유비쿼터스 홈네트워크 환경에서의 침해 위협 및 대응 방안

유동영° 김영태 노병규

한국정보보호진흥원

{ydy°, ytkim, nono}@kisa.or.kr

Response and Threat of Home Network in Ubiquitous Environment

Dongyoung Yoo° Youngtae Kim ByungGyu No

Korea Information Security Agency

요 약

최근 들어, 홈네트워크에 대한 관심이 날로 높아지고 있다. 정부에서는 IT839 전략의 하나인 홈네트워크 서비스를 시범 사업을 통해 활성화하려고 하고 있다. 이러한 서비스가 일반 대중들에게 혜택을 누리게 하기 위해서는 많은 노력이 필요한데, 이러한 노력 중 가장 중요한 것이 표준화이다. 현재 홈네트워크 표준화는 사용자 서비스 측면에서 많은 부분에서 개발되고 있다. 하지만 아직까지 시큐리티(Secrutity) 요구 사항이 반영이 되고 있지 않은 부분이 있다. 이러한 시큐리티 요구가 반영되고 있지 않은 이유로는 홈네트워크의 위협에 대해서 간과하고 있기 때문이다.

홈네트워크는 유선(Wired)과 무선(Wireless)이 공존하고 있다. 이것들이 새로운 기술이 아니고, 기존에 존재하는 기술을 바탕으로 개발되기 때문에 기존의 외부 위협들은 그대로 홈네트워크에 반영될 것이다. 또한 향후 도래할 유비쿼터스 환경도 홈네트워크에 접목될 것이라고 누구나 인지하고 있다. 유비쿼터스와 같은 다양한 환경에서는 현재보다도 복잡한 위협이 존재할 것이다. 본 논문에서는 현재의 홈네트워크 환경을 분석하고 이에 따르는 보안 위협과 향후 다가올 유비쿼터스 환경의 침해 유형에 대해서 살펴보고자 한다.

1. 서 론

인터넷이 발달하면서 다양한 IT 서비스가 창출되고 있다. 그 중에서 우리의 실생활과 가장 가까이 제공 될 서비스 중의 하나가 홈네트워크 서비스이다. 국내에서도 차세대를 이끌어갈 서비스 하나로 홈네트워크를 선정하고 이에 따르는 시범 사업 추진 및 관련 산업 육성을 하고 있다. 하지만 홈네트워크를 사용할 사용자들은 서비스에 대한 편리성만을 요구하고, 이에 따르는 침해 위협에 대해서는 무관심한 상황이다.

현재 홈네트워크 서비스는 그림 1과 같이 4가지의 분야로 표현되고 있다. 첫째, AV 네트워크는 집안의 가전제품 중 오디오, 비디오와 같은 종류의 기기들의 네트워크를 구성하기 위한 것으로 주로 IEEE1394 프로토콜을 이용하여 상용화되고 있다. 둘째, 전력선을 이용한 PLC 네트워크는 설치가 간단하고 간단한 제어 명령들을 전송할 수 있어 냉장고, 세탁기와 같은 간단한 명령 체계를 가지는 장비들을 제어하는 데에 상용화되고 있다. 셋째, 서비스 네트워크로서 원격 검침 및 방범과 같이 외부에서 댁내의 사용량을 점검하는데 주로 구성된다. 마지막으로 무선 네트워크는 설치가 어려운 홈네트워크 장비 및 가전을 쉽게 연동할 수 있는 기술로서 향후 홈네트워크를 연결하는 가정 중추적인 역할을 수행할 것이다.

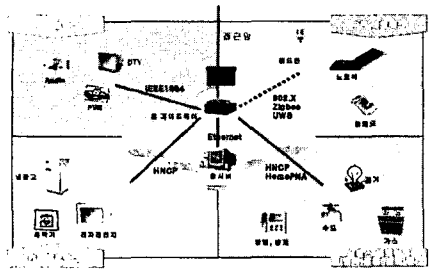

그림 1 홈네트워크 서비스 개요

현재 홈네트워크의 가장 큰 현안은 가정에서 인터넷 및 디지털 가전기기 사이의 의사 소통 즉 호환성 문제이다. 또한 호환성 문제로 발생되는 침해 위협도 존재하고, 기존의 인프라를 그대로 수용하기 때문에 기존 인프라의 침해 위협도 같이 수반되고 있다는 것이 문제점으로 지적될 수 있다.

