주 제

홈네트워크 서비스에서 정보보호 필요성 및 고려사항

한국정보보호진흥원 유동영

목 차

I. 서 론
II. 홈네트워크 동향 및 보안 필요성
III. 홈네트워크 보안취약성 및 소요기술
IV. 홈네트워크 서비스 모델의 보안 고려사항
V. 결 론

I. 서 론

IT 기술 발달이 우리의 실상활에 많은 영향을 미치고 있다. 90년대말 가정에 ADSL이 설치되면서 급격하게 우리의 가정도 인터넷의 한 부분이 되기 시작했다. 현재 우리나라의 초고속인터넷 가입자 수는 2005년 6월말 현재 약 1200만 가구가 보급되어[1], 국내 대부분의 가정에 초고속망이 설치됐다고 해도 과언은 아닐 것이다. 이러한 초고속 인터넷 서비스의 발달은 가정의 IT에 대한 의존성을 증대하여, 인터넷을 단순한 정보제공 공간으로 뿐만 아니라, 이를 이용하여 댁내 서비스 질을 향상시키고, 생활을 편리성을 증대시킬 수 있는 역할을 기대하고 있다. 이와 맞물려 정보통신부에서는 IT839 전략을 발표[2]하고, 8대서비스 중의 하나로 홈네트워크(Home Network)를 선정함으로서 홈네트워크 서비스가 가까운 미래에 우리의 생활에 깊숙이 파고들어 생활에 융화될 것을 예고하고 있다.

이러한 홈네트워크 서비스를 창출하기 위해서 정부에서는 정보화의 순기능이란 측면에서 산 · 학 · 연 · 관이 협력하여 신규 서비스 모델을 창출하도록 노력하고 있다. 하지만 정보화의 순기능 이면에는 해킹, 개인정보 침해와 같은 역기능이 반드시 생기기 마련인데, 이에 대한 대책을 강구하는 것에는 많은 노력을 하지 못하고 있는 실정이다. 흔히 정보보호를 얘기할 때 "소 읽고 외양간 고치지 말자!"라는 비유를 들어 설명하곤 한다. 최근 홈네트워크 서비스 현황을 살펴보면 서비스 창출을 우선하고 있어 보안사고가 일어난 뒤에 대책을 세우는 현상이 일어날 수 있을 것으로 판단된다.

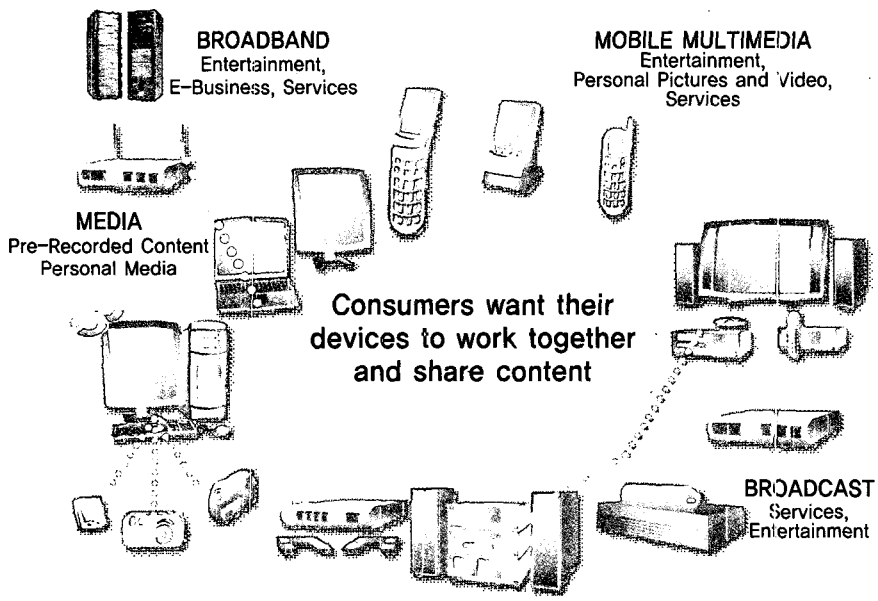
본 고에서는 II절에서 최근 홈네트워크 동향 및 보안 필요성에 대해 살펴본다. III절은 홈네트워크 보안취약성 및 소요기술을 살펴봄으로서, 홈네트워크의 실질적인 보안 위협을 분석해보고, IV절에서는 홈네

트워크 서비스 모델의 보안 고려사항을 정의하고 이에 대한 구체적인 대응 방안을 논의한다. 마지막으로 V절 결론에서는 홈네트워크의 미래와 보안서비스 전망에 대해서 살펴본다.

II. 홈네트워크 동향 및 보안 필요성

홈네트워크 서비스의 성공 여부는 많은 수의 사용자가 서비스를 사용하여 활성화가 되는 것이다. 많은 수의 사용자가 사용할 수 있기 위해서는 댁내 서비스 및 제품에 대한 호환성 확보가 일순위라 할 수 있겠다. 국외에서도 다양한 홈네트워크 표준이 추진되고 있다. 국외에서 가장 활발하게 추진되고 있는 협의체는 DLNA(the Digital Living Network Alliance)라 할 수 있다. DLNA는 우리나라에서는 삼성전자가 대표적으로 참여하고 있으며, 대부분 외국기업으로서 후지쯔(Fujitsu), 게이트웨이(Gateway), HP, 인텔(Intel), IBM, 켄우드(Kenwood), 레노보(Lenovo), 마이크로소프트(Microsoft), NEC(NEC Personal Products), 노키아(Nokia), 파나소닉(Panasonic), 마쓰시타 전기공업 (Matsushita Electric Industrial), 필립스(Philips), 샤프(Sharp), 소니(Sony), ST마이크로일렉트로닉스(STMicroelectronics), 톰슨(Thomson) 등 17개 업체가 주도하여 포럼을 이끌고 있다. (그림 1)은 DLNA가 추구하는 비전을 한눈에 살펴볼 수 있다.

