전자통신동향분석 제20권 제2호 2005년 4월

유비쿼터스 홈 서버 보안 요구사항 및 구현방안

Security Requirements and Proposals for the Home Server in Ubiquitous Home Networks

김정태 (J.T. Kim)	유비쿼터스홈서비스연구팀 연구원
범민준 (M.J. Beom)	유비쿼터스홈서비스연구팀 연구원
박혜경 (H.K. Park)	유비쿼터스홈서비스연구팀 선임연구원
백의현 (E.H. Paik)	유비쿼터스홈서비스연구팀 책임연구원, 팀장

목 차

유비쿼터스 환경의 현실화와 일반화의 시발점인 홈 네트워크 기술은 PC와 노트북, 프린터, 냉장고, DTV, 오디오/비디오를 포함하는 댁내의 모든 가전기기들을 하나의 네트워크로 연결함으로써 사용자가 언제 어디에 있든 인터넷을 이용하여 댁내의 상황을 모니터링하고 모든 기기들을 제어할 수 있게 해주는 기술이다. 현재 대부분의 기업들은 각자 회사의 네트워크를 보호하기 위하여 방화벽(firewall)이나 침입탐지시스템(intrusion detection system) 및 가상 사설망(virtual private network) 등의 방어책을 응용하고 있지만, 홈 네트워크는 기업과 비교하여 규모면에서나 보안 기술에 대한 고려 및 응용이 활발하지 않다. 이러한 다양한 보안 정책은 다가올 유비쿼터스 홈 네트워크 환경에서의 중추적 역할을 해야 될 홈 서버의 중요한 역할 중 하나이다. 따라서 본 문서의 유비쿼터스 홈 네트워크 환경에서 홈 서버의 보안 요구사항 및 구현방안들을 살펴 본다.

Ⅰ. 서론

홈 네트워크는 콘텐츠 및 솔루션들을 외부 서비스 네트워크 환경, 즉 인터넷 망을 통해 연동하기 때문에 공중 네트워크에서 일어나는 해킹이나 바이러스 침입 등의 위험에 노출되어 있다. 이러한 잠재적 위험 요소를 고려하여 본 문서에서는 다가올 유비쿼터스 환경에서 보다 신뢰성을 갖춘 안전한 홈 네트워크 서비스 및 여건들을 제공하기 위하여 요구되는 홈 서버의 보안 요구 사항들을 각 홈 네트워크 구성 요소별로 살펴봄과 동시에 대비책으로 여러 보안 기술들을 제시한다.

