주 제

홈네트워크 보안기술 동향

한국전자통신연구원 한종욱, 이덕규, 정교일

차 례

I. 서 론
II. 홈네트워크 기술 동향
III. 홈네트워크 보안기술 동향
IV. 보안요구사항
V. 결 론

요 약

홈네트워크는 기술의 통합적인 제공에 따라 높은 신뢰성이 필요하지만, 안전성이 확보되지 않는 홈서비스는 사용자로부터 외면을 받을 수 밖에 없고 더욱이 홈서비스에 따라 개인의 경제손실 뿐 아니라 개인정보의 도용으로 인해 생명까지도 위협받을 수도 있으므로 홈서비스 활성화에 있어 보안기술이 차지하는 중요성은 매우 크다고 할 수 있다.

본고에서는 안전한 홈네트워크 구축을 통하여 홈서비스가 활성화될 수 있도록 홈네트워크 구축시 고려되어야할 홈네트워크의 보안취약성 및 관련 보안기술 개발동향을 설명하고, 보안요구사항에 대해서 설명한다.

I. 서 론

홈네트워크 기술은 통신과 방송 융합, 유비쿼터스 사회로의 빠른 이동 등 IT 전반적인 환경에서 빠른 변화와 함께 사용자의 특성을 고려해야함으로, 다양한 분야의 기술들이 융합되어 IT 분야 통합과 같은 성격을 가지고 있다. 기간통신사업자를 축으로 기간망의 고도화로 시작된 네트워크 인프라는 이제 최후의 실핏줄인 홈네트워크로 발전하고 있으며, 홈네트워크 기술은 유선뿐 아니라 무선 부분에서도 급속한 발전을 이루고 있다. 이러한 홈네트워크가 발전하게 되는 가장 중요한 이유는 인터넷의 급격한 발전으로 이뤄지고 있으며, 현재, 초기에 비해 다양한 서비스는 물론 지능형 서비스를 통해 브로드밴드 서비스가 이뤄지고 있다. 그러나 인터넷을 기반으로 한 사이버 해킹공격은 급격히 증가하고 있어 국내 해킹 · 바이러

스 신고접수 건수는 2003년 26,179건에서 2004년 24,297건, 2005년 49,633건으로 인터넷 성숙단계의 진입과 동시에 폭발적으로 증가하여 전년도 대비 2005년 바이러스 피해는 줄어들고 있는 실정이나, 국내 해킹은 60% 이상증가하고 있다[1~3].

언제 어디서나 컴퓨팅이 가능한 유비쿼터스 컴퓨팅 사회에서는 개인의 컴퓨팅 환경 의존도가 증가함에 따라 사이버공격으로 인한 개인생활의 위협도 증가할 수밖에 없다. 더욱이 향후에는 헬스케어 서비스와 같이 개인의 생명과 직결된 홈서비스가 활성화될 것이므로 사이버공격으로 재산뿐 아니라 생명까지 위험에 처하는 경우가 늘어나게 될 것이다. 홈네트워크는 유비쿼터스 컴퓨팅 환경으로 가는 시작점이라고 할 수 있으므로, 인터넷을 통한 사이버 공격의 급증은 눈앞에 현실로 다가오고 있는 홈네트워크의 활성화를 방해하는 장애물로 대두될 것이 틀림이 없으므로 이에 대한 대응책 마련이 시급하다고 할 수 있다.

따라서 본 고에서는 안전한 홈네트워크 구축을 통하여 홈서비스가 활성화될 수 있도록 홈네트워크 구축시 고려되어야할 홈네트워크의 보안취약성 및 관련 보안기술 개발동향을 살펴보고, 보안요구사항에 대하여 기술한다.

II. 홈네트워크 기술 동향

홈네트워크의 기본 개념은 집안의 정보가전기기를 네트워크로 묶고 이를 외부의 인터넷 망과도 연결하여 집 내부 및 외부 어디서나 사용자의 위치에 관계없이 정보가전기기를 제어할 수 있도록 하고 각종 편의를 위한 홈서비스를 제공하겠다는 것이다.

홈네트워크 기술은 크게 4개의 중점 기술로 분류될 수 있다. 이중에서 홈 플랫폼 기술은 외부망과 가정을 연결하고 가정내 다양한 서비스를 제공하여 유무선 통합 홈네트워크 환경 및 고품질의 융합서비스를 가능케하는 홈서버/게이트웨이, 홈네트워크 보안 및 개방형 서버 기술로 구성된다. 우선 홈플랫폼 기술은 외부 인터넷과 연결을 위한 가입자망으로 xDSL, Cable, FTTH(Fiber To The Home), PLC (Power Line Communication), IEEE802.11 등 다양한 유·무선망의 사용이 가능하다. 홈네트워크는 적용 대상에 따라 여러대의 PC 및 컴퓨터 관련 장비간의 통신을 위한 정보 네트워크, 가전장비 제어를 위한 자동화 네트워크, 음향 및 영상기기나 게임기 등의 오락 또는 문화생활을 위한 엔터테인먼트 네트워크 등 3가지 네트워크로 나눌 수 있다[11].