DLNA는 주로 댁내에서의 홈 엔터테인먼트(Entertainment)에 관한 표준을 추진하는데, 2004년에 첫 번째 가이드로서 "Home Network Device Interoperability Guidelines v1.0"를 발표[3]함으로서, 홈네트워크 디바이스에 대한 호환성의 중요성을



(그림 1) DLNA 비전

강조하고 있다. 본 가이드에서는 가전제품, PC, 무선기기 간의 제품간 컨텐츠 공유를 하기 위한 설계 방안에 대해서 설명하고 있다. 하지만 가이드 내용 중 아쉬운 점은 정보보호(예를 들면 컨텐츠 접근 권한 등)에 관한 항목이 아직 논의되지 않는 부분이다. 물론, 제품 및 컨텐츠 사업자 위주로 결성된 포럼이지만, 각각 회사의 면면을 볼 때 결코 보안문제에 대해서 모른척 할 수 있은 그런 업체들이라고 생각되지 않는다.

한편, 국내 홈네트워크 서비스는 분야별 개별 사업자가 홈네트워크 서비스를 제공해 왔다. 하지만 2003년 하반기부터 시작된 정부의 홈네트워크 시범사업이 국내 홈네트워크 서비스 방향을 제시하고 있어 시범사업 모델의 향방에 따라 향후 국내 홈네트워크 서비스 방향이 결절될 것으로 사료된다. 정보통신부 IT839 전략의 하나인 홈네트워크 서비스는 가정의 이용자에게 정보가전제어, 양방향 D-TV, VoD, 헬스케어 및 원격교육 등 미래형 서비스를 제공하는 산업을 육성하고, 통신 · 방송 · 건설 · 가전 및 솔루션 등이 결합되어 연관 산업에 대한 신규 수요창출을 하고자 전략적으로 추진하고 있는 사항이다. 흔히 말하듯 홈네트워크 서비스는 향후 IT기술이 종합선물이라 할 수 있다. 때문에 정부로서는 이러한 홈네트워크 서비스를 활성화하여 '05년까지 200만 가구에 보급하고, '07년에는 전체가구의 60% 수준인 1,000만 가구에 홈 네트워크를 보급하여 국내 경제 활성화에 이바지하려고 하는 것이다. 이에 정부는 홈네트워크에 관련 있는 서비스, 제조, 건축업계가 참여하는 시범사업을 통해 미래형 서비스를 발굴하여 현재 1,300가구에 종합서비스 시범적용 추진하고 있고, 민간업계의 홈 네트워크 보급 촉진을 위해 홈네트워크 인프라 구축 재원을 장기 저리로 융자 지원하고 있다. 그리고 궁극적으로 홈 네트워크의 조기 보급을 통해 '10년까지 110조원의 생산유발효과 및 73조 원의 부가가치유발효과 달성하고, 가정을 쾌적하고 편리한 정보생활 공간으로 변모시켜 개인에게 풍요로운 지능형 홈네트워크 환경 제공을 목표를 두고 있다. 하지만 이런 풍요로운 비전 이면에는 혹시 일어날지 모르는 보안사고 문제를 안고 가고 있는 상황이다.

홈네트워크 우리나라 산업의 SWOT(Strength Weakness Opportunity Threat)분석에 의하면 강점(Strength)으로는 전체인구의 약 1/4에 달하는 초고속통신망 가입자와 PC, 2인당 1대꼴로 가지고 있는 휴대폰 등이 홈네트워크 서비스로 진입하는데 많은 잇점을 제공한다는 것이고, 단점(Weakeness)으로는 홈네트워크 산업을 이끈 주요 제품의 핵심부품면에서 해외의존도가 높아 제품단가 상승이 수익률 저하로 나타날 수 있으며, 대기업 주도형의 형태로 자리를 굳힐 경우 중고시업의 입지가 약화되고 산업전반의 불균형 현상을 초래할 소지가 있다. 또한 기회(Opportunity)로서는 홈네트워크 산업의 발전이 타 산업과의 연관성이 높아 산업전체 파급효과를 창출하고 국가 경쟁력을 증대시킬 수 있고, 위협으로서는 국가전체 시장에 비해 참여가가 많아 과잉 경쟁심화 가능성이 있으며 일부 국가 간의 전략적 제휴 등으로 표준화 블록화 및 그로 인한 로열티 문제가 발생할 가능성이 있다[4]. 이러한 분석에 대하여 각계 기대와 우려가 교차되지만 궁극적으로 홈네트워크 시대가 오는 것은 누구도 부정하지 않기 때문에 좀더 먼저 준비하는 것이 바람직할 것이다.