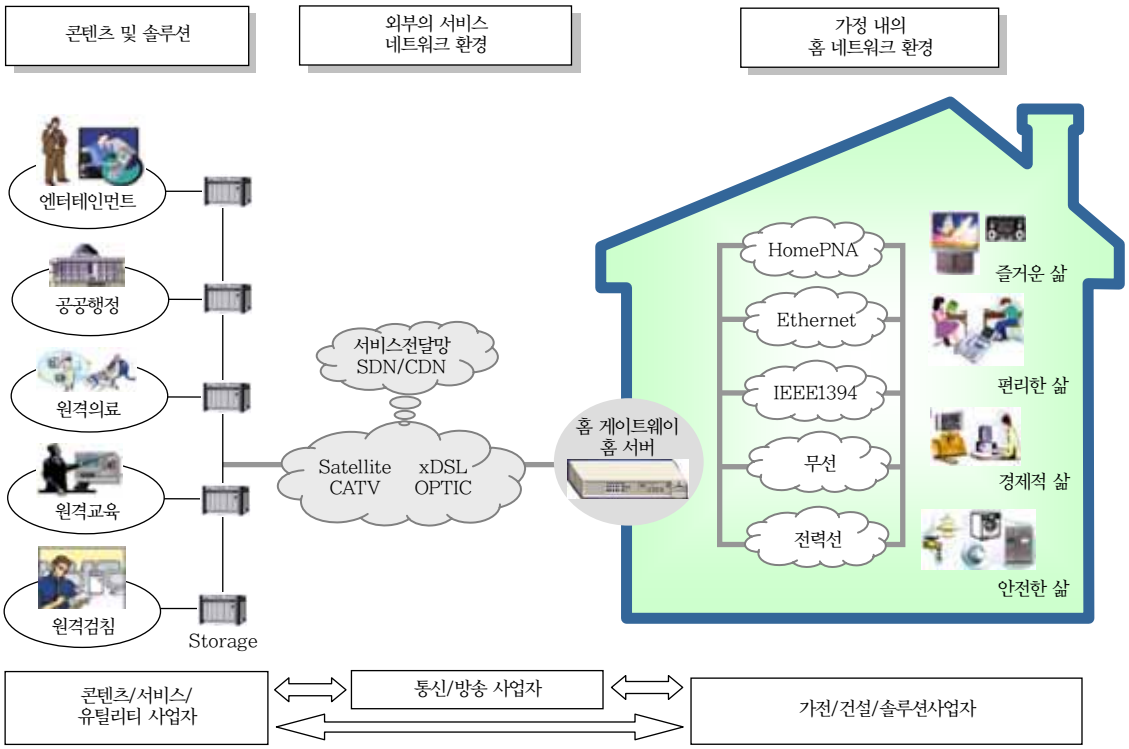
Ⅱ. 홈 네트워크 구성요소

(그림 1)에서 보여주듯 홈 네트워크를 구성하는 요소로는 기본적으로 외부의 서비스 네트워크(외부망)를 포함하여 서비스 관련 콘텐츠 및 솔루션, 댁내·외의 다양한 장치들과 홈 서버·게이트웨이로 분류될 수 있다[1].

디지털 홈 서비스를 위한 정보의 흐름의 관점에서 크게 홈 네트워크를 재 분류하면 외부망, 홈 네트워크, 홈 서버·게이트웨이로 나눌 수 있다. 각 구성 요소들의 특성을 살펴 보면 다음과 같다.

1. 외부의 서비스 네트워크

서비스를 가정까지 전달해 주기 위한 외부의 네트워크는 (그림 1)에서 제시된 바와 같이 서비스 전달망(SDN) 또는 콘텐츠 전달망(CDN)이 존재하며 세부적인 기반 기술로는 DSL, Satellite(위성), CATV, OPTIC(광통신) 등 다양하게 존재한다. 즉, 디지털 홈 서비스 관련 정보들을 처리하고 분배 및 관리해 주는 부분으로 콘텐츠/서비스 공급자와 댁내 사용자간의 중계자 역할을 한다.



(그림 1) 디지털 홈 네트워크 구성도

2. 홈 네트워크

디지털 홈을 구축하기 위해 네트워크 기능이 부가된 TV, 오디오시스템, 인터넷냉장고, 보안시스템, 프린터, 팩스, 휴대폰, PDA 등 광범위하고 다양한 기능의 정보가전기기들과 이들 사이를 연결하는 홈 네트워크 기술, 즉 IP/Non-IP 통합 프로토콜이 필요하며 이 기술은 크게 유선과 무선으로 분류된다. 유선형태의 대표적인 기술로는 Ethernet, HomePNA, PLC, IEEE1394, USB, 이더넷 등 다양한 기술이 존재하며, 무선형태로는 Bluetooth, IEEE 802.11 WLAN, HomeF, IrDA, UWB 및 무선 1394 등의 기술이 있다[2]. 지금까지 홈 네트워크에서 사용될 전송 매체의 분류를 살펴보면 〈표 1〉과 같다[3].

〈표 1〉에서 살펴본 각각의 기술들은 세분화된 특성들은 다양한 홈 네트워크 서비스들을 가능하게 하고 특히 최근에는 표준화에 따른 UWB나 무선 1394를 이용하는 댁내 가전 서비스가 크게 늘어나고 있다.

3. 홈 게이트웨이

홈 게이트웨이는 여러 가지 유무선 홈 네트워크 기술들 중 하나 이상의 댁내망 기술과 xDSL, 케이블, 광 전송장치 및 위성 등 하나 이상의 액세스망 기술을 상호 접속하거나 중계하고 그 상위 계층에 미들웨어 기술을 부가함으로써 가정의 사용자에게 다양한 멀티미디어 서비스를 제공하기 위한 클라이언트 장치이다[4]. ETRI에서 개발한 FTTH 홈 게이트웨이의 세부 시스템사양 및 서비스를 살펴보면 〈표 2〉와 같다.