정보 네트워크는 컴퓨터 및 그 관련 장비간의 통신을 위한 네트워크로 블루투스, 무선랜, HomeRF (Home Radio Frequency) 등을 이용한 무선통신과 이더넷, 전화선 (HomePNA : Home Phoneline Networking Alliance), 전력선(PLC : Power Line Communication) 등을 이용한 유선통신으로 구성이 가능하다. 장비 제어를 위한 미들웨어로는 마이크로소프트 진영이 중심이 되어 TCP/IP 프로토콜을 활용한 UPnP(Universal Plug and Play)와 자바 진영이 중심이 된 Jini라는 프로토콜이 있다. 자동화 네트워크는 보안장비, 조명, 환기, 에어컨 등의 가전장비 제어를 위한 네트워크로서 2Mbps 이하의 저속의 통신으로 가능하며, 주로 전력선을 활용하여 통신을 한다. 여기에는 LonWorks, HnCP(Home Network Control Protocol) 등의 미들웨어가 이용되고 있다. 엔터테인먼트 네트워크는 가전장비나 음향 및 영상기기 (TV, VTR, DVD Player, Audio, 게임기 등)에 적용되며, 100-400Mbps 정도의 고속으로 동영상이나 음악, 게임 등을 실시간으로 전송하는 네트워크이다. 여기에는 UPnP AV나 HAVi(Home Audio Video interoperability)라는 음향 및 영상 장비간의 통신 및 제어를 위한 미들웨어가 사용 가능하다. 대부

분의 가정에서는 이러한 3가지 네트워크 모두를 필요로 하므로 백색가전기기, 컴퓨터 관련 장비, 음향 및 영상 장비 등을 효과적으로 엮을 수 있도록 다양한 네트워크 및 미들웨어들을 브릿지할 수 있는 홈게이트웨이를 개발하고 있으며, ETRI에서는 다양한 미들웨어간의 연동을 가능하게 해주는 통합미들웨어를 개발하고 있다.

<표 1>은 홈네트워크 기술에 대한 분류를 나타내었다.

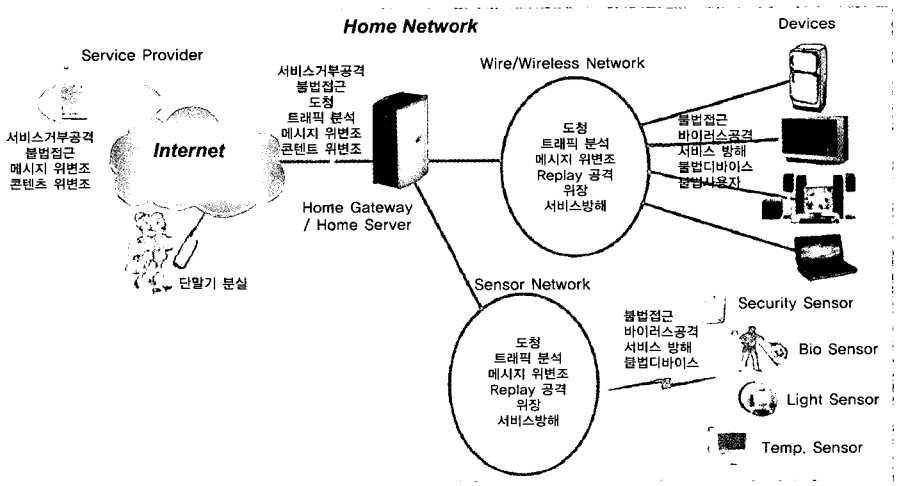
〈표 1〉 홈네트워크 기술 분류

대분류	중분류	소분류
홈네트워크 기술	홈 플랫폼 기술	홈서버/홈게이트에이 기술
		홈네트워크 보안
		개방형 서버 기술
	유/무선 홈네트워킹 기술	유선 홈네트워킹 기술(Ethernet, PLC, IEEE 1394)
		무선 홈네트워킹 기술(WLAN (802.11a/b/g/n), WPAN(UWB, Zigbee)
	정보가전 기술	지능형 정보가전
		홈센서 기술(RFID, 센서)
	지능형미들웨어 기술	홈네트워킹 미들웨어 기술
		상황적응형 미들웨어 기술
		멀티 모달 인터페이스 기술

III. 홈네트워크 보안기술 동향

3.1. 홈네트워크 보안취약성

홈네트워크에서는 다양한 유?무선 네트워크와 프로토콜 등의 혼재로 기존 인터넷 등에서 발생되던 보안취약성외에도 추가적으로 고려해야할 보안취약성이 존재하고 있다. 즉, 홈네트워크의 모든 정보기기들은 인터넷과의 연결로 다양한 사이버공격의 대상이 될 수 있으며, 홈네트워크내의 정보기기의 다양성과 기기간 자원의 공유 등으로 보안측면에서 고려해야할 요구사항은 더욱 복잡하고 다양한 특성을 지니게 된다. 더욱이 홈네트워크의 정보가전기기들은 상대적으로 컴퓨팅 능력이 낮아 강력한 보안기능의 탑재가 어려우므로 사이버공격에 이용되거나 목표가 될 가능성이 더욱 높다고 할 수 있다. 홈네트워크에는 Ethernet, HomePNA, PLC, IEEE 802.1x, Bluetooth, UWB(Ultra Wide Band) 등 다양한 홈네트워킹 기술이 사용 가능하나 홈네트워크 측면에서 매체의 보안취약성을 해결할 수 있는 대응기술을



(그림 1) 홈네트워크의 보안취약점

갖고 있지 못하며, 미들웨어의 경우에도, 각 미들웨어들이 요구하는 보안기능을 모두 만족할 수 있고 개별 미들웨어를 통합한 통합미들웨어 환경에서도 유연하게 보안기능을 제공할 수 있는 보안인프라가 아직 개발되지 못하고 있다.

(그림 1)은 홈네트워크에서 발생될 수 있는 보안 취약성을 정리한 것이다. 인터넷 등에서 발생되던 취약성이 홈네트워크 내부망에서도 그대로 발생됨을 알 수 있으며, 내부망의 복잡함을 고려할 때 우선적으로 종합적인 보안프레임워크를 정립하는 것이 필요하겠다.

홈네트워크에서 디바이스가 가져야할 보안 취약성은 이동성(Mobility), 개체인증, 동일 개체 인증, 데이터 발신처 인증, 접속/비접속 기밀성 등이 있다. 이와 같은 사항에 대해 각 디바이스의 보안이 유지되지 못한다면, 사용자의 정보가 유용될 소지를 가지고 있으며, 이와 같은 문제점은 아래의 사항과 연결하여 생각해 볼 수 있다.