현재 홈네트워크 서비스를 추진하고 있는 모습을 살펴보면, 단순하게 기존의 홈 오토메이션(Automation) 확장 차원을 넘어서, IT 인프라와의 융화(Convergence)를 모색하고 있다. 이에 따라, 우리가 현재까지 발견하지 못한 보안문제를 그대로 홈네트워크로 이동하고 있는지도 모른다. 또한 홈네트워크 신규 기기에서 발생될 수 있는 보안문제도 현재까

지 알려지지 않았지만, 누구도 발생하지 않는다고 말할 수 없을 것이다.

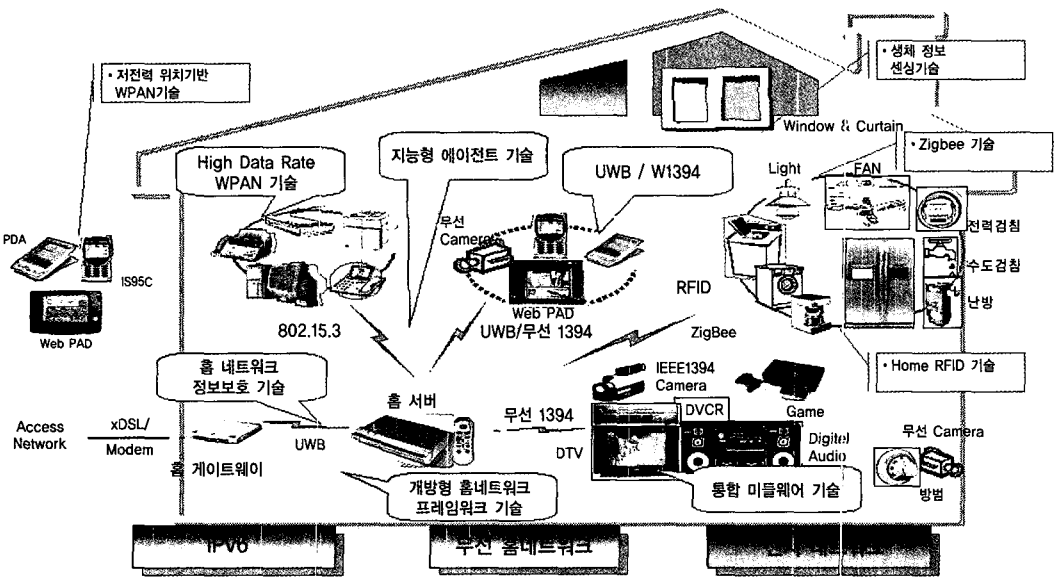
III. 홈네트워크 보안취약성 및 소요기술

앞에서도 살펴본 것과 같이 홈네트워크에는 유·무선 네트워크 프로토콜과 이를 지원하는 미들웨어, 댁내의 홈기기 등이 있다. (그림 2)와 같이 홈네트워크에는 사용자 서비스 요구와 이를 제공하기 위한 다양한 기술이 산재해 있다[6]. 하지만 직관적으로 살펴보면, 댁내망에 접근하기 위한 접근망과 댁내망 자체로 나누어 볼 수 있다. 이러한 관점에서 보안 취약점을 구분해 보면 홈기기 시스템에 대한 해킹, 바이러스 공격, 정보유출, 콘텐츠 위변조, 프라이버시 침해 등으로 나누어 홈네트워크의 침해 위협 유형을 구분할 수 있다.

그리고 이러한 기본적인 침해유형 유형에 의하여 각 프로토콜 별로 세부적인 내용을 살펴보면 다음과 같다.

1. 접근망 취약성

접근망의 홈게이트웨이를 기준으로 외부 서비스 사업자와 연동되는 망을 말하며, 댁내망 접속 지점에 대한 네트워크 패킷 수집을 통하여 댁내의 금융정보 및 사용자 ID 등이 노출될 수 있다. 현재 홈네트워크의 사용자 로드인 정보 등은 홈네트워크 시범사업자에 의하여 암호화 채널을 제공하는 형태로 보호하고 있다. 하지만, 시범사업자 외의 개별 사업자들의 서비스 제공방식은 아직까지 알려지지 않고 있는 실정이다.(그림 3)은 접근망을 통하여 홈게이트웨이로 접속되는 사용자 정보를 수집하여 우리에게 위협이 될 수 있는 부분을 나타낸 것이다.

