운 주변기기 접속 Interface 규격으로 규격이 다른 글쇠판, Mouse, Printer, Modem, Speaker 등을 비롯한 주변기기 등을 개인용 컴퓨터(PC)에 접속하기 위한 인터페이스의 공동화를 목적으로 한다. PC 본체에 유니버설 시리얼 버스(BUS) 접속기를 하나만 갖추고 있으며 주변기기 등을 Star Connection 또는 방사형 형태로 최고 127대까지 연결할 수 있다. 주변기기 등을 PC와 연결할 때 S/W나 H/W를 별도로 설정할 필요 없이 모든 주변기기를 동일한 접속기로 접속

하기 때문에 PORT수를 획기적으로 줄일 수 있을 뿐만이 아니라 설치가 간편하고, 휴대형 PC의 소형화가 가능하게 되는 장점이 있다. [표 1]은 유선 홈 네트워크 기술의 보안 취약점을 정리한 내용이다[3].

[표 1] 유선 홈 네트워크 기술의 보안 취약점

기술	보안 취약점
IEEE1394	-데이터 송수신으로 인한 유출 및 변조
PLC	-제어정보/데이터 전송 시 유출 및 위변조
HomePNA	-SNMP 기능 내장 -인증과 프라이버시 서비스들을 제공 -서비스 거부와 트래픽 분석의 보안 취약성 존재
USB	-오류발생시 재전송 불가 -키보드나 마우스 등 저속 전송 모드에 적용 -대역 보증이 없어 제어정보/데이터 전송 시 유출 및 위변조에 취약성 존재

2. 유선 네트워크의 보안 취약점

2.1. Bluetooth

블루투스에 대한 보안 취약성을 세 가지 정도로 정리할 수 있다.

- ○ 블루스니핑 : 휴대폰 보안 취약점을 이용하여 폰에 저장된 전화번호목록이나 일정표를 읽고 변형시키고 복사하는 기술
- ○ 블루버깅 : 주인이 알지 못하게 그 기기의 명령을 이용하는 기술로 다른 사람의 전화를 이용하여 몰래 통화하고 전화번호부를 뒤질 수 있다.
- ○ 블루재킹 : 스팸처럼 명함을 익명으로 마구 퍼트리는 것

2.2. Zigbee

Zigbee는 각 계층별로 보안 서비스들을 제공한다. 동일한 Zigbee 기기 내에서는 MAC, 네트워크, 응용 프로그램 계층 각각에서 사용하는 키는 동일하다. Zigbee의 경우 Zigbee만의 고유한 취약성은 밝혀진 사실은 없다. 하지만, Zigbee 프로토콜이 무선에 기반을 두고 있기 때문에 일반적인 무선랜 취약성을 그대로 재현될 수 있다[3].

2.3. 무선랜

무선랜은 AP를 이용하기 때문에 불필요한 곳에서도 접근이 가능하다. 따라서 비인가 사용자가 쉽게 접근하는 문제가 발생된다. 게다가 아직까지 전파 도달 범위에 대한 표준안이 마련 중이기 때문에 외부로 전파가 세어 나가는 것을 막는 대비책이 필요하다. 서비스 거부공격의 여러 형태로 홈 네트워크 서비스의 가용성을 저해하는 공격으로 배터리 소모, 정상적인 동작 방해 등이 있다. 그리고 무선 환경에서 노출된 SSID를 통해 불법 사용자는 홈 네트워크 내의 정보를 무단으로 사용 가능하다. [표 2]는 무선 홈 네트워크 기술의 보안 취약점을 정리한 내용이다[3].