홈네트워크에서는 헬쓰케어 서비스와 같이 생명과 직결된 바이탈신호들의 사용이 증가할 것으로 생각되고 있으며, 더욱이 생체정보를 이용한 사용자 확인으로 사용자에게 최적의 자동화된 홈서비스가 제공될 것이므로 주요 생체정보에 대한 노출이나 위변조를 통한 공격에 대비할 수 있는 보안기술개발이 필요하겠다. 또한 개인의 행동특성이나 생활습관에 관련된 정보를 불법적으로 수집, 분석함으로써 개인에 대한 새로운 프라이버시 침해 가능성도 높다고 할 수 있다.

3.2. 홈네트워크 보안기술 동향

홈네트워크는 인터넷과의 연결로 인하여 인터넷에서 발생되고 있는 다양한 사이버공격에 그대로 노출되어 있어 해킹, 악성코드, 웜 및 바이러스, DoS (Denial of Service) 공격, 통신망 도 · 감청 등에 보안취약성을 갖고 있다. 따라서 인터넷을 통한 사이버 공격에 대응하기 위해서 대부분의 보안기능을 홈게이트웨이에 집중, 구현하여 안전성을 강화하는 형태로 기술개발이 이루어지고 있다. 현재까지 보안기능이 탑재된 다양한 상용 홈게이트웨이 제품이 개발되어 시판되고 있다. 홈게이트웨이는 댁외의 공중망과 댁내의 홈네트워크를 연결하는 입구로서 외부의 불법 침입에 대해 일차적인 대응 방안을 제공한다는 개념에서 최우선적으로 보안기능이 탑재되고 있으며, 홈게이트웨이에 탑재된 대표적인 보안기능에는 Firewall, VPN(Virtual Private Network) 등이 있다.

표 2는 현재까지 개발 및 상용화된 보안기능이 제공되는 홈게이트 제품 현황을 나타낸 것이다. 국외 제품의 경우, 대부분이 미국제품으로 보안측면에서 제공되는 기능은 Firewall, VPN 등으로 대부분이 제한적인 유사한 보안기능만을 제공하고 있다.

〈표 2〉 홈게이트웨이 보안제품 현황

구 분	업 체 명
국내	ETRI, 알피에이네트웍스, 시큐베이, 디지스타, 지맥스테크놀로지, 기가링크
국외	Wipro, HotHardWare, FutureSoft, 2wire, linksys,3com, 3eti, MaxGate, D-Link

안전한 홈서비스 제공을 위해서는 홈네트워크 구성요소에 대한 접근제어 및 이를 위한 인증기능이 필요하게 된다 따라서 홈게이트웨이 보안제품외에 홈네트워크 자원에 대한 접근제어 및 인증기능 등이 제공되는 기술 및 제품들이 국내외에서 개발되고 있다.

<표 3>은 현재까지 개발되었거나 개발 중인 주요 홈네트워크 보안기술 개발 현황이다.

홈게이트웨이와 정보가전기기간의 제어를 위해 필요한 미들웨어들에서도 기본적인 보안기능이 제공되고 있으며, 관련 보안기능에 대한 표준화도 이루어지고 있다. 주요 미들웨어별 세부적인 보안기능에 대

〈표 3〉 주요 홈네트워크 보안기술 개발 현황

구분	업체명	관련 보안기능 개발현황
국내	ETRI	• 홈서비스 사업자가 요구하는 인증수단과 상이한 사용자가 원하는 인증수단을 사용해서도 인증을 받을 수 있게 하는 편의성이 강화된 안전한 통합인증기술 개발 • 홈네트워크에 적합하고 편의성이 강화된 보안정책 기반의 경량화된 접근제어기술개발 • 홈디바이스 환경에 적합한 경량화되고 편의성이 강화된 멀티홈 도메인용 디바이스 인증 · 인가 기술 개발
	안랩유비웨어	• 홈네트워크 자원에 대한 원격접근을 위한 PKI 기반의 홈네트워크 인증, 인가보안솔루션을 개발
	이니텍	• 디지털 방송을 위한 PKI 기반의 홈네트워크 보안 솔루션 개발
	소프트포럼	• 셋톱박스용 PKI 기반의 사용자 인증기술 및 암호기술개발
국외	MicroSoft	• PC를 홈 엔터테인먼트의 중심으로 설정하여 디지털 서비스를 제공하는 e-Home을 추진 중 • PC 접근을 위해 비밀번호 또는 지문 인식을 통한 사용자 인증을 연구
	CablesLabs	• 북 · 남미 케이블회사들로 구성된 CablesLabs에서 CableHome이라는 표준을 추진 중 • 홈게이트웨이의 장치 인증, 컨트롤 데이터 및 다운로드 소프트웨어의 암호화 제공, 원격 홈게이트웨이의 Firewall 기능 등을 지원
	NTT	• 일본 NTT 데이터, 후지쯔, 미쯔비시, 도쿄공업대 등에서 개인키를 포함한 스마트카드를 이용하여 원격지에서 홈네트워크를 관리하는 기술에 대해 연구 중

해서는 <표 4>에 정리하였다[5~9].