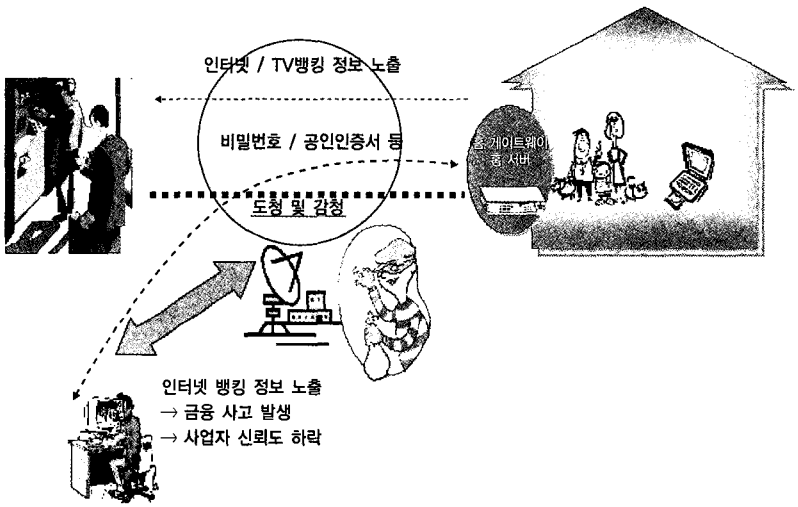


(그림 2) 홈네트워크의 다양한 기술

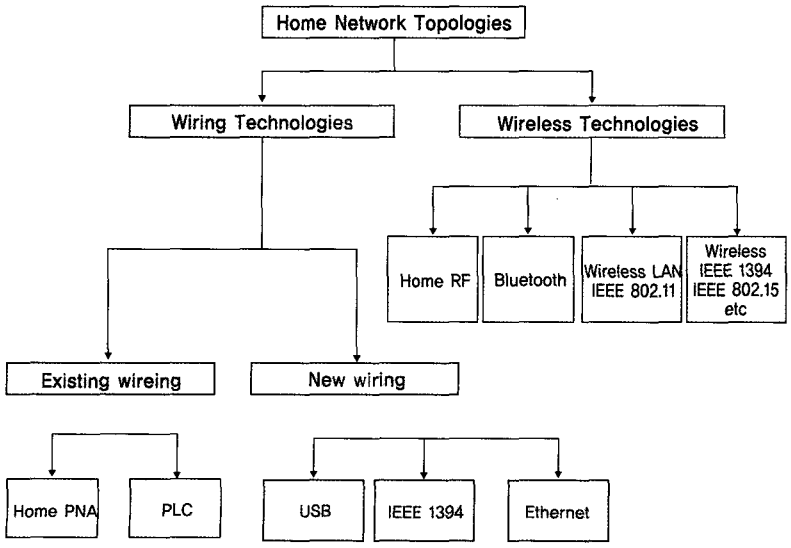
2. 댁내망 취약성

댁내망에는 댁내에서 처리하고 관리하기 위하여 기존 홈에서 설치되어 있는 기술을 이용하여 구축하는 방식과 새로운 선로를 설치하여 구축하는 방식으로 나눌 수 있고, 여기에 유선과 무선이 혼용되어 사용되고 있다[6]. (그림 4)는 홈네트워크 기술표준에 근거하여 분류한 네트워킹 기술 분류도이다.

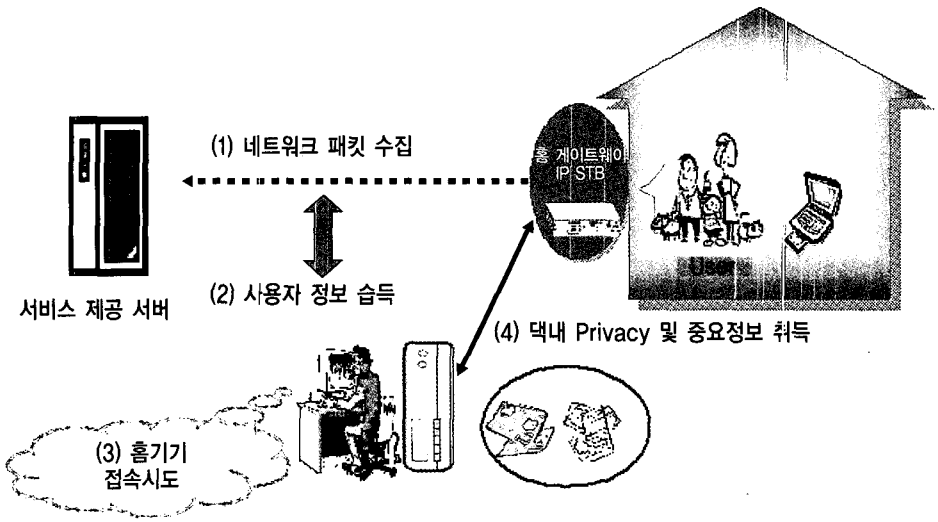
이상의 네트워크 기술이 궁극적으로 댁내의 홈기기와 연동하여 서비스를 제공하는 이러한 연동의 취



(그림 3) 홈네트워크 접근망 위협 사례



(그림 4) 홈네트워크 기술 분류도



(그림 5) 홈게이트웨이 불법 접속

약점과 기술 자체의 취약점으로 인해 많은 보안위협이 노출되게 된다. 다음은 분류별 보안위협에 대하여 설명한다.

2.1 홈기기

현재 댁내망에 제공되는 기기에는 홈게이트웨이를 기준으로 유선망과 무선망으로 구분할 수 있다. 먼저, 홈기기로 대표할 수 있는 홈게이트웨이의 취약점을 살펴보면 (그림 5)와 같이 나타낼 수 있다. 일반적으로 홈게이트웨이를 관리하는 관리프로그램을 설치하게 되는데, 현재 대부분의 관리 프로그램들이 웹기반의 관리 프로그램을 사용하고 있어, 웹서버 및 하위의 CGi 취약점을 이용하여 관리자 권한을 획득할 수 있는 취약점이 있을 수 있다. 특히, 홈게이트웨이는 댁외와 댁내를 연결하는 홈네트워크 안전의 첫 관문이라 할 수 있고, 이에 따라 홈게이트웨이의 침해는 곧바로 홈네트워크 전반에 걸쳐 위협으로 발전될 가능성이 높다. 따라서 홈게이트웨이의 보안 기능은 무엇보다도 중요하고 보안 역할을 수행할 수 있는 보안 기술 개발도 필요하다[7][8].