〈표 1〉 홈 네트워킹 기술의 특징 비교

구분		동작원리	속도	신뢰성	비용	장점	단점
유선 네트워크	Ethernet	서버와 허브를 갖는 CAT5 배선 사용	10~100 Mbps	높음	고	- 100Mbps까지의 빠른 데이터 전송속도 - 신뢰성있는 표준을 기반으로함	- 높은 비용 - 특수배선 필요 - 인텔리전트 네트워킹을 위해 서브, 라우터, 서버 필요
	Phone Line	기존 전화선 이용	1~10 Mbps	높음	저	- 10Mbps까지의 빠른 데이터 전송속도 - 기존 옥내전화배선사용 - 설치용이, 낮은 비용	- 장치들이 유선으로 네트워크에 연결되어야 함
	Power Line	기존 옥내전력선 사용	1~10 Mbps	보통	저	- 빠른 데이터 전송속도 - 기존옥내에 배선된 전력선 이용 - 유연성, 설치용이	- 전송장애와 간섭을 받을 수 있음 - 네트워크 환경불량 - 표준이 없음
무선 네트워크	HomeRF	2.4GHz 무선 주파수 사용	10Mbps	보통~ 높음	중	- 10Mbps까지의 빠른 데이터 전송속도 - 신뢰성있는 표준을 기반 - 배선이 필요없는 이동성 - 저렴한 비용	- 동작범위 문제 - 구조적 장애물을 가질 수 있음 - 기지국이 요구됨 - 널리 확산되지 못함
	IEEE 802.11b	2.4GHz 무선 주파수 사용	2~11 Mbps	보통~ 높음	다양	- 빠른 데이터 전송속도 - 신뢰성 있는 표준을 기반으로 함 - 배선이 필요없는 유연성 - 시장에서 매력적인 대안임	- 비용이 높음 - 동작범위 및 구조적 장애물 가짐 - 기지국 필요
	블루투스	2.4GHz 무선 주파수 사용	1Mbps	보통~ 높음	중	- 이동성 - 비용저렴 - 개인네트워크가 가능해짐	- 제한된 동작범위 - 데이터 전송속도가 낮음 - 장치들에 블루투스칩 탑재되어야 함

〈표 2〉 FTTH 홈 게이트웨이 기본 스펙 및 서비스

Processor	- CPU 533MHz/ Embedded Linux 2.4.20
Network Interface	- 1Gbps EPON(802.3ah) - Gigabit Ethernet(1000base-T,X) - Fast Ethernet, VDSL
Home Interface	- 6 ports fast & 1 port gigabit Ethernet - WLAN(802.11a/b/g) - Internet Telephone(G.711/713.1) - Video Door Phone
Services	- IP Broadcasting - SIP based Internet Telephone - Visitor Confirmation Service - Net-filtering Firewall - H/W Accelerated IPSec VPN

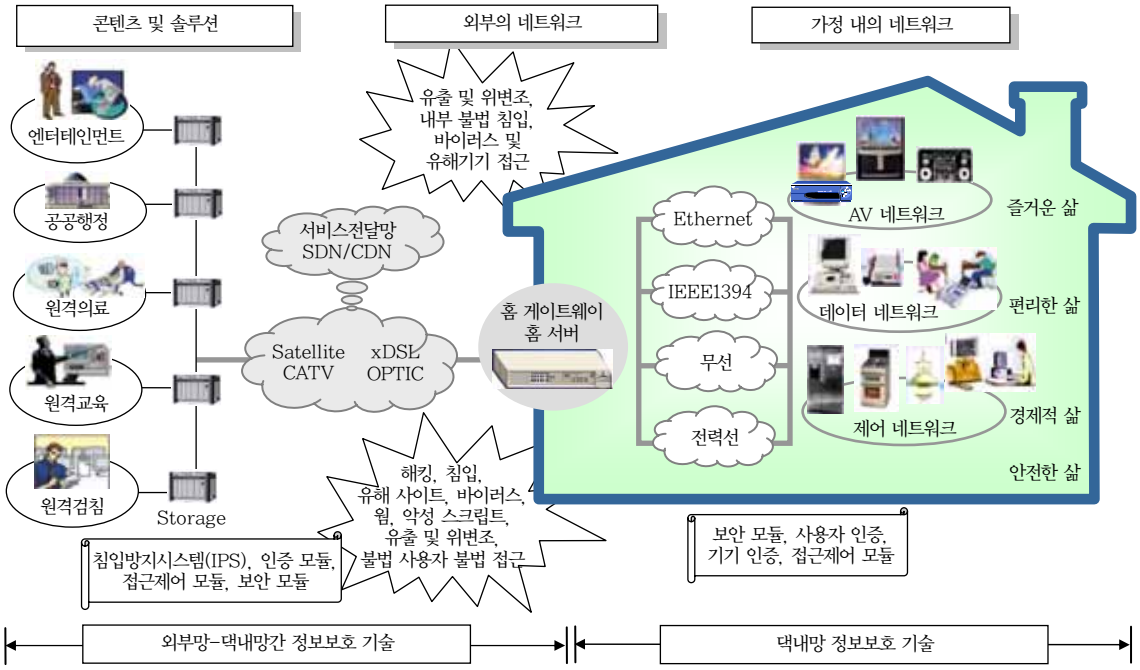
〈자료〉: ETRI 2004.