〈표 4〉 주요 홈네트워크 미들웨어별 보안기능

미들웨어	제공 보안기능 현황
UPnP	Ver 1.0에서는 보안기능이 정의되어 있지 않음 Ver 2.0에서 보안기능이 추가될 예정임 - 제품 인증기능 제공 - 기기간 인증기능 제공 - 접근제어를 위한 Device가 자체적인 ACL 제공 - 기밀성 제공
Jini	Ver 1.0의 보안기능은 Java Security에 의존 - 사용자 인증 기능 제공 - 기기간 인증 기능 제공 - 메시지 무결성 및 기밀성 제공 - 접근제어 기능 제공 Ver 2.0에서 추가적으로 상호인증, 인가기능, 코드 무결성 등에 대한 기능이 강화됨
Havi	Havi 인증서를 이용한 인증기능 제공 접근제어 기능 제공
LoneWorks	기기간 인증기능 제공
HNCP	보안기능 정의 안되어 있음 (Ver 1.0)
OSGi	다양한 플랫폼 지원 표준화에서 보안을 제공을 위한 워킹그룹 운영

3.3. 홈네트워크 보안기술표준화 동향

현재 홈네트워크 서비스 산업은 시장 형성을 위한 초기 단계로 국내외를 막론하고 모든 사용자들이 널리 이용할 수 있는 표준화된 보안기술이 없는 실정이다. 각 가전 제조사나 홈네트워크 서비스 업체들은 저마다의 기술을 이용하여, 이종의 유무선 네트워크상에서 홈오토메이션과 같은 제한된 홈서비스 및 홈기기 개발에 초점을 맞추고 있다. 이런 이유로 홈네트워크를 구성하기 위한 기술이나 보안을 적용하는 방법은 각 기술 간에 많은 차이를 가지며 이러한 점은 홈네트워크 산업의 활성화에 큰 장애물로 작용하고 있다. 국내에서는 SKT와 KT를 중심으로 홈네트워크 시범서비스를 위한 컨소시엄을 구성하고 있으며, 실제 정보보호 대책은 사용자의 아이디와 패스워드를 이용한 단순한 인증 방식에 그치고 있다.

따라서 통일된 홈네트워크 모델이 없는 상황에서 적용되는 다양한 네트워크나 미들웨어에 따라서 제공 가능한 보안기술도 상이할 수 밖에 없으므로 표준화 관점에서 우선적으로 종합적인 보안요구사항을 정의하고 이를 반영한 보안프레임워크 모델 표준화를 추진하고 있다.

국내 표준화의 경우, ETRI가 제안한 홈네트워크 사용자 인증메커니즘이 2005년 1월 홈네트워크시큐리티포럼의 사실표준으로 채택되었고, 2005년 12월 TTA 국내표준으로 제정되었다. 그리고 홈네트워크 접근제어기술에 대한 표준화를 위해 ETRI에서 개발한 보안정책 언어에 대한 표준안이 TTA와 홈네트워크시큐리티포럼에서 심의 중에 있다.

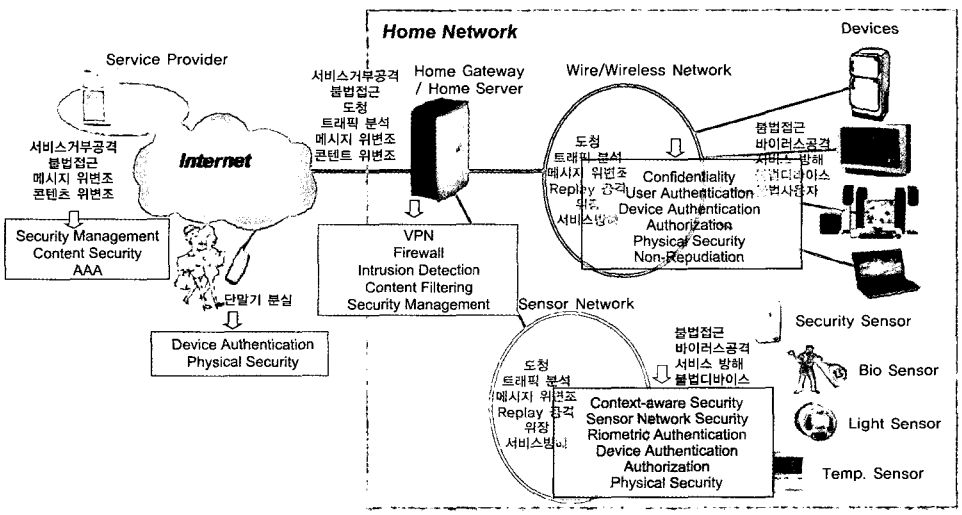
국제 표준화의 경우는, ITU-T SG17의 Q.9에서 추진되고 있으며 ETRI에서 제출한 홈네트워크 서비스의 사용자 인증 메커니즘(Xhomesec-3)외에 보안프레임워크(Xhomesec-1), 홈네트워크 서비스의 디바이스 인증서 프로파일(Xhomesec-2) 등 총 3개의 표준화 프로젝트가 진행되고 있다. 특히 스위스 제네바에서 열린 ITU-T SG17 10월 회의에서는 상기 3개 프로젝트의 향후 계획에 대한 협의가 있었으며, Xhomesec-1의 첫 드래프트 표준을 2006년 4분기에, Xhomesec-2의 첫 드래프트 표준을 2007년 4분기, Xhomesec-3의 첫 드래프트 표준을 2007년 4분기까지 만들기로 결정되었다.

최종 드래프트가 만들어지는 것은 통상 첫 드래프트가 만들어진 시점으로부터 약 1년 이상이 소요되므로, 내년 4월에 ITU-T SG17회의가 한국에서 열리기로 결정된 만큼 국제 표준화를 위한 좀 더 적극적인 노력이 수행된다면 홈네트워크 보안 분야에서 국제표준을 선도할 수 있는 좋은 결과를 기대할 수 있을 것이다.