또한 양방향 DTV, IP 셋톱박스, 홈패드 등과 같이 외부에서 악의적으로 기기 위장하거나, 불법 기기 인증을 통해서 내부 접근자로 위장하거나 불법적 접근을 통하여 임의로 제어할 수 있는 가능성 존재할 것이다. 또한 기기의 물리적 장애 및 오작동 문제로 인해서 저장 정보의 유출 및 해당기기의 사용 불능으로 인해 사용자 필요 시점에 불편을 초래할 수도 있다.

2.2 유선 프로토콜

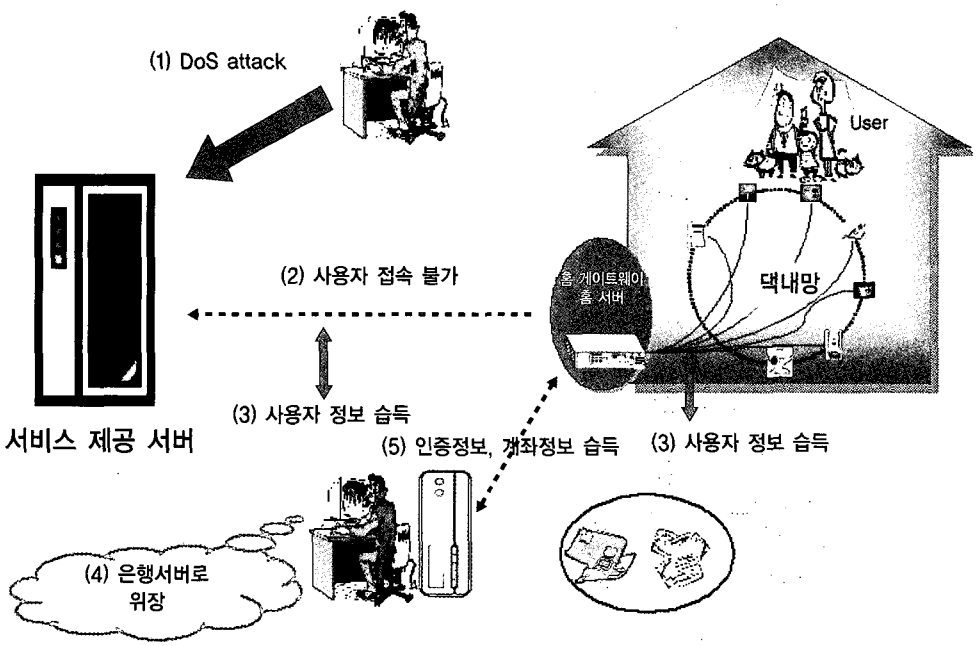
댁내망 유선의 경우, 대표적인 프로토콜로서 Ethernet(IEEE802.3), PLC, IEEE1394 등으로 말할 수 있다. PLC에서는 댁내의 전기 사용량을 모니터함으로서, 댁내 사용자의 패턴을 인식하여 개인의 프라이버시 침해 가능성을 내포하고 있다. 특히 인터넷을 위한 접속망과 유선의 댁내망(주로 Ethernet)은 현재 인터넷에서의 취약점(해킹, 바이러스/웜 등)을 그대

로 내포하고 있어, 타 프로토콜의 피해로 확산되지 않기 위해서는 현재 적용하고 있는 보안대응기술을 신속히 적용해야 할 것이다. 전반적으로 Ethernet, PLC, IEEE1394 등 홈네트워크 내부 유선망은 내부 접근자로 위장이 가능하며, 불법적인 접근자의 제어 가능성이 존재하고, 물리적 장애 및 오작동 문제, 홈 내부의 통신 장애를 일으킬 수 있다. (그림 6)은 홈네트워크 유선망에 대한 보안위협을 나타내고 있다.