2. 본 론

2.1 홈네트워크 보안 환경 분석

홈네트워크에는 홈패드, 홈서버, 홈게이트웨이 등 많은 수의 기기들이 존재하는데, 그 중에서 현재 상용화되고 있는 것이 홈게이트웨이 분야이다. 홈서버의 경우도 홈게이트웨이의 보조 역할을 할 것으로 기대하고 있지만 단독으로 홈서버 제품을 출시하지는 않고 있다. 현재 홈게이트웨이는 2001년 12월에 정보통신표준협회를 통하여 표준을 제정하였다[1]. 하지만 최근에 홈게이트웨이에는 이더넷(Ethernet), PLC, IEEE1394 등의 많은 프로토콜과 서비스 등이 탑재되고 있어 좀더 향상된 성능을 요구하고 있다. 또한 사용자 인증 및 접근제어와 같은 보안 기술도 요구되고 있는 실정이다. 현재 국내·외 연구의 공통점을 살펴보면 홈네트워크의 심장인 홈게이트웨이가 모든 프로토콜을 지원하는 방향으로 발전하고 있고 여기에 AAA 인증과 같은 기능도 구현되고 있다.

유선(Wired) 홈 네트워킹 기술은 전력선 기술(PLC), Ethernet, IEEE1394 등이 있다. PLC 및 HomePNA는 기존에 구축돼 있는 전력선 및 전화선을 이용한 것으로 대부분의 주거공간엔 이미 배선이 돼 있어 발전 가능성이 높다. IEEE1394는 보안과 관련하여 복제방지 부분만을 고려했다. 따라서 인증된 디바이스(Device)만이 접근할 수 있도록 하는 기기간의 인증 부분을 제공한다. 주로 데이터 보호에만 초점을 두고 있어 향후 사용자 접근과 관련하여 미들웨어에서 이를 뒷받침해줄 필요가 있다. HomePNA는 기존의 구축된 전화망을 이용하여 고속의 댁내 망을 구축하기 위한 기술로서, 현재 3가지(1.0, 2.0, 3.0) 표준을 채택하고 있다. HomePNA 표준에는 다른 주파수와 간섭이 일어나는 취약성을 제외하고는 기기 인증 및 접근제어 부분은 고려하고 있지 않아, 향후 홈네트워크에 적용하는데 어려움이 있을 것으로 예상된다. PLC 기술은 전력선을 이용한 통신 기술로서 가스 검침·원격 제어·보안(CCTV)·오디오(AV) 등 다양한 분야의 애플리케이션이 최근에 출시되고 있다.

무선망의 경우 현재 속도 부분에서는 많은 개선이 이루어지어 802.11X 계열의 경우 54Mbps(802.11g)까지의 개발되었지만, 보안성 검토를 해보면 802.11b를 사용해야 최소의 보안성을 보장하고 있고, 좀 더 나은 보안성을 유지하기 위해서는 802.11i 수준이 필요하다[2]. 무선망에서는 2Mbps 이내의 전송이 가능한 HomeRF 2.01(2002.07.01)을 발표하였다. 발표 스펙에서는 시큐리티 요소와 관련하여 보안 구조(Security architecture) 부분을 명시하고 있다[3]. Zigbee에서는 키 교환 등과 같은 인증 메커니즘을 제공하고, 두 기기간의 인증 부분을 제공함으로서 향후 홈네트워크에서 제공되어야 할 홈 무선기기간의 인증 부분에 대하여 그 역할을 수행할 수 있을 것이다[4]. 블루투스(Bluetooth)는 블루투스 SIG에서는 3가지 보안 모드를 제공하는데, 신뢰받은 단말기(trusted device)에 대해서는 무제한으로 모든 서비스가 사용이 가능해 보안상의 취약점을 내포하고 있다. 최근에는, 해커에 의해서 몇몇의 블루투스 지원 핸드폰의 사용자 정보가 외부로 유출되는 사건도 있었다. 핀란드의 휴대폰 제조업체 노키아는 블루투스 기술을 탑재한 자사 일부 휴대폰이 '블루스나핑(bluesnarfing)과 블루버깅(bluebugging)'공격에 취약하다 발표하였다. 휴대폰에는 아무런 침투 흔적도 남지 않아 자신의 정보가 노출됐는지 조차 확인할 수 없는 실정이다[5].