IV. 보안요구사항

4.1. 보안프레임워크

홈네트워크에서는 이기종의 유무선 네트워크와 다양한 프로토콜 등의 혼재로 기존 인터넷 등에서 발생되던 보안취약성 외에도 추가적으로 고려해야할 보안취약성이 많이 존재한다. 홈네트워크의 다양한 정보가전기기들은 인터넷과의 연결로 사이버공격의 대상이 될 수 있으며, 더욱이 홈네트워크내의 정보기기의 다양성과 기기간 자원의 공유 등으로 보안측면에서 고려해야할 보안요구사항은 더욱 복잡해지고 다양화되고 있다. 또한, Ethernet, HomePNA, IEEE1394, PLC, IEEE 802.1x, Bluetooth, UWB 등 다양한 홈네트워킹 기술이 활용될 것으로 예상되고 있으나 대부분은 보안취약성에 대한 대응기술이 아직 개발되지 못하고 있으며, 무선랜의 경우와 같이 제공되는 기술의 경우도 아직 취약성을 갖고 있는 등, 각 네트워킹기술에서 발생될 수 있는 다양한 보안취약성이 문제가 될 수 있다.

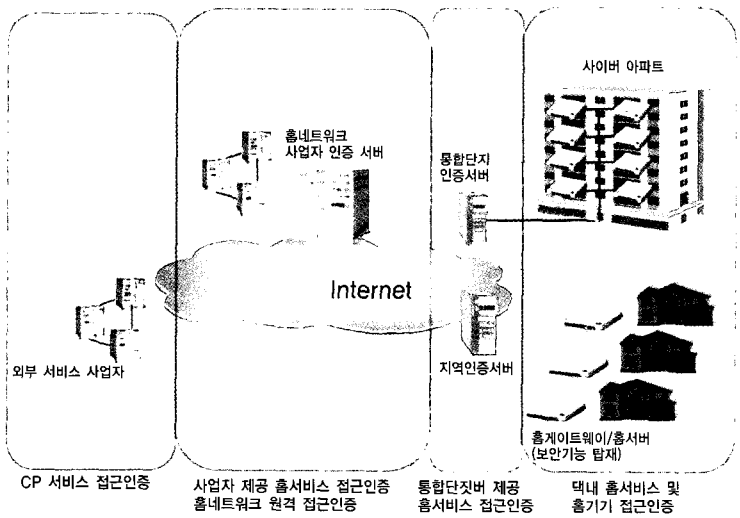


(그림 2) 홈네트워크 보안취약성 대응을 위한 보안기능

(그림 2)는 홈네트워크에서 발생될 수 있는 보안 취약성을 해결하기 위해 적용 가능한 보안기능을 정리한 그림이다. 하지만 국내 홈네트워크의 경우는 사이버아파트의 경우와 같이 밀도가 높은 네트워크 환경을 갖고 있으며, 구성되는 홈디바이스가 상대적으로 저성능, 경량화된 디바이스들이므로 기존의 보안기술을 그대로 적용하기에는 무리가 따를 수 있다.

따라서 홈네트워크를 구성하는 다양한 통신매체나 프로토콜 등에 독립적으로 적용할 수 있는 홈네트워크 환경에 적합한 보안프레임워크를 우선적으로 정립되어야 하겠다. 또한, 홈네트워크의 발전전망을 고려하여 현재 추진 중인 시범서비스에서 연동될 수 있는 수준의 보안기술과 향후 유비쿼터스 컴퓨팅 환경에 근접한 홈네트워크 모델에서 활용될 수 있는 보안기술을 모두를 고려한 단계적인 홈네트워크 보안 프레임워크를 연구해야 한다.

(그림 3)은 홈네트워크 시범서비스 사업모델의 인증기능을 고려하여 보안프레임워크를 정립하는 경우를 설명하는 그림이다. 홈네트워크 환경에서 발생될 수 있는 인증서비스는 크게 댁외 인증서비스와 댁내 인증서비스로 구분할 수 있다. 댁외 인증 서비스는 홈서비스 사업자나 ISP망을 통해 원격으로 댁내 홈네트워크 자원에 접근하는 접근인증, 외부 컨텐츠사업자가 제공하는 서비스를 사용하기 위한 접근인증, 인터넷 서비스를 받기 위한 가입자 인증 등이 있을 수 있다. 댁내 인증서비스에는 댁내에서 홈기기나 홈서비스의 사용을 위해 요구되는 접근인증이 있다. 댁외 인증서비스는 아파트단지를 관리하는 단지서버나 지역별 홈네트워크를 통합 관리하는 지역서버에서 이루어지는 인증서비스, 홈서비스 사업자나 ISP가 제공하는 인증서비스, 서비스 사업자가 제공하는 인증서비스 등으로 다시 세분할 수 있다. (그림 3)에서와 같이 해당 영역마다 관리주체에 따라 역할이 분담되어 사용자 인증이 이루어질 수 있다. 현재 시범서비스에서는 댁내외 인증기능이 사업자 인증서버로 집중되어 있어 사용자 프라이버시 문제가 발생될 소지가 많다고 할 수 있다.



(그림 3) 홈네트워크 인증모델

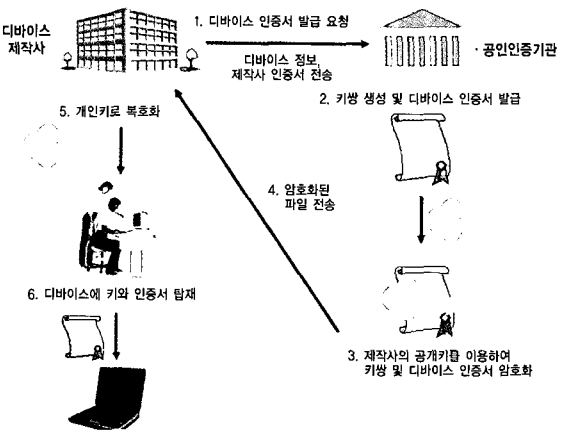
따라서 홈네트워크 인증모델에서 최우선적으로 고려해야할 부분은 인증을 받기 위해 필요한 사용자 인증정보를 누가 갖고 있느냐이다. 향후에는 상황인지기반의 사용자 인증서비스의 활용이 증가할 것으로 예상되고 있으며, 노인 등과 같은 홈구성원의 특성상 생체기반의 사용자 인증기술의 필요성이 더욱 증가할 것이다. 따라서 생체인증기술은 다른 사용자 인증기술에 비해 생체정보의 특성상 노출로 인한 피해정도가 매우 크다고 할 수 있으므로 안전성 확보가 필수적으로 요구되는 생체인증기술에 대해서는 외부 사업자가 생체인증정보를 갖지 않고 댁내망에서 집적 관리하는 방향으로 인증서비스가 이루어져야 할 것이다. 물론 댁내에서 인증정보 관리를 위해서는 사용자 개입을 최소화한 관리기술의 지원이 필요하며, 인증정보 보호를 위한 안전성 확보방안이 우선적으로 개발되어야 한다.