[표 2] 무선 홈 네트워크 기술의 보안 취약점

기술	보안 취약점
WLAN	-실시간 공격과 도청으로 인한 평문의 노출 -DoS 공격의 위험 존재
초광대역 통신	-무선기반 시스템의 개방성 때문에 정보의 유출 위험 존재 -WEP 암호화 기술을 보안하기 위한 연구 필요
무선랜	-높은 전송속도 지원이 필요할 뿐만 아니라 seamless connection 지원을 위한 안정적인 제어와 통신이 가능한 MAC 개발이 필요
무선1394	-잠재적으로 유해한 클라이언트가 이용자로 가장하여 정보의 유출을 유도할 수 있는 위험 존재
Zigbee	-블루스키핑, 블루버깅, 블루재킹

3. 홈 게이트웨이 취약점

홈 게이트웨이는 인터넷망과 댁내망의 연결, 댁내망 정보기기들 사이의 인터페이스 접속기능을 담당하므로 다양한 외부 네트워크로부터 콘텐츠 및 서비스를 안전하게 제공 받기 위해서는 외부망으로부터의 해킹, 악성코드, 웜 및 바이러스, DoS, 유무선 통신 도·감청 등 외부 보안 공격들을 고려해야 한다. 다양한 정보기기들이 홈 게이트웨이에 연결되어 상호 운용되면, 홈 게이트웨이와 정보가전기기간의 메시지/데이터의 유출과 인증되지 않은 정보기기의 연결에 보안취약성이 있으므로 외부 네트워크와 내부 정보가전기기의 중간 매개체 역할을 하는 홈 게이트웨이는 보다 체계적인 보안 및 인증 기술이 필요하다. [표 3]은 홈 게이트웨이가 가진 외부 인터페이스 및 서비스를 고려한 세분화된 보안 기술에 대한 취약점을 정리한 내용이다[3].

〔표 3〕 홈 게이트웨이 취약점

항목	인증	접근제어	기밀성/무결성	서비스 거부공격
홈 게이트웨이	-내/외부 접근자위장	-불법접근자의 제어 가능성 -불법적트래픽 차단	-서버저장정보의 유출 -물리적 장애 및 오작동 문제	-장비사용불능

4. 홈 기기 취약점

〔표 4〕는 홈 기기 / 정보가전 기기의 취약성을 정리한 내용이다.

〔표 4〕 홈 기기 / 정보가전 기기 취약점

항목	인증	접근제어	기밀성 / 무결성	서비스 거부공격
PC	OS의 각종 보안취약점을 이용한 불법인증	불법적인 백도어 프로그램 제어	PC에 저장된 데이터 유출, 삭제	웜바이러스에의한 서비스 중단
터치 스크린	무선네트워크의 취약점내제	정보가전등 타기기에 대한 불법적 제어 가능성	물리적 장애 및 오작동	
PDA, 모바일폰	-무선단말기 os취약점을 통한 불법인증 -무선네트워크의 취약점내제	무선단말기의 분실, 도난을 통해 비인가자의 불법사용	기기에 저장된 개인 정보 유출	악성코드의 유입으로 CPU를 소모시키는 공격
DTV 셋탑박스, 냉장고, 세탁기, 에어컨	기기위장, 불법기기 인증	불법적 접근자의 제어 가능성 존재	물리적 장애 및 오작동	기기 사용불능

5. 홈 미들웨어 기술의 취약점

미들웨어가 갖는 최대의 약점은 서비스마다 다양한 구현기술을 필요로 하고, 다양한 미디어, 프로토콜들, 미들웨어 표준 미비 등을 들 수 있다.

5.1. UPnP

UPnP 장치 보안 서비스는 인증, 접근권한제어, 재전송 방어 그리고 개인정보보호를 위한 강력한 수단을 제공한다. 그리고 장치는 자신만의 고유한 ACL을 가지고 있으며, 보안 콘솔이 ACL을 가지고 있다. 또한 보안 콘솔이 ACL 정책을 수립하고 관리한다.

5.2. HAVi

HAVi는 RSA알고리즘과 160비트 SHA-1 해쉬 알고리즘을 이용하여 기기간의 인증을 제공한다. 그러나 접근 제어 기능은 제공하지 않으므로 불법 침입자가 접근할 가능성이 존재하며, 메시지 전송 시 암호화를 하지 않고 메시지 위·변조를 검사하지 않으므로 기밀성과 무결성이 보장되지 않는다.

