특집

안전한 홈네트워크 구축을 위한 보안요구사항

한종욱* 김도우* 주홍일** 이윤경** 남택용*** 장종수****

목 차

1. 서 론

인터넷 정보가전기기의 등장과 초고속망 이용자의 폭발적인 증가, 그리고 여러 대의 PC를 가진 가정이 증가하면서 가정 내에서 사무실과 같은 통신서비스 환경을 갖추고자 하는 것이 홈네트워크의 시발점이라고 할 수 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, 국내의 경우 지난 외환위기 이후 급격히 증가하고 있는 추세다. 현재, 우리나라의 인터넷 이용인구는 2천8백만이고 인터넷이용률은 세계 최고수준인 65%에 이른다고 한다. 그러나, 반면에 인터넷을 기반으로한 사이버 해킹공격은 급격히 증가하고 있어 국내 해킹·바이러스 신고접수 건수는 2001년 5,333건에서 2002년 15,192건, 2003년 26,179건으로 인터넷 성숙단계의 진입과 동시에 폭발적으로 증가하여 전년도 대비 2003년 국내 해킹은 60% 이상, 바이러스 피해는 100% 이상 증가하고 있다[1~3].

언제 어디서나 컴퓨팅이 가능한 유비쿼터스 컴퓨팅 사회에서는 개인의 컴퓨팅 환경 의존도가 증가함에 따라 사이버공격으로 인한 개인생활의 위협도 증가할 수 밖에 없다. 더욱이 향후에는 원격진료와 같이 개인의 생명과 직결된 유비쿼터스 서비스가 활성화될 것이므로 사이버공격으로 인해 재산뿐 아니라 생명까지 위험에 처하는 경우가 늘어나게 될 것이다. 홈네트워크는 유비쿼터스 컴퓨팅 환경으로 가는 시작점이라고 할 수 있으므로 인터넷을 통한 사이버 공격의 증가는 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 홈네트워크의 보안취약성 및 관련 보안기술 개발동향에 대해서 설명하고, 홈네트워크 구축 시 고려되어야할 보안요구사항 등에 대하여 기술하였다.

* 한국전자통신연구원 선임연구원
** 한국전자통신연구원 연구원
*** 한국전자통신연구원 정보보호연구단 개인정보보호연구팀 팀장
**** 한국전자통신연구원 책임연구원, 정보보호연구단 네트워크보안그룹장

2. 홈네트워크 기술 동향

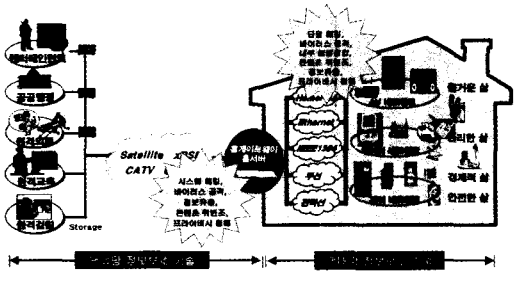
홈네트워크의 기본 개념은 집안의 정보가전기기를 네트워크로 묶고 이를 외부의 인터넷 망과도 연결하여 집 내부 및 외부 어디서나 사용자의 위치에 관계없이 정보가전기기를 제어할 수 있도록 하고 각종 편의를 위한 홈서비스를 제공하겠다는 것이다.

홈네트워크는 외부 인터넷과 연결을 위한 가입자망으로 xDSL, Cable, FTTH(Fiber To The Home) , PLC(Power Line Communication), 위성, IS-95, 3G, 4G, IEEE802.11 등의 다양한 유·무선망의 사용이 가능하다. 홈 네트워크는 그 적용 대상에 따라 여러 대의 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. 정보 네트워크는 컴퓨터 및 그 관련 장비간의 통신을 위한 LAN으로서 1-100Mbps 정도의 속도를 요구한다. 이를 위해서는 무선 통신을 위한 블루투스, 무선랜, HomeRF(Home Radio Frequency)과 유선통신을 위한 이더넷, 전화선을 이용한 통신 (HomePNA : Home Phoneline Networking Alliance), 전력선을 이용한 통신(HomePlug) 등을 이용할 수 있으며, 장비 접속을 위한 표준 프로토콜로는 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 최소한의 속도로 장비 제어용으로 활용되는 X-10과 이보다는 속도가 개선된 CEBus나 LonWorks 등의 프로토콜이 이용되고 있다. 엔터테인먼트 네트워크는 가전장비나 음향 및 영상기기 (TV, VTR, DVD Player, Audio, 게임기 등) 등에 적용되며, 100-400Mbps 정도의 고속으로 동영상이나 음악, 게임 등을 실시간으로 전송하는 네트워크이다. 여기에는 소니 진영이 중심이 된 IEEE 1394 프로토콜이 이용되며, HAVi(Home Audio Video interoperability)라는 음향 및 영상 장비간의 통신 및 제어를 위한 프로토콜이 사용되고 있다. 대부분의 가정에서는 이러한 3가지 네트워크 모두를 필요로 한다. 즉 일반적인 가전기기, 컴퓨터 관련 장비, 음향 및 영상 장비가 모두 가정 내에 존재하므로 이들을 효과적으로 엮을 수 있는 다양한 방안들이 나오고 있다. 이와 같이 홈 네트워크는 컴퓨터 및 그 관련 장치간의 통신뿐만 아니라 각종 가전기기나 방법/방재 기기, 건강 검진용 기기의 제어, 음향 및 영상기기 제어 등에 널리 이용될 수 있다[2].