4.2. 디바이스 인증

불법 디바이스의 사용을 방지하지 위해서는 홈네트워크의 구성요소인 디바이스 자체에 대한 인증과정이 필요하다. 현재까지 디바이스 인증은 미들웨어 레벨에서 제공되고 있다. UPnP의 경우, 디바이스 마다 부여된 Security ID로 디바이스의 홈네트워크 등록과정에서 디바이스 인증이 이루어지고 있으며, Havi의 경우에는 디바이스마다 고유한 인증서를 발행하여 디바이스 인증 수행시 사용하고 있다.

(그림 4)는 디바이스 인증서 발급과정의 예를 설명한 그림이다.

디바이스 유효성 확인을 위한 시리얼 넘버나 인증서 등은 개별 제조업체 등에서 자체적으로 발행하고 있어 향후 디바이스에 대한 다양한 사후 서비스 제공이나 유비쿼터스 컴퓨팅 환경에서 디바이스 및 사용자 인증 기능과 결합한 새로운 서비스의 제공을 위해



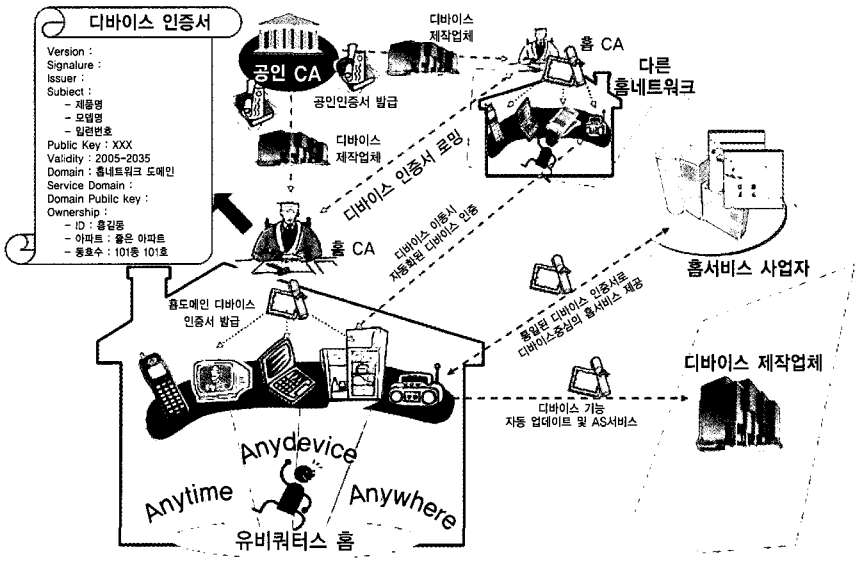
(그림 4) 디바이스 인증서 발급과정

서는 디바이스 인증정보에 대한 통일된 발급체계 및 관리체계에 대한 기술적, 정책적인 연구가 필요하다.

향후, 홈네트워크 서비스는 디바이스간의 협업을 통해 디바이스가 서비스의 주체가 되어 디바이스들이 판단하여 사용자 상황에 맞는 최적의 서비스를 제공하는 형태로 진화할 것이다. 또한 홈네트워크는 유비쿼터스 서비스의 한 도메인으로서 홈네트워크간에, 홈네트워크와 사이버오피스간에, 홈네트워트와 텔래메틱스 도메인간에 다양한 서비스 도메인간의 seamless한 홈서비스를 제공하게 될 것이다. 따라서 향후에는 홈디바이스간의 신뢰관계 구축이 매우 중요한 보안이슈가 될 것이며, 현재 (그림 5)와 같이 PKI기술을 기반으로한 싱글 도메인 인증기술이 아닌 서비스 도메인간의 인증기능 로밍이 가능한 멀티도메인 인증기술이 요구될 것이다.

4.3. 사용자 인증

홈네트워크에서는 디바이스 인증 외에 디바이스를 사용하는 사람의 신원확인을 위한 사용자 인증기능도 반드시 필요하다. 홈네트워크에는 생체인식, 패



(그림 5) 디바이스 인증서 개념

스워드, 인증서, 스마트카드 등 다양한 사용자 인증기술의 활용이 가능하겠지만, 유비쿼터스 컴퓨팅 환경으로의 진화를 고려할 때 정보단말기기의 낮은 성능을 고려한 사용자 인증기술의 활용 및 적용성이 검토되어야 하며, 사용자 편의성을 고려하여 더욱 편리한 생체 중심의 사용자 인증수단에 대한 기술개발도 요구된다. 홈네트워크 사용자 인증기술은 댁내뿐 아니라 댁외에서도 홈네트워크 자원에 대한 원격 접근을 위해 필요하며, 댁내에서 인터넷뱅킹과 같은 서비스 사업자가 제공하는 서비스를 사용하기 위해서도 필요하다. 따라서 기존의 다양한 사용자 인증기술을 수용할 수 있는 종합적인 사용자 인증 인프라기술 개념으로 개발되어야 한다.