5.3. Jini

Jini는 서비스 제공자, 즉 서버와 서비스 객체, 프락시 사이의 프로토콜을 제한하지 않는다. 따라서 프로토콜을 보안 요구사항에 맞춰 변경 가능하다. 그러나, 이것은 서비스 개발자에게 비용을 요구하며 자주 발행하는 보안 요구사항에 쉽게 그리고 안전하게 접근하지 못한다.

Ⅲ. 홈 네트워크 인증 분석

홈 게이트웨이 접근하는 관리자 및 사용자의 신원을 확인하는 기능이 필요하며, 최근에 ID와 패스워드 기능뿐 아니라, 지문, 손, 안면, 홍채 등 신체적 특성을 이용한 생체인식 장치가 점차 사용되고 있다. 홈 네트워크에 관련된 내용은 아래와 같이 정리할 수 있다.

1. 홈 네트워크 인증 영역

1.1. 2계층 인증

네트워크를 이용하는데 있어서 가장 기본적인 부분에서 인증, 즉 기기와 사용자에 대한 인증을 요구해 내부적인 보안을 처리한다.

1.2. 기기 인증

정보가전기기의 연결이 발생하는 경우 부정한 정보가전기기인지를 확인하는 기능이 필요하다. PC 및 사용자 내부 단말들의 인증은 네트워크를 사용하는데 있어서 필요한 요소의 조합으로 네트워크 접속을 제한한다.

2. 현재 사용 중인 인증

시스템 관리자는 홈 게이트웨이 사용자의 프로파일

레코드를 설정하여 등록된 모바일 기기 혹은 외부에서 휴대폰용 무선인터넷을 거쳐 가정용 홈 게이트웨이에 접근하여 사용한다.

Ⅳ. 홈 네트워크 보안 기술

1. 홈 게이트웨이 보안 고려사항

가까운 미래에 홈 네트워크의 보급이 확산되고 다양한 형태의 홈 네트워크 서비스가 보급되면 사이버 공격의 대상 범위 또한 홈 네트워크로 상호연결 되어 있는 냉장고, 세탁기, 가스레인지와 같은 가전기기 및 센서 등으로 확대될 가능성이 높다. 홈 네트워크 서비스의 침해사고 발생은 그 피해가 인터넷과는 비교가 안 될 정도로 심각할 것으로 예상된다. 홈 네트워크 서비스가 널리 보급되기 위해서 우선적으로 다음과 같은 보안 요소에 대한 고려가 있어야 한다.

(1) 개인과 가족의 신원을 정확히 확인하여 타인이 홈 네트워크를 불법적으로 사용하는 것을 막아야 한다.
(2) 홈 네트워크 서비스를 안전하게 이용하기 위해 인증을 받은 사용자의 신원에 따라 기기 혹은 서비스를 차등적으로 이용할 수 있는 권한을 부여할 수 있어야 한다.
(3) 홈 네트워크상에서 돌아다니는 개인정보 등의 민감한 데이터가 타인에게 노출되지 않도록 하는 개인프라이버시 보호를 위한 기술도 필요하다.

2. 홈 게이트웨이 보안 목표

가용성(Availability) : 정보 시스템이 적절한 방법으로 사용되고 정당한 방법으로 권한이 주어진 사용자에게 정보 서비스 접근을 보장하고 데이터 백업, 중복 유지, 위협 요소 제거 기술 필요