4. 홈 서버

홈 서버는 비디오, 전화, 웹, 전자우편, 팩스 등 가정에 있는 각종 미디어의 정보들을 저장, 통합, 분배하는 일종의 컴퓨터 장치를 말한다. 가전업체의 경우, 방송이나 전화 및 인터넷을 통하여 가정으로 들어오는 외부 콘텐츠를 저장 및 재분배하는 것을 홈 서버의 주요 기능으로 정의하고 있다. 홈 서버는 디지털 영상이나 음악을 저장하는 장치로 사용될 뿐 아니라 PC의 외부 저장장치로 기능하여 가정에서의 정보제어센터의 역할을 수행한다. 반면에 디지털 방송관련 업체들은 양방향 기술을 이용한 대화형 TV에서 수신기가 시청자의 기호에 맞는 프로그램을 자동적으로 녹화해주고, 보고 싶은 프로그램을 언제라도 꺼내 시청할 수 있는 기능을 제공하는 홈 서버의 역할을 수행해야 된다고 보고 있다. 삼성의 차세대 홈 서버인 MagicGate는 방송 수신, 멀티미디어, 홈 네트워크, mobile SVR, 인터넷, 기타 유무선 정합의 네트워킹 기능을 종합적으로 제공한다.

Ⅲ. 구성요소별 보안 취약성

홈 네트워크 구성요소인 외부 서비스 네트워크-홈 서버 · 게이트웨이-댁내망-정보가전기기간에 전달되는 사용자와 서비스 제공자의 정보에 대한 보안



(그림 2) 홈 네트워크 보안 취약성과 정보보호 기술

취약성을 분석한다. (그림 2)는 홈 네트워크를 홈 서버·게이트웨이를 경계로 크게 외부망과 내부망으로 분류한다[5].

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 서버·게이트웨이의 보안 취약점 분석이 우선적으로 요구된다.

1. 홈 서버·게이트웨이 보안 취약점

소비자가 정보가전 제품과 같은 가정 내의 모든 정보 단말기를 인터넷이나 휴대정보 단말기로 연결하여 언제 어디서나 손쉽게 제어할 수 잇는 홈 서비스 환경에서 다양한 가정정보 서비스를 안전하게 제공 받기 위해서는 외부망(인터넷)과의 연결은 필수적이다. 홈 서버·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. 또한, 다양한 정보기기들이 홈 서버에 연결되어 상호 운용되면, 홈 서버-정보가전기기간의 메시지/데이터의 유출과 인증되지 않은 정보기기의 연결에 보안취약성이 있으므로 외부 네트워크와 내부 정보가전기기의 중간 매개체 역할을 하는 홈 서버·게이트웨이는 보다 체계화된 보안 및 인증 기술이 필요하다. 마지막으로 홈 서버·게이트웨이의 공존으로 인한 보안 수준 및 기술 적용의 표준화 측면에서의 고려도 필요하다. 각 연결망의 특성, 특히 홈 서버·게이트웨이가 가진 외부 인터페이스 및 서비스를 고려한 세분화된 보안 기술의 적용이 요구된다.

2. 댁내·외부 네트워크 보안 취약점

댁내·외부 네트워크는 특히 무선구간에서 가정 밖의 불법 사용자의 개입으로 인하여 전송 정보의 유출 및 위변조에 대해 보안 취약성이 존재하며, 유선의 경우도 마찬가지이다. 댁내 통신망은 특히 무선 구간에서의 인증, 데이터 보호 등에서 취약성이 있으며, 각 통신망에 구현된 보안 구조 또는 프레임워크에 접근제어, 사용자/단말 인증 및 암호화 기능을 수용해야 한다. 먼저 댁내 각 유선 홈 네트워킹 기술의 특성 및 보안 취약점을 간단히 살펴보면 〈표 3〉과 같다.

가트너의 조사에 따르면 무선 홈 네트워킹을 지원하는 표준 무선 기술[7]들은 〈표 4〉와 같이 분류된다.

각 무선 홈 네트워킹 기술들의 특성 및 보안 취약점을 살펴보면 〈표 5〉와 같다.