홈네트워크에서는 구성원의 의지에 따라 사용자 인증을 요청하는 경우도 있지만, 구성원 의지와 관계없이 구성원 상황에 따라 사용자가 인증이 되어 구성원에 적합한 서비스가 제공되는 경우도 예상할 수 있다. 그러므로 기존의 사용자 인증기술 외에 향후 홈서비스에 적합한 새로운 사용자 인증기술도 필요하게 될 것이다. 예를 들어, RFID 태그 기반의 사용자 인증기술의 활용 가능성이 높아지고 있으므로 유비쿼터스 컴퓨팅 환경에 적합한 새로운 사용자 인증기술에 대한 연구가 필요하겠다.

또한, 인증정보의 안전성 확보를 위해서 댁내외 인증정보가 분리되어 관리되어야 하므로 댁내에서 댁외의 인증서비스를 받기 위해서는 댁내에서 사용되는 다양한 인증기능이 댁외 사업자가 제공하는 인증기능과 연동될 수 있도록 하는 정합환경의 개발이 필요하다.

4.4. 접근제어

홈서비스에 따라 홈네트워크 자원에 대한 접근권한 제어 기능이 요구된다. 홈구성원별로 제공받을 수 있는 홈서비스의 종류가 다르고 홈네트워크 구성요소에 대한 제어 범위도 다르므로 이에 대한 접근제어

기능이 필요하다. 유비쿼터스 컴퓨팅 환경을 고려할 때 접근제어를 위한 ACL은 단말기기가 내장하고 있는 것이 효율적이라고 할 수 있지만 안전성 측면이나 사용자 편리성 측면에서 일관된 보안정책따라 접근권한이 제어되어야 하므로 홈게이트웨이에서 종합적으로 관리하는 방안에 대해서도 검토가 필요하겠다. 또한, 인증 정보 유출로 인한 불법적인 접근시도가 발생한 경우, 보안정책을 능동적으로 변경하여 공격에 대응하는 보안기능에 대해서도 연구가 필요하겠다. 미들웨어별로 ACL 관련 정책 및 구현기술이 다르므로 미들웨어별 접근제어 정책을 종합 관리할 수 있는 기술에 대해서도 검토가 필요하다.

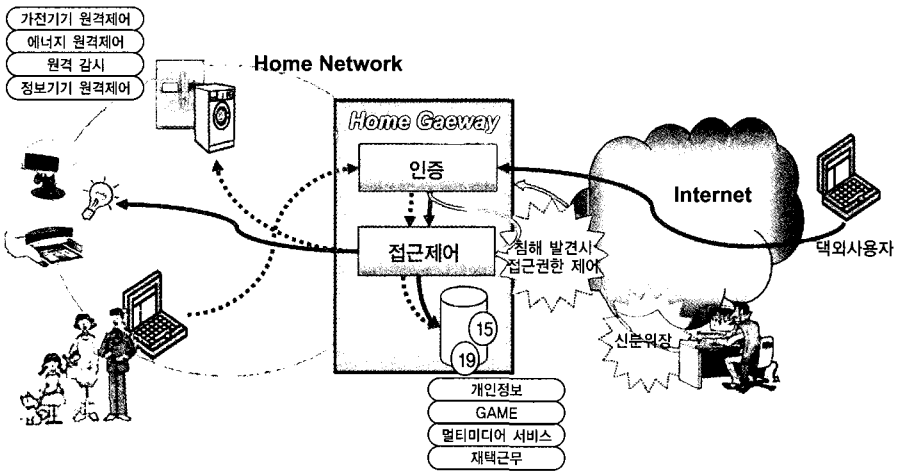
(그림 6)은 홈네트워크 환경에 적용할 수 있는 ETRI에서 개발한 접근제어서비스를 설명하는 그림이다. 홈구성원의 역할에 따라 권한을 정의하여 홈서비스 및 홈기기에 대한 홈구성원별 접근제어 서비스를 제공하도록 하였다. 비 IT 사용자도 간단하고 편리하게 보안정책을 수립, 변경할 수 있도록 개발하였으며, 개별 홈네트워크 뿐 아니라 단지내 서버차원에서 사용할 수 있도록 확장가능한 형태로 개발하였다.

4.5. 미들웨어 보안기능

<표 4>에 기술한 것과 같이 하나의 홈네트워크를 구성하는 경우에도 여러 가지의 다양한 미들웨어가 사용되고 미들웨어별로 제공되는 보안기능도 다르고 구현방법도 상이하므로 보안측면에서 고려해야할 부분이 많다고 할 수 있다. 다양한 미들웨어간 연동을 위해 ETRI 디지털홈연구단에서 개발한 통합미들웨어와 연동될 수 있는 사용자 인증 및 접근제어 기능을 ETRI 정보보호연구단에서 개발하였다. 하지만 궁극적으로는 홈서비스에 대한 보안기능은 미들웨어 레벨에서 적용되는 형태가 가장 효율적이라고 생각되므로 향후 차세대 미들웨어 개발시 보안기능에 대한 개발도 동시에 이루어져야 하겠다.

4.6. 기 타

홈네트워크 환경에 적합한 경량화된 암호 알고리즘 및 인증 프로토콜이 안전성 측면보다는 효과적인 홈서비스 제공을 위해 우선적으로 개발이 필요한 보



(그림 6) 홈네트워크 접근제어기능 개념

안기능이라고 할 수 있다. 그밖에 홈게이트웨이에서의 침입에 대한 대응기능 및 VPN서비스의 고도화도 필요하며, End-to-End 보안서비스를 위해 정보가전기기에서의 기밀성 제공 기능도 개발이 필요하겠다. 외부 스팸메일이나 불법적인 컨텐츠로부터 홈구성원 특히, 아이들을 보호할 수 있는 보안기능의 개발도 필요하다.