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, 홈네트워크 내의 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 갖고 있지 못하며, 미들웨어의 경우에도, 각 미들웨어들이 요구하는 보안기능을 모두 만족할 수 있고 개별 미들웨어를 통합한 통합미

들웨어 환경에서도 유연하게 보안기능을 제공할 수 있는 보안인프라가 아직 개발되지 못하고 있다.

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



(그림 1) 홈네트워크의 보안취약점

3. 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. 인터넷을 통한 사이버공격에 대응하기 위해서 대부분의 보안기능을 홈게이트웨이에 집중, 구현하여 안전성을 강화하는 형태로 기술개발이 이루어지고 있다. 홈게이트웨이는 이외에도 댁내망에서 정보가전기기와의 연동을 통한 제어시 불법적인 디바이스 접속을 통해 주요 자원에 대한 공격이나 주요 데이터의 유출 가능성이 존재하고 있으므로 이에 대한 대책 마련이 필요하다. 홈네트워크 내부망에서 특히, 무선구간의 경우 구성요소 및 데이터 보호 등에 취약성을 갖고 있어 구성요소간 인증기능과 데이터의 암호화 기능이 필요하겠다[4].

현재까지 홈네트워크 구성요소 중 가장 많은 연구가 진행된 것은 홈게이트웨이 부분으로, 다양한 상용 제품이 개발되어 시판되고 있다. 홈게이트웨이는 댁외의 공중망과 댁내의 홈네트워크를 연결하는 입구로서 외부의 불법 침입에 대해 일차적인 대응 방안을 제공한다는 개념에서 최우선적으로 보안기능이 탑재되고 있다. 홈게이트웨이에 탑재된 대표적인 보안기능에는 Firewall, VPN (Virtual Provate Network) 등이 있다.

〈표 1〉은 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 1〉 홈게이트웨이 보안제품 현황

구분	업체명
국내	ETRI, 알파에이네트웍스, 시큐베이, 디지스타, 자맥스테크놀로지, 기가링크
국외	Wipro, HotHardWare, FutureSoft, 2wire, linksys,3com, 3eti, MaxGate, D-Link

〈표 2〉 주요 홈네트워크 보안기술 개발 현황

구분	업체명	관련 보안기능 개발현황
국내	안랩유비웨어	○ 댁외에서 원격으로 홈네트워크 자원에 대한 접근을 위해 PKI 기반의 홈네트워크 인증, 인가보안솔루션을 개발
	이니텍	○ 디지털 방송을 위한 PKI 기반의 홈네트워크 보안 솔루션 개발
	소프트포럼	○ 셋톱박스용 PKI 기반의 사용자 인증기술 및 암호기술개발
	시큐어넷	○ 홈네트워크 보안 서버 운영과 인증 솔루션 개발 ○ 원격지에서 댁내의 홈네트워크를 제어, 관리하는 관제서비스 예정
국외	Micro Soft (미국)	○ PC를 홈 엔터테인먼트의 중심으로 설정하여 디지털 서비스를 제공하는 e-Home을 추진 중 ○ PC 접근을 위해 비밀번호 또는 지문 인식을 통한 사용자 인증을 연구
	Cables Labs	○ 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, 마쯔비시, 도쿄공업대 등에서 개인키를 포함한 스마트카드를 이용하여 원격지에서 홈네트워크를 관리하는 기술에 대해 연구 중

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

〈표 2〉는 현재까지 개발되었거나 개발 중인 국내외 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 대해서는 〈표 3〉에 정리하였다[5~9].