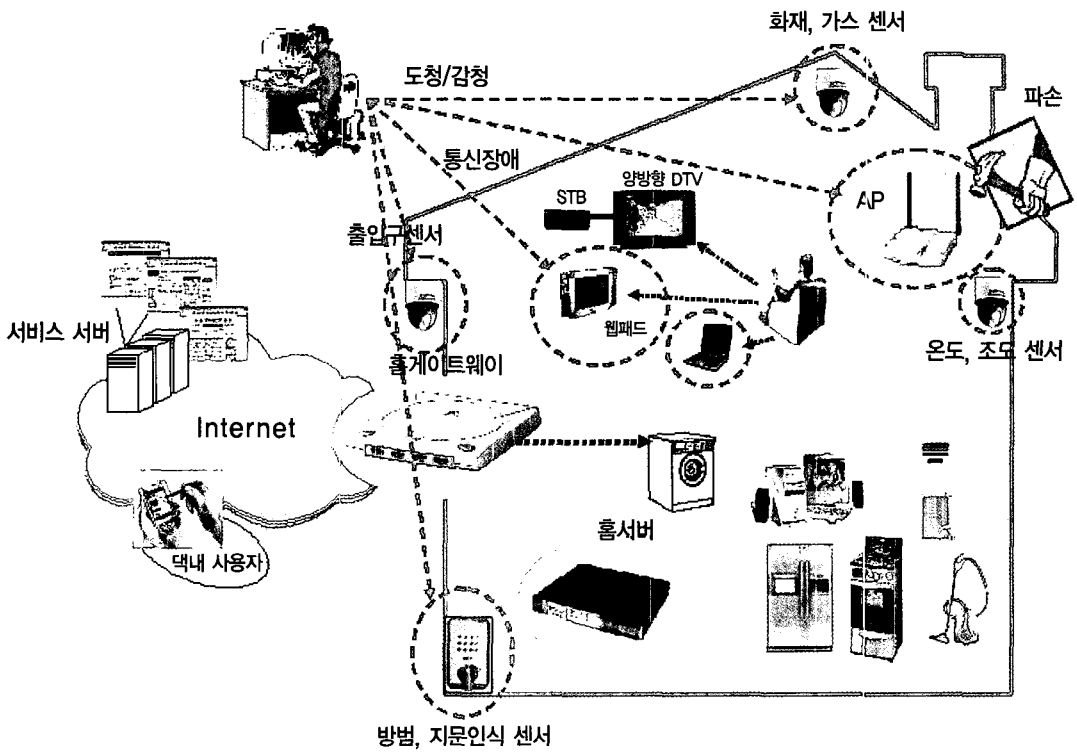
2.3 무선 프로토콜

홈네트워크에 적용할 수 있는 무선 프로토콜은 무선랜, HomeRF, Bluetooth, UWB, ZigBee 등이 있다. 무선 프로토콜은 근본적으로 도청과 감청이 가능한 프로토콜이다. 그렇기 때문에 송신자와 수신자 사이의 보안설정이 무엇보다 중요하다. 따라서 최소한 홈네트워크 서비스 중 댁내 기기에 대한 제어 신호는 암호화를 통한 신호 전송이 필요하다. 만약 이 부분이 해결되지 않는다면, 내 · 외부 접근자 위장으로 불법적 접근자의 제어 가능성이 존재하고, 비인가 사용자의 접근 허용이 가능하며, 물리적 장애 및 오작동 문제를 일으킬 수 있다. 또한, 무선망의 특징을 이용한 주기적인 무선 접속요청을 통해 서비스 거부공격에 의한 홈 내부통신 장애 등이 일어날 수 있다. (그림 7)은 홈네트워크에서 사용 가능한 화재, 가스, 방범 센서 및 댁내 무선에 대한 도청을 기반으로 무선망이 보안위협을 도식화하고 있다.

현재 홈네트워크를 구축하는데 근간이 되는 것은 유선망 프로토콜을 근간으로 하고 있지만, 접근망을 제외하고, 댁내망에서는 무선 프로토콜이 유선 프로토콜을 대체할 가능성이 높다. 무선 프로토콜을 서비스 설치가 쉽고, 이동성이 뛰어나 유비쿼터스 홈네트워크 환경으로 가기 위한 필수 조건을 충족한다[8].



(그림 6) 홈네트워크 유선망 보안위협



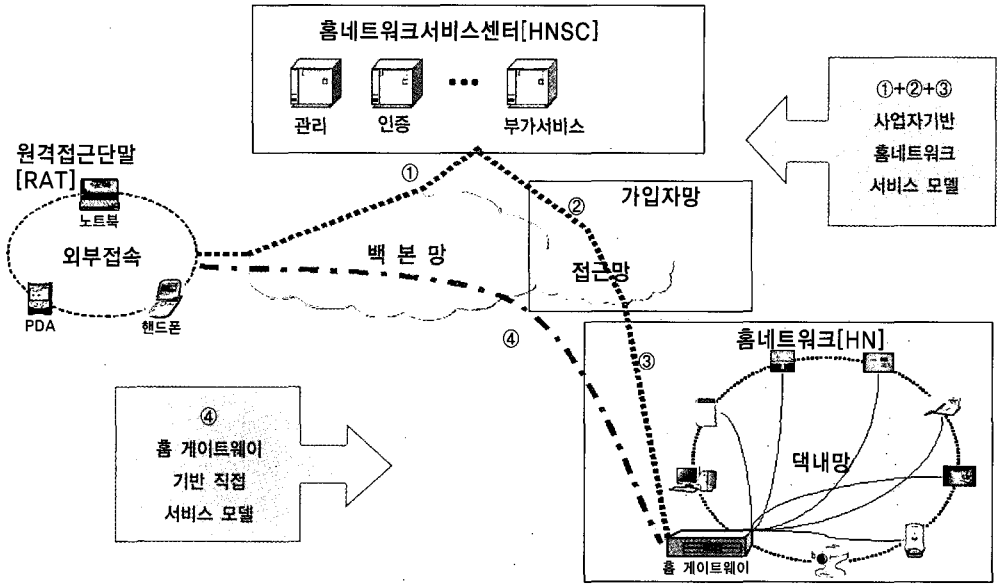
(그림 7) 홈네트워크 무선망 보안위협

따라서 향후 RFID/USN과 같은 인프라와 접목될 가능성까지 고려해보면 무선망의 보안위협에 대하여 기술적이 진보도 필요하다.

IV. 홈네트워크 서비스 모델의 보안 고려사항

홈네트워크에는 다양한 IT 기술과 홈기기가 적용된다. 일반적인 홈네트워크 구조를 살펴보면, 댁외의 원격접근단말(Remote Access Terminal: 이하 RAT)를 통해서 홈네트워크(Home Network: 이하 HN) 서비스에 접속하여 댁내 서비스를 제어하고 제공받는 것을 말한다. (그림 8)에서는 일반적인 홈네트워크 모델에 두 가지 모델을 정의하고 있다. 첫째는 홈네트워크 서비스센터 기반 간접 서비스 모델(HNSC based Indiretly Service Model: 이하 HBISM)이고, 둘째는 홈게이트웨이 기반 직접 서비스 모델(Home-gateway based Directly Service Model: 이하 HBDSM)이다.