〈표 3〉 유선 홈 네트워킹 기술의 특성 및 보안 취약점

기술	보안 취약점
IEEE1394&802.3(Ethernet)[6]	- Physical Layer는 IEEE1394 및 Ethernet 디바이스의 케이블과 물리적으로 연결 - 실제 데이터 송수신으로 인한 제어정보/데이터 전송 시 유출 및 위변조의 위험 존재
전력선 통신(PLC)	- HNCP는 전력선 통신 기반의 기기들 사이의 통신 방법에 대한 기준 제공 - 제어정보/데이터 전송 시 유출 및 위변조에 취약성 존재
HomePNA	- SNMP 기능 내장 - 인증(authentication)과 프라이버시(privacy) 서비스들을 제공 - 서비스 거부(Denial of Service)와 트래픽 분석(traffic analysis)의 보안 취약성이 존재
USB	- USB는 데이터를 패킷 단위로 전송 - 오류 발생 시 재전송 불가 - 저해상도 디지털 카메라, PC 카메라 등에 이용 - 키보드나 마우스 등 저속 전송 모드에 이용 - 대역 보증이 없어 제어정보/데이터 전송 시 유출 및 위변조에 취약성이 존재

〈표 4〉 주요 근거리 무선 기술들의 비교

표준	IEEE802.11b	Bluetooth	IEEE802.11a	UWB
주파수 대역폭	2.4GHz(ISM band)	2.4GHz(ISM band)	5GHz(U-NII band)	3.1~10.6GHz
커버리지	100m	10m	50m	10m
최대속도	11Mbps	10Mbps	54Mbps	500Mbps 이상
Spatial Capacity	1,000	30,000	83,000	1,000,000

주) Spatial Capacity: Bit/Sec/Square-meter 혹은 bps/m^2
〈자료〉: ETRI 2002, Gartner 2002, Intel Technology Journal 2001.

〈표 5〉 무선 홈 네트워킹 기술의 특성 및 보안 취약점

기술	보안 취약점
WLAN	- IEEE 802.11의 WEP 알고리듬에서 키 스트림의 단순성 - 실시간 공격과 도청으로 인한 평문의 노출 - DoS 공격의 위험 존재
초광대역통신(UWB)	- 110Mbps의 고속 데이터 전송이 가능 - 전송 거리가 10m 이내이며 벽을 통과하지 못함 - 홈 네트워크 시스템에의 적용에는 클러스터 네트워크로만 사용이 가능 - 무선 기반 시스템의 개방성 때문에 정보의 유출 위험 존재 - WEP 암호화 기술을 보완하기 위한 연구중
무선 PAN (IEEE802.15.4)	- 초저가의 칩에 20kbps와 250kbps 전송속도만 지원 - 무선 제어 시스템으로 최적 - 고속 WPAN(IEEE802.15.3) 기술은 55Mbps의 초고속 데이터 전송에 70m의 전송 거리 지원 및 QoS와 security를 제공 - 높은 전송속도 지원이 필요할 뿐만 아니라 seamless connection 지원을 위한 안정적인 통신과 제어가 가능한 MAC 기술 개발 필요
무선 1394 (High Performance Serial Bus)	- 54Mbps 지원 무선 네트워킹 기술 - 무선 1394의 기반을 둔 DHCP(RFC2855) 활용[8] - 잠재적으로 유해한 클라이언트가 이용자 가장(masquerading)으로 정보의 유출을 유도할 수 있는 위험 존재
무선 RF[9]	- PC와 가정용 소비자 가전제품 간의 무선 연결 제공 - HRFWG는 공유 무선 액세스 프로토콜(shared wireless access protocol)이라 불리는 가정용 무선 스펙 제공 - 제품의 대역폭(특히 고대역폭)과 허가권 문제 - 홈 RF의 1.6Mbps 제품들은 802.11b 경쟁제품들의 범위에 비해 성능 저조 - SWAP의 고주파 라디오 발신에 대해 허가 필요
Zigbee[10]	- 저속 전송속도를 갖는 홈오토메이션 및 데이터 네트워크를 위한 표준 기술 - 인터넷을 통한 전화 접속으로 홈 오토메이션 활용 - IEEE802.15.4 MAC 하위계층 기반 보안서비스 제공 - 각 장치들은 인증된 네트워크 내의 다른 장치들의 정보를 가지고 접근제어 - 128bit 대칭키 알고리듬을 이용하는 데이터 암호화 서비스 제공 - 프레임 무결성(frame integrity) 서비스 제공

3. 정보가전기기의 보안 취약점

내부망, 즉 유비쿼터스 홈 네트워크 환경을 고려하여 댁내 다양한 가전 및 A/V 장치들의 보안 취약점을 살펴보면 〈표 6〉과 같다.