〈표 3〉 주요 홈네트워크 미들웨어별 보안기능

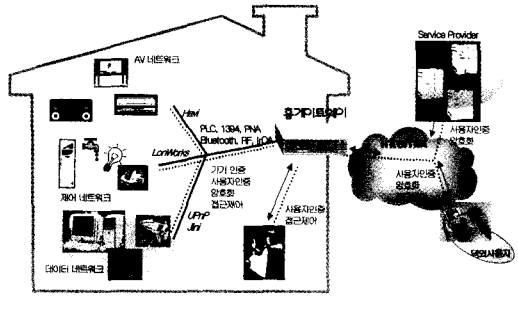
미들웨어	보안기능 현황
UPnP	○ Ver 1.0에서는 보안기능이 정의되어 있지 않음 ○ Ver 2.0에서 보안기능이 추가될 예정임 - 제품 인증기능 제공 - 기기간 인증기능 제공 - 접근제어를 위한 Device가 자체적인 ACL 제공 - 기밀성 제공
Jini	○ Ver 1.0의 보안기능은 Java Security에 의존 - 사용자 인증 기능 제공 - 기기간 인증 기능 제공 - 메시지 무결성 및 기밀성 제공 - 접근제어 기능 제공 ○ Ver 2.0에서 추가적으로 상호인증, 인가기능, 코드 무결성 등에 대한 기능이 강화됨
Havi	○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

4. 보안요구사항

4.1 홈네트워크 보안프레임워크

홈네트워크에서는 이종의 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 홈네트워크 내의 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)는 홈네트워크에서 발생될 수 있는 보안취약성을 해결하기 위해 요구되는 보안기능을 정리한 그림이다. 홈네트워크를 구성하는 다양한 통신매체나 프로토콜 등과 관계없이 요구되는 보안기능을 만족할 수 있는 보안프레임워크가 정립되어야 하며, 홈네트워크의 발전전망을 고려하여 현재 추진 중인 시범서비스에서 연동될 수 있는 수준의 보안기술과 향후 유비쿼터스 컴퓨팅 환경에 근접한 홈네트워크 모델에서 활용될 수 있는 보안기술로 나누어 실질적인 기술개발을 추진하는게 효율적이겠다.



(그림 2) 홈네트워크 보안취약성 대응을 위한 보안기능

4.2 디바이스 인증

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

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

4.3 사용자 인증

홈네트워크에서는 디바이스 인증 외에 디바이스를 사용하는 사람의 신원확인을 위한 사용자 인증 기능도 반드시 필요하다. 홈네트워크에는 생체인식, 패스워드, 인증서, 스마트카드 등 다양한 사용자 인증기술의 활용이 가능하겠지만, 유비쿼터스 컴퓨팅 환경으로의 진화를 고려할 때 정보단말기기의 낮은 성능을 고려한 사용자 인증기술의 활용 및 적용성이 검토되어야 한다. 홈네트워크 사용자 인증기술은 댁내뿐 아니라 댁외에서도 홈네트워크 자원에 대한 원격 접근을 위해 필요하며, 댁내에서 인터넷 뱅킹과 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. 예를들어 RFID 태그 기반의 사용자 인증기술의 활용 가능성이 높아지고 있으므로 유비쿼터스 컴퓨팅 환경에 적합한 새로운 사용자 인증기술에 대한 연구가 필요하겠다.

4.4 기기간 인증

원할한 홈서비스 제공을 위해서는 기본적으로 홈네트워크 구성요소 간의 자원공유를 위한 신뢰가 확보되어야 한다. 이를 위해서는 구성요소 간의 기기간 상호인증이 필요하다. 현재 기기 간의 인증기능은 어느 정도 미들웨어 레벨에서 제공하는 보안기능에 의존할 수 있다. 하지만, 모든 미들웨어가 보안기능을 제공하고 있지 않으므로 이에 대한 해결방안이 수립되어야 하며, 기기 간 인증기능은 다양한 홈서비스를 위한 기본적인 보안기능이라고 할 수 있으므로 홈서비스 제공을 위해서는 다른 보안기능과의 원할한 연동성이 확보되어야 한다. 즉, 사용자 인증 기능, 접근제어 기능 등을 위해서는 기본적으로 기기 간 인증기능이 우선되어야 하므로 다른 보안기능과의 연동성이 고려되어야 한다. 또한, 현재 개발 중인 통합미들웨어 상에서도 유연성있는 기기 간 인증기능이 제공되어야 하므로 통합미들웨어 환경에서의 인증 기능에 대한 연구도 필요하다.