다음은 2가지 서비스 모델별 특징이다. ① HBISM에서는 댁내 사용자가 홈네트워크 제어서비스 등을 사용하고자 할 때 사용자 인증 및 접근권한 제어를 홈네트워크 서비스센터(Home Network Service Center: 이하 HNSC)에 위임하는 것이다. 이에 인증받은 홈네트워크 서비스센터에서는 사용자 요청을 바탕으로 서비스를 제공하는 것이다. HBISM의 문제점은 댁내 홈네트워크 서비스 관리에 대한 서비스 집

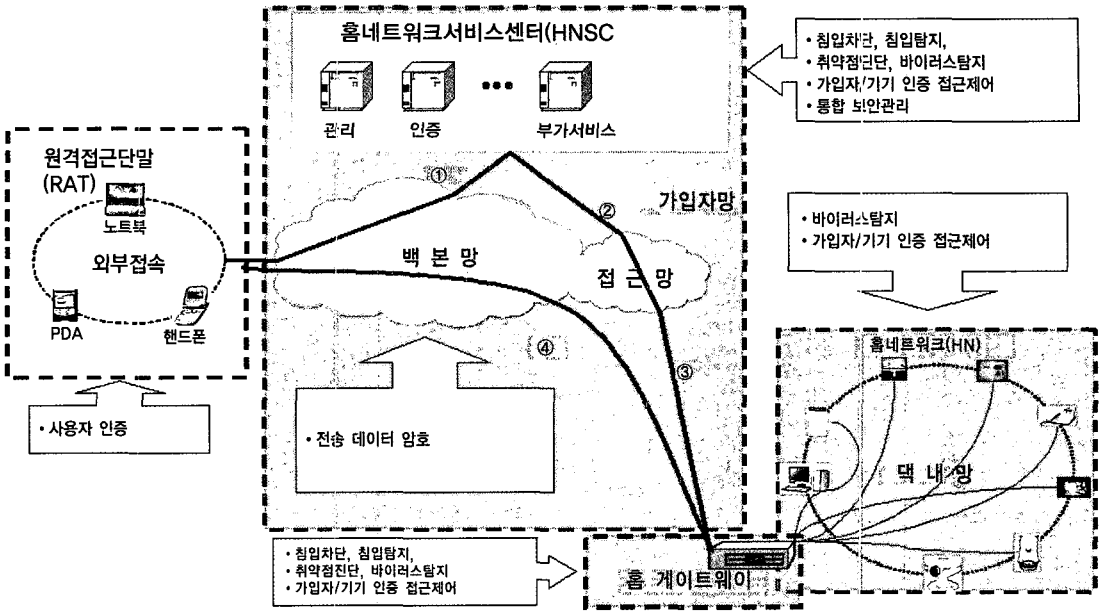


(그림 8) 홈네트워크 서비스 모델

중과 이에 대한 신뢰의 문제이다. 현재 국내 시범사업자의 경우 HBISM 모델을 채택하고 있다. 이 모델의 경우 보안기능을 HNSC와 홈게이트웨이를 통해서 이중 구조로서 대응할 수 있는 구조를 가지고 있다. 하지만 현재 홈게이트웨이의 성능 저하로 인하여 간단한 보안필터 기능도 사용하지 않고 있는 실정이다. 따라서, 현재 홈네트워크 시범사업 구조와 같이 HNSC의 보안성에 따라, 전체 홈네트워크 서비스의 보안성이 결정되게 된다. 그리고 HBISM의 구조상 HNSC를 이용하는 비용 문제가 발생되는데, 이는 서비스 차별화로서 풀 수 밖에는 없을 것이다. ② HBDSM에서는 홈네트워크 사용자가 댁내 홈게이트웨이를 접속하여 직접 홈기기를 제어하는 모델로서, 홈게이트웨이의 보안 능력에 의존적이다. 따라서 홈게이트웨이의 성능과 보안성이 밀접하게 된다는 얘기다. 이러한 모델은 사용자가 외부 위임자를 신뢰하지 않고, 직접 제어함으로서 신뢰와 비용 부분을 해결할 수 있을 것으로 판단된다. 하지만, 홈게이트웨이가 외부 해킹에 의해서 침해됐을 경우, 댁내의 모든 정보가 노출될 가능성이 있어 신중한 고려가 필요하다.

다음은 홈네트워크 보안 취약성을 해결하기 위한 소요 기술을 구간별로 구분하였다. 본 구분은 앞에서 말한 두 가지 서비스 모델에 전반적으로 적용할 수 있을 것으로 판단된다. (그림 9)에서와 같이 원격접근 단말에서는 사용자인증이 필요한데, 현재 ID와 패스워드를 이용하여 적용하고 있다. ID와 패스워드를 이용하는 경우, 네트워크 패킷 수집을 통한 취약점이 노출되어 문제가 발생될 가능성이 있다. 향후에는 공인인증서 및 생체 인증 등 다양한 사용자 인증 기법을 적용하여 보다 편리하고 안전하게 제공되어야 하겠다.