Ⅳ. 구성요소별 보안 요구사항

유비쿼터스 홈 네트워크의 보안요소는 일반 통신 네트워크의 보안요소에서 기인하며 4대 요소[11]로는 정확성(authenticity), 제한성(access con-

〈표 6〉 댁내 가전 및 A/V 장치들의 보안 취약점

원인	취약점
공중망(인터넷)	바이러스나 웜에 노출 위험
통합 네트워크	통신선로 상의 데이터 보호 불가피
원격접속	데이터 및 기기의 손상 위험
홈 네트워크	해킹 및 불법행위로 사생활 침해 위험
멀티미디어	정보 가전기기에 저장된 데이터 보호 불가피
지불 시스템	데이터의 유출 및 변형에 따른 위험 존재 – 사용자 인증(authentication) – 프라이버시(privacy)

trol), 무결성(integrity), 기밀성(confidentiality) 등의 4가지가 있다. 각 보안요소별 특징을 살펴보면 다음과 같다.

1. 유비쿼터스 홈 네트워크 보안요소

• 정확성

사용자나 단말들을 인식하는 데 있어 아주 중요한 요소다. 사용자 인증에 있어서 가장 간단한 방법은 ID와 패스워드를 사용하는 방법이며, 두 가지 이상의 요소를 이용해 인증하는 방법(ClearText+Smart Card 등), PIN과 카드를 동시에 일치시키는 방법뿐만 아니라 토큰을 이용하는 방법 등 좀 더 강화된 인증방법들이 사용된다.

• 제한성

정확성의 연장에서 이뤄지는 요소로, 어떤 부분의 서비스를 위한 네트워크 접근 시도인지를 파악해 접근에 제한을 두는 방법이다. 방화벽이 바로 제한성을 이루는 데 필요한 장비 중 하나다. 네트워크 접속에 필요한 요소를 확인하면 장비, 애플리케이션, 프로토콜, 사용자, 사용자 그룹(서브넷)을 파악할 수 있으며, 권한까지도 쉽게 알 수 있다. 이를 이용해 비즈니스, 업무 환경 등을 종합해 보안 정책을 수립하며 접근을 제한한다.

• 무결성

원래의 데이터가 전송된 후에 어떻게 변경됐는지 등의 상태를 점검하는 것이다. 이는 비인가된 자에 의한 정보의 변경, 삭제, 생성 등으로부터 데이터를 보호해 정보의 정확성과 완전성 보장을 뜻하며 디지털 서명(digital signature)과 메시지의 정확성 확인 등은 이런 데이터의 무결성을 확인할 수 있는 기술이다.

• 기밀성

정보의 비밀이 어느 정도 보장될 수 있는가에 대한 부분이다. 전자우편을 예로 들면 완전한 텍스트 형식으로 전송되고 있기 때문에 보고자 한다면 그리 어렵지 않은 방법으로 확인할 수 있다. 그러나 전자우편에 아주 중요한 정보가 들어 있는 경우도 있기 때문에 이를 감추기 위해 암호화(scrambling)를 한다. 그럼으로써 복호화(unscrambling) 키가 있는 사용자만이 정보를 확인할 수 있게 된다. 이런 암호화/복호화 기술을 암호화(encryption)라고 말한다.

2. 구성요소별 보안 요구사항

앞서 살펴 본 4대 네트워크 보안요소는 유비쿼터스 홈 서버ㆍ게이트웨이에서 또한 고려되어야 한다. 부가적으로 홈 네트워크라는 환경은 일상 생활과 밀접하게 연관된 정보가전기기들에 내장되어야 하므

〈표 7〉 홈 네트워크 구성요소별 보안요구 사항

구성요소	요구 보안기능
홈 서버ㆍ게이트웨이	– 사용자 & 기기간 인증기능 – 접근제어기능 – 무결성 및 기밀성(인증 및 제어관련정보) – 디바이스 보안기능의 관리 – 보안정책관리기능 – 외부 보안서비스 연동기능 – 서비스 정보 댁내망 기밀성 – VPN 기능(IPSec VPN) – 네트워크 침입탐지기능(TCP wrappers) – 네트워크 침입차단기능(firewall) – 유해정보 차단 및 제공 콘텐츠 보호기능 – 서비스 정보에 대한 기밀성
댁내ㆍ외 네트워크 디바이스	– 사용자 인증 & 기기간 인증기능 – 접근제어기능 – 무결성 및 기밀성(인증 및 제어관련정보) – VPN 기능 – 서비스 정보에 대한 기밀성

로 경제적이고 높은 신뢰성을 제공해야 한다.

이와 동시에 침입을 실시간으로 차단할 수 있는 침입방지 시스템, 사용자/정보가전기기 인증 기술, 그리고 메시지/데이터 암호화 기술들이 유비쿼터스 홈 네트워크 환경으로의 효과적 적용이 요구된다.