4.5 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 접근제어기능이 필요하다. 유비쿼터스 컴퓨팅 환경을 고려할 때 접근제어를 위한 ACL(Access Control List)은 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.

4.6 미들웨어 보안기능

〈표 3〉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. 현재 ETRI에서 미들웨어의 통합화를 추진하고 있으므로 미들웨어 상에서 보안기능의 통합화에 대한 연구도 필요하겠다. 또한, 홈네트워크 보안프레임워크 연구과정에서 미들웨어의 보안기능 외에 추가적인 새로운 보안기능의 개발 필요성에 대해서도 검토가 필요하므로 이를 위한 미들웨어 보안기능에 대한 안전성 분석이 필요하겠다.

4.7 기타

홈서비스 활성화를 위해서는 안전성 강화보다도 사용자 편리성이 최우선적으로 고려되어야 한다. 보안기능 제공을 통해 홈서비스의 안전성은 강화될 수 있지만 사용자 편리성은 저하될 수도 있으므로 보안기능 개발 시 사용자 편리성에 대한 고려가 있어야 하겠다. 특히, 홈네트워크 보안을 위한 보안정책을 관리하는 경우, 홈네트워크 구성원의 개입없이 자동화된 rule에 의하여 정책이 관리되는 기술의 개발이 필요하겠다.

홈네트워크 환경에 적합한 lightweight한 암호알고리즘 및 인증 프로토콜도 안전성 보다는 효과적인 홈서비스 제공을 우선적으로 고려해야 한다는 점에서 개발이 필요한 보안기능이라고 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.

5. 결 론

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 디지털홈 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 노무라총합연구소의 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 신성장동력으로

서 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 경제손실뿐 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.

참고문헌

[1] 박광로, 송영준, "홈네트워킹", TTA저널, 제78호, pp.101-109, 2001.

[2] 전호인, "디지털홈기술 및 표준화동향", TTA저널, 제88호, pp.59-73, 2003.

[3] 이윤철, "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.

저자약력

한 종 욱

1989년 광운대학교 전자공학과 (공학사)
1991년 광운대학교 전자공학과 (공학석사)
2001년 광운대학교 전자공학과 (공학박사)
1991년-현재 한국전자통신연구원 선임연구원
관심분야 : 홈네트워크 보안, 암호시스템, Optical Security
이 메 일 : hanjw@etri.re.kr

김 도 우

1997년 경남대학교 전산통계학과 (이학사)
1999년 경남대학교 컴퓨터공학과 (공학석사)
2003년 경남대학교 컴퓨터공학과 (공학박사)
2003년-현재 한국전자통신연구원 선임연구원
관심분야 : 홈네트워크 보안, 자바 기술
이 메 일 : dwkim@etri.re.kr

주 홍 일

1996년 금오공과대학교 전자공학과 (공학사)
1998년 경북대학교 전자공학과 (공학석사)
1999년-현재 한국전자통신연구원 연구원
관심분야 : 홈네트워크 보안, 암호시스템, RFID, Smart Card
이 메 일 : juhong@etri.re.kr

남 택 용

1987년 충남대학교 계산통계학과 이학사
1990년 충남대학교 계산통계학과 이학석사
2003년 한국외국어대학교 전자정보공학과 박사수료
1987년 ~ 현재 한국전자통신연구원 정보보호연구단
개인정보보호연구팀 팀장
관심분야 : 개인정보보호, 능동보안, 인터넷,
차세대네트워크구조 등
이 메 일 : tynam@etri.re.kr

이 윤 경

1999년 경북대학교 전자공학과 (공학사)
2001년 포항공과대학교 전자공학과 (공학석사)
2001년-현재 한국전자통신연구원 연구원
관심분야 : 홈네트워크 보안, 센서네트워크 보안,
스마트카드
이 메 일 : neohappy@etri.re.kr

장 종 수

1984년 경북대학교 전자공학과 (공학사)
1986년 경북대학교 전자공학과 (공학석사)
2000년 충북대학교 컴퓨터공학과 (공학박사)
1989년-현재 한국전자통신연구원 책임연구원,
정보보호연구단 네트워크보안그룹장
관심분야 : 네트워크 보안, 정책기반보안관리, 침입방지기술
이 메 일 : jsjang@etri.re.kr