또한 홈네트워크에서의 사용자 정보를 가지고 있는 디바이스의 보안도 중요하게 다뤄야할 문제로써 다음의 4가지에 대한 요구사항은 중요하다고 할 수 있다.

개체 인증은 사용자 자신의 디바이스를 이용하여 멀티홈 도메인으로 이동하더라도 이동한 멀티홈 도메인에서 인증을 받을 수 있어야 하며, 동일 개체 인증은 멀티홈 도메인내에 다른 디바이스가 위치해 있더라도 이동하기전의 사용자 정보로 인증이 가능해야한다. 이와 같은 인증은 다양한 등급의 보호기능을 제공할 수 있다. 데이터 발신처 인증은 동일한 멀티홈 도메인에서 사용자 정보를 제공할 때, 전송되어온 사용자 정보가 올바른 디바이스에 전송되었음을 확인하여야한다. 마지막으로 접속/비접속 기밀성은 접속 혹은 비접속 상태라 할지라도 사용자의 정보는 안전하게 보호, 전송되어야함을 의미한다.

V. 결 론

우리나라는 세계수준의 네트워크 인프라와 전자/반도체 기술등이 있으므로 PC 보급과 광대역 통신과 같은 인프라 보급이 뒷받침 된다면 홈네트워크 수요가 활성화 될 것이다. 또한, 정보통신부에서는 "디지털 라이프 실현을 위한 디지털 홈 구축계획"을 발표하면서 가정을 누구나 기기 시간 장소에 구애받지 않고 다양한 홈서비스를 제공받을 수 있는 디지털 생활공간으로 전환하고, 2007년까지 천만가구에 디지털 홈 구현을 위한 홈네트워크를 구축할 것이라는 비젼을 제시했다. 산업자원부 역시 차세대 신성장동력 발굴을 위해 차세대 성장엔진으로 "스마트 홈"산업을 선정하여 집중 육성하고 있다. 또한, "디지털홈" 사업의 활성화를 위해 KT와 SK텔레콤이 주축이 된 양대 컨소시엄을 통해 시범사업을 전개하고 있다. 유비쿼터스 컴퓨팅 환경 구현을 통해 창출될 시장규모가 580조원을 상회할 것이라는 노무라종합연구소의 연구보고서만 보아도 유비쿼터스 컴퓨팅 환경의 시작점으로 인식되고 있는 홈네트워크가 가져올 기대효과는 엄청날 수 있다고 생각되며, 정부의 홈네트워크 시장 육성의지와 맞물려 관련 업체들이 적극적으로 시장에 참여하고 있어 신성장동력으로서 홈네트워크 시장에 대한 기대감은 매우 높다고 할 수 있다.

이상과 같은 정부의 산업육성정책과 산업체들의 적극적인 시장참여로 홈네트워크 분야 활성화를 통한 경제적, 사회적 기대가 높아만 가고 있지만, 안전성이 확보되지 않는 홈서비스는 사용자로부터 외면을 받을 수 밖에 없고 더욱이 홈서비스에 따라 개인의 경제손실 뿐 아니라 생명까지도 위협받을 수도 있으므로 홈서비스 활성화에 있어 보안기술이 차지하는 중요성은 매우 크다고 할 수 있다.

따라서 본 고에서 정의한 홈네트워크 보안프레임워크부터 세부 보안기능 등에 대한 요구사항 등을 모두 반영한 홈네트워크 기술을 개발한다면 홈네트워크 분야를 통해 예상되고 있는 세계시장 선점을 통한 경제적 기대효과 및 미래 지향의 가정환경 구현이 가능해지리라 생각된다.

[참 고 문 헌]

[1] 박광로, 송영준, "홈네트워킹", TTA저널, 제

78호, pp.101-109, 2001.
[2] 전호인, "디지털홈기술 및 표준화동향", TTA 저널, 제88호, pp.59-73, 2003.
[3] 윤철, "최근의 홈네트워크 기술동향 및 시장전망", 주간기술동향, 제1098호, pp.22-33, 2003.
[4] Carl M.Ellison, "Interoperable Home Infrastructure Home Network Security." Intel Technology Journal, Vol 6., pp.37-48, 2002.
[5] www.jini.org
[6] www.upnp.org
[7] www.echelon.com
[8] www.havi.org
[9] "Home Network Control Protocol(HNCP) Prespec. Ver. 1.5", PLC 포럼 디지털 가전위원회, 2003.
[10] 박광로, "IT839 전략 표준화: 홈네트워크", TTA저널, pp78-84, 2005.
[11] 서대영, "표준기술동향: 홈네트워크를 위한 Open Services Framework", TTA저널, pp98-106, 2005.

한종욱

1985년 광운대학교 공과대학 전자공학과 공학사
1991년 광운대학교 전자공학과 공학석사
2001년 광운대학교 전자공학과 공학박사
1991년 ~ 현재 한국전자통신연구원 홈네트워크보안연구팀 팀장
2004년 ~ 현재 홈네트워크시큐리티포럼 분과장
관심분야 : 홈네트워크보안, 네트워크보안, Optical Security

이덕규

2001년 순천향대학교 공과대학 컴퓨터공학과 공학사
2003년 순천향대학교 전산학과 공학석사
2006년 순천향대학교 전산학과 공학박사
2006년 ~ 현재 한국전자통신연구원 홈네트워크보안연구팀 Post-doc
관심분야 : 홈네트워크 보안, 키관리, 콘텐츠 보안

정교일

1981년 한양대학교 전자공학과 공학사
1983년 한양대학교 전자계산학과 공학석사
1997년 한양대학교 전자공학과 공학박사
1982년 ~ 현재 한국전자통신연구원 정보보호기반그룹 그룹장
2006년 ~ 현재 TTA TC1 의장
2006년 ~ 현재 홈네트워크시큐리티포럼 의장
관심분야 : Security, Biometrics, 홈네트워크보안, RFID