홈 네트워크 구성요소별 보안요구 사항은 〈표 7〉에서 제시된 바와 같다.

부가적으로 최근 네트워크 환경은 이동성과 편리성, 보안성이 차지하는 부분이 점차 커짐에 따라 디렉토리 서비스(directory service)를 기반으로 각각의 조직과 사용자의 필요에 따라 네트워크 사용 권한을 부여하는 인증 중심의 통합 보안 솔루션 도입도 고려해야 할 것이다.

Ⅴ. 홈 네트워크 보안 기술

1. 홈 네트워크 보안 영역

홈 네트워크의 보안 영역은 크게 2계층 인증과 방화벽/액세스 컨트롤, VPN 등 세 개의 영역으로 나눌 수 있다. 2계층 인증은 네트워크를 이용하는 데 있어서 가장 기본적인 부분에서 인증(장비와 사용자에 대한 인증)을 요구해 내부적인 보안을 이룰 수 있는 방법이다. 방화벽/액세스 컨트롤은 내부 서버들이 접속하는 부분, 원격 사용자의 검색을 위해 보통 두 개 또는 그 이상의 방화벽을 설치해 목적에 맞게 동작을 구현시킨다. 한편 VPN은 회선 비용을 절감하기 위해 인터넷을 이용한 원거리 접속 솔루션이다. 이와 같은 기본 보안 영역을 고려한 홈 네트워크 보안 기술은 홈 서버·게이트웨이, 댁내·외부 홈 네트워크, 정보가전기기로 나누어져 통합적으로 개발 및 응용되어 유비쿼터스 홈 네트워크의 안정성을 보장해야 한다.

2. 홈 서버·게이트웨이 보안 기술

홈 서버·게이트웨이를 통해서 전달되는 사용자와 서비스 제공자의 정보가 부정한 사용자나 위험으로부터 보호되어야 하며, 동시에 사용자와 집안의 정보에 대한 프라이버시가 보호되어야 한다. 또한 침입, 해킹, 바이러스 등과 같은 외부 침입 행위에 대한 방어 기능도 필요하다.

• 정확성

홈 서버·게이트웨이에 접근하는 관리자 및 사용자의 신원을 확인하는 기능이다. 앞서 살펴본 바와 같이 기본적인 ID와 패스워드 기능뿐 아니라 지문, 손, 안면, 홍채 등 신체적 특성을 이용한 생체인식 장치가 점차 사용되고 있다.

• 기기 인증

정보가전기기의 연결이 발생하는 경우 부정한 정보가전기기인지를 확인하는 기능이다. PC 및 댁내 단말들의 인증은 네트워크를 사용하는 데 있어서 필요한 요소, 즉 스위치 포트, MAC 어드레스, IP 어드레스 프로토콜의 조합으로 네트워크 접속을 제한할 수 있다.

• 제한성

사용자가 외부로부터 홈 서버·게이트웨이나 댁내 망에 연결된 정보가전기기에 접근을 시도하는 경우 미리 정해진 접근권한 제어를 수행하는 기능이다. 접근제어는 서비스 및 사용자별로 제한을 두어 효과적으로 관리될 수 있다.

• 침입방지 기능

패킷 필터링, 침입과 해킹, 악성코드(웜, 바이러스, 트로이목마, 스크립트) 등과 같은 외부 침입에 대해 방어하는 기능이다. 방화벽의 활용은 비인가 패킷을 차단하고 악성코드의 침입 위험을 줄일 수 있으나 댁내망에 존재하는 무선랜 기반의 댁내 단말들과의 상호작용은 여전히 문제점으로 남아 있다. 대부분 무선 AP를 댁내 방화벽 내부에 두는 것은 바람직하지 않다.

• 무결성

홈 서버·게이트웨이상의 중요한 데이터나 댁내 외로 전송되는 데이터에 변경이 발생하는 경우 이를

확인하는 기능이다. Digital Signature나 Certificate Authority의 활용으로 무결성을 보장할 수 있으나 홈 네트워크라는 환경을 고려해 무결성 보장 기술들의 적절한 적용 및 활용이 요구된다.

• 기밀성

홈 게이트웨이를 통하여 전송되는 데이터가 인가되지 않은 사용자에게 노출되는 경우 그 내용이 알려지는 것을 방지하는 기술이다. 최근 고도화된 암호화 기술, 특히 1024/2048bit 기반의 AES나 Elliptic Curve 기술을 이용한 암호화를 사용하여 댁내·외 정보 및 데이터의 기밀성을 보장할 수 있다.