비밀성(Confidentiality) : 소극적인 공격으로 부터 정보를 보호, 인가되지 않은 정보의 공개를 막음

접근통제(Access Control) : 암호화 등의 기술 필요

무결성(Integrity) : 정보의 정확성, 완전성, 일치성을 유지

물리적 통제(Physical Control) : 회복 메커니즘(Recovery Mechanism)등의 기술 필요

인증 (Authentication) : 메시지 또는 전자문서의 출처를 확인하고, 해당 출처의 신분이 거짓이 아님을 확인하는 과정

부인 봉쇄 (Non-Repudiation) : 메시지의 송/수신자가 전송 사실을 부인 할 수 없도록 함

접근 제어 (Access Control) : 목적 시스템에 대한 정보자원의 접근을 통제

3. 홈 네트워크 적용 보안기술

안전한 홈 네트워크 구축을 위한 적용 보안기술은 방화벽, 암호화/복호화, IPSec, SSL/TLS 등이 있다. 홈 게이트웨이 보안을 위해서 개발해야 할 기술로는 유효한 사용자를 구별하고 다양한 정보기기 간에 안전한 통신 및 제어를 가능하게 하는 인증 인프라 기술이 필요하며, 침해상황에 따라 접근권한을 능동적으로 제어할 수 있는 기술이 필요하다. 또한, 홈 네트워크의 다양한 유무선 매체 및 관련 프로토콜을 고려한 통합 보안 환경에 적용 가능한 경량화 된 보안 메커니즘이 필요하다. 이 경량화 된 보안 메커니즘은 홈 네트워크 환경에 적합한 인증 및 암호 모듈 개발과 홈 네트워크 자원보호를 위한 접근권한 제어 모듈 개발로 구분된다.

Ⅴ. 정 리

지금까지 홈 네트워크 취약점 분석내용과 인증분석 내용에 대해서 정리하였다. 홈 네트워크 보안상의 문제점 및 해결 방안을 살펴보면, 홈 네트워크에는 이종의 유무선 네트워크와 프로토콜 등의 혼재로 다양한 보안 취약성이 존재에 대한 해결방안은 홈 네트워크의 안전성 확보를 위해서는 다양한 보안취약성을 고려한 종합적인 보안 인프라 구축하고 추진해야겠다.

홈 네트워크 환경에 적용이 가능한 사용자 중심의 경량화 된 인증체계가 없고 홈 네트워크 자원 보호를 위한 접근제어 기술이 미비에 대한 해결방안으로는 안전한 홈서비스 제공을 위해 사용자편리성과 정보단말 성능을 고려한 경량 의 인증체계 및 접근제어기술 개발과 홈서비스 활성화 및 개발결과물의 상용화 유도를 위해 다양한 사용자 인증기술이 정합 가능하도록 개발해야 한다.

홈 네트워크 정보보호 기술에 대한 국내외 표준화 미비 및 개발 기술의 활성화를 위해서는 기술 표준 제정이 필요에 대한 해결방안으로는 홈 네트워크 시큐리티 포럼을 통하여 개발결과의 기술검증 및 국내외 표준화 작업 추진이 이루어져야 하겠다.

앞서 언급했듯이, KISA, ETRI를 필두로 많은 업체에서 홈 네트워크 보안개발에 많은 부분 진전이 있다.

그러나, 국내 홈 네트워크를 주도하는 회사들끼리의 홈 기기 연동이 되지 않는 것이 현실이다. 또한 개발된 모듈을 홈 네트워크에 탑재하여 구축된 사례 또한 많이 않다. 따라서, 실제로 구축된 시스템에서 사용하여 보고, 이에 대한 문제점을 계속적으로 분석하여 새로운 보안 모듈의 개발이 필요하다 하겠다.

참 고 문 헌

[1] Steve G, Ungar, "Home Network Security," *IEEE Fourth International Workshop on Network Appliance*, 2004..

[2] 서광현, "디지털 홈 구축 정책방향," *TTA 저널 88호 한국정보통신기술협회*, 2006.3.

[3] 유비쿼터스 홈네트워크 침입대응 기술, *한국전자통신연구원*, 2005. 5.

[4] 홈 네트워크, *IITA 기술정책정보단*, 2004. 3.

[5] 홈 네트워크 산업 정책 동향, *KIPA*, 2005. 4.

〈著者紹介〉

고 훈 (Hoon Ko)

정회원

1998년 2월 : 호원대학교 컴퓨터학부 졸업

2000년 2월 : 숭실대학교 컴퓨터학과 석사

2004년 8월 : 숭실대학교 컴퓨터학과 박사

2002년 9월~2006년 8월 : 대진대학교 컴퓨터공학과 초빙교수

2006년 9월~현재 : 충남대학교 차세대정보기술SW인력양성사업단 계약교수

관심분야 : Home Network Security, Msec, Authentication 등.