전송망에 대한 보안고려는 대부분 전송데이터 노출로 인한 위협에 대응하는 것으로서, 현재로서는 댁



(그림 9) 홈네트워크 구간별 보안고려 사항

내 제어신호에 대한 데이터 암호가 필요한 실정이다. 또한, HNSC에서는 댁내로 유입되는 모든 보안위협에 대처하기 위하여 침입차단, 침입탐지, 취약점 진단, 바이러스탐지, 사용자 인증 및 기기인증과 통합 보안관리(인원 및 장비) 등의 보안 고려사항이 있다. 특히, HNSC에서는 관리적인 고려사항이 많이 적용이 되는데, 서비스 가입자 대부분의 개인정보 및 댁내에 접근할 수 있는 것에 대한 권한위임 등에 대하여 SLA 등을 명시하여 사업자와 사용자 간의 역할 및 책임에 대하여 명확히 해야 한다.

V. 결 론

정보통신부 IT839 전략 중 우리의 실생활에 가장 많은 영향력을 발휘할 서비스는 홈네트워크 서비스이다. 유비쿼터스 홈네트워크 서비스를 창출하는데 있어 기술의 진보와 사용자의 편리성을 고려하는 것은 당연하다. 하지만 사용자에게 발생될 여러 가지 불편 사항을 무시하는 서비스는 결코 성공할 수 없을 것이다. 이러한 불편 사항 중 서비스 장애를 통한 불편이 있는가 하면, 보안관리 부재로 인한 불편도 있을 것이다. 서비스 장애는 단순하게 서비스 복구를 통하면 해결된다. 하지만 보안 문제는 이와는 다르다. 홈네트워크 해킹을 통한 사용자의 개인정보나 금융정보는 단순히 타인이 그 정보를 습득하는 것으로 끝나지 않고, 이를 악용하려는 의도가 많다. 때문에 사고 발생 후에도 이를 수습하는데 많은 노력이 필요하다. 어쩌면 서비스 투자비용보다 손실비용이 더 클지도 모른다.

또한, 향후 통신과 방송의 융합을 위한 광대역통신망(BcN)이 FTTH(Fiber To The Home)과 연계될

경우, 홈게이트웨이의 하드웨어와 소프트웨어 구조는 BcN형 홈네트워크 성능을 실현할수록 개발되어야하고, 네트워크상의 보안기술도 도입의 필요성이 제기되고 있다.[10] 때문에 향후에는 좀더 복잡하고 다양하게 홈네트워크 진화될 가능성이 높아, 현재 시점에 필요한 보안 요구는 무엇보다 중요하다고 할 수 있다.

결론적으로 말하면, 본격적인 홈네트워크 서비스에 진입하기 전에 기본적인 홈네트워크 보안을 고려하여 서비스 모델 설계부터 안전한 홈네트워크 서비스 모델을 창출하는 것이 바람직할 것이다. 우리는 흔히 말하는 것 중 하나가 "병은 감추지 말고 알려라" 라는 말이 있다. 마찬가지로 보안문제도 발생될 가능성이 있는 문제를 감춘다고 해서 해결되는 것이 아니라, 이를 공개하여 관련 제도 개선과 기술개발로서 해결하는 것이 바람직할 것이다. 나아가서 홈네트워크 서비스의 안전성을 보장하기 위해 보안서비스를 제공하는 것이 서비스 사업자의 당연한 의무로 생각하고, 사용자는 서비스 안전을 위해 안전 수칙 준수 등 보안에 대한 경각심을 갖는 것이 필요하다. 아울러 좀더 나은 서비스를 제공하기 위해 차별화된 보안 서비스를 개발하여, 사용자들에게 보안의 필요성을 인지시켜, 서비스 수준에 따라 안전이 보장된다는 인식의 전환도 필요하다.

[참 고 문 헌]

[1] "2005년 6월 기준 인터넷통계 월보", 인터넷정보진흥원, 2005. 7. 22

[2] "국민소득 2만불로 가는길 [IT839 전략]", 정보통신부, 2005

[3] "Home Networked Device Interoperability Guidelines", Members of the Digital Living Network Alliance(DLNA), June 2004

[4] "국내 및 해외 홈네트워크 산업 현황과 미래발전 전략", 홈네트워크산업협회저, 2005. 5

[5] "홈네트워크 관련정책 및 기술취약성", 제1회 홈네트워크 시큐리티 워크숍, 김태근, 정보통신연구진흥원, 2004. 7. 12

[6] "디지털 홈 네트워크 기술 표준 개론", 한치문 · 박광로 공저, 한국정보통신기술협회(TTA), 2004. 2

[7] "유비쿼터스 홈네트워크 환경에서의 침해 위협 및 대응 방안", 유동영, 김영태, 노병규 한국정보보호진흥원, 2004. 10 학술발표논문집 31권 제2호, 한국정보과학회

[8] "홈네트워크 침해 위협에 대한 홈게이트웨이 보안요구 및 대응방안", 유동영, 김영태, 노병규, 조병진, 한국정보보호진흥원, 2004. 11 추계학술발표논문집 11권 제2호, 한국정보처리학회

[9] "홈네트워크 보안요구 현황 및 대응기술 전망", NetSec-KR 2005, 제11회 정보통신망 정보보호 워크숍, 유동영, 한국정보보호진흥원, 2005. 4. 21

[10] "BcN과 홈네트워크", 이정욱, 2005. 3. 5 발행

유동영

1997년 숭실대학교 전자계산학과 공학사
2000년 숭실대학교 컴퓨터학과 공학석사
1997년 한강시스템 사원
2000년 줄라이네트 주임연구원
2000년 ~ 현재 한국정보보호진흥원 선임연구원