또한 모바일 환경에 대한 보안 기술로 홈 서버·게이트웨이는 다음과 같은 보안 대응책을 마련하여야 한다. ID/패스워드를 통한 기본적인 모바일 장비의 보안 및 DoS 공격, 바이러스나 웜, 코드나 설정 파일에 대한 보안을 고려해야 한다. 또한 댁내 모바일 장치에 대한 MAC/IP 주소 및 telnet에 대한 보안, 장비에 대한 접근 제한, RADIUS나 LDAP를 통한 사용자 접근 제한, 트래픽의 암호화(SSL, SSH, TLS) 등의 서비스를 제공해야 한다. 마지막으로 비상시를 위한 자동 복구 및 치유 기능도 고려되어야 할 것이다.

Ⅵ. 결론

본 문서에서는 신뢰성 있고 안전한 홈 네트워크 서비스를 제공하기 위하여 각 구성요소의 보안 취약성을 분석하였고, 이를 바탕으로 각 구성요소가 고려해야 하는 보안 요구사항들에 관하여 기술하였다.

홈 네트워크를 위한 정보보호 기술은 기밀성, 무결성, 인증, 접근제어, 가용성 등의 요구 사항을 충족시켜야 하는데, 이를 위해 침입방지, 사용자 및 정보가전기기 인증, 접근권한제어, 암호화 기술 등을 적용하여 홈 네트워크 구성요소들의 보안 요구사항을 기술하였다. 특히 유·무선랜 구간을 포함하여 홈 서버·게이트웨이의 통합적인 암호화 및 보안 알고리듬을 포함한 IPSec VPN은 유비쿼터스 홈 네트워크의 보안을 위한 보다 향상된 안전성을 제공하는 보안 도구가 될 것이다.

약어 정리

AES	Advanced Encryption System
AP	Access Point
CATV	Cable TV
CDN	Contents Delivery Network
DSL	Digital Subscriber Line
EPON	Ethernet Passive Optical Network
HNCP	Home Network Control Protocol
HomeF	Home Radio Frequency
HomePNA	Home Phoneline Networking Alliance
HRFWG	HomeRF Working Group
IrDA	Infrared Data Association
LDAP	Lightweight Directory Access Protocol
PIN	Personal Identification Number
PLC	Power Line Communication
RADIUS	Remote Authentication Dial-In User Service protocol
SDN	Service Delivery Network
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
UWB	Ultra Wide Band
WEP	Wired Equivalent Privacy

참 고 문 헌

[1] 서광현, “디지털홈 구축 정책방향,” *TTA Journal*, Vol.88, Aug. 2003, pp.20-29.
[2] 전호인, “디지털홈 기술 및 표준화 동향,” *TTA Journal*, Vol.88, Aug. 2003, pp.59-74.

[3] 박용우, “홈네트워킹,” 정보통신산업동향, Oct. 2001. p.305.
[4] 한국정보통신기술협회, “홈 게이트웨이 정보통신 표준,” 2001.
[5] 박광로, “디지털홈 포럼 최종 연구 보고서,” 한국 정보통신 기술 협회, Dec. 2003.
[6] 무선1394, http://www.1394ta.org
[7] 무선 홈 네트워크 기술, http://kidbs.itfind.or.kr:8888/WZIN/jugidong/1089/108901.htm
[8] K. Fujisawa, “RFC2855-DHCP for IEEE 1394,” IETF, 2000, http://www.ietf.org/rfc/rfc2855.txt?number=2855
[9] 홈RF, http://www.homerf.org
[10] Embedded Systems Programming, “Home Networking with Zigbee,” 2004, http://www.embedded.com/showArticle.jhtml?articleID=18902431
[11] CERT®Coordination Center,“Home Network Security,” Carnegie Mellon University. 2001, http://www.cert.org/tech_tips/home_networks.html
[12] Carl M. Ellison, “Home Network Security,” *Intel Technology Journal: Interoperable Home Infrastructure*, Vol.6, Issue 4, ISSN 1535-766x, Intel Co, Nov. 2002.
[13] Kim Thomas, “Building a Secure Home Network,” 2001, http://www.sans.org/rr/papers/index. php?id=611
[14] Samsung Economic Research Institute, http://www.seri.org
[15] 과학 기술부, “홈 네트워크 기술,” 2002, http://www.kdra.or.kr/sup/vision1-3.pdf
[16] Zigbee, http://www.zigbee.org
[17] Enterasys Networks, “무선랜 시장의 성장을 위한 표준 제정,” http://www.enterasys.com/kr/products/whitepapers/rf_0103.pdf
[18] 한국 알카텔, “효율성/안정성 보장하는 네트워크 보안 A to Z,” 2003.