2.2 침해 위협 및 대응 방안

유선망에서는 도청 및 신분 위장이 계속해서 존재하고, 서비스 거부와 같이 홈게이트웨이를 무력화 시킬수 있는 부분이 존재한다. 특히 홈네트워크에서는 다른 위협과 달리 사용자의 고의적이지 않은 실수로 발생하는 경우도 많이 발생될 것으로 예상되어, 실제 공격과 사용자 실수 부분도 많은 고려가 필요하다.

무선망에 대한 보안 문제를 정리해 보면, 첫째 현재 무선망에 대한 보안 중 가장 시급한 문제가 유선망에 비해 쉽게 도청을 당할 수 있다는 것이다. 둘째로는 다양한 형

태의 서비스거부(Denial of Service) 공격에 노출될 수 있다. 무선망의 특성상 네트워크에 접속하려는 단말에 대해서는 계속해서 연결 요청을 하려고 하는데, 이러한 연결 요청이 하나의 AP에 가상(Virtual)으로 다수가 요청될 경우 신규로 접속을 요구하거나, 현재 접속한 단말에서도 서비스가 불가한 경우가 생길 수 있다.

이상에서 살펴본 홈네트워크 환경를 바탕으로 기본적인 침해 유형을 살펴보면 다음과 같다.

표 1 홈네트워크 침해 유형

공격 유형	공격 내용	대상
도청	패스워드, 중요 데이터, 특정 서비스의 기능 등에 대한 정보 수집	접근망 패킷 댁내망 패킷
신분위장	홈네트워크 프로토콜의 취약점을 이용(IP spoofing, Prediction 등)하여 정당한 사용자나 시스템으로 위장	홈게이트웨이 댁내망
서비스거부 공격	네트워크 사용량 초과 메일 폭탄 다량의 무선랜 접속 요구	홈게이트웨이 무선AP
개인정보 (Privacy)	특성 서비스의 사용량 수집	전기 사용시간 TV 시청시간

이상의 침해 유형들은 기존의 유·무선망을 그대로 수용하여 홈네트워크의 인프라를 구축하고, 부가적으로 홈네트워크에 필요한 부분만을 통합하는 형태로 서비스가 구축되었기 때문이다. 그러므로 현재 우리가 대응하고 있는 침해사고의 대응 방법을 이용한다면 일반적인 공격에 대해서는 대응 할 수 있을 것이다. 표 2는 홈네트워크의 개념적 대응 방안을 명시하였다.

표 2 개념적 대응 방안

보안대책	사용되는 보안 메커니즘
인증	- 최소의 패스워드 기반 인증 - 인증서 기반의 인증
접근통제	- 접근통제 목록, 사용자, 가용목록 이용 - 사용자 권한 기반의 접근 제어
데이터 비밀성	- 메시지의 암호화 - 패킷필터링 라우팅/방화벽 기능 이용
모니터링	- 접근제어 정보의 변경에 대한 로그 - 감사 도구의 사용

3. 결 론

현재 국내 홈네트워크 서비스는 정보통신부에서 추진한 1차, 2차 시범 사업을 필두로 하여 각 홈네트워크 산업계의 기술 개발에 의존하고 있는 실정이다. 이러한 산업계 주도의 홈네트워크 제품 및 서비스는 자칫 사용자의 편의성만을 강조한 채 사용자의 정보보호에는 무관심할 수 있다. 향후 홈네트워크에서 보안과 관련된 많은 연구가 있을 것으로 예상된다. 그 중에서도 가장 중요한 부분은 보호정책을 수립하고 이를 사용자가 편리하게 사용할 수 있게 하는 것이다. 보안 정책을 기술하기 위한 보안 프레임워크 개발하고, 이를 적용한다면 최소한의 사용자 정보보호가 이루어 질 것이다.

일차적으로 홈네트워크 사용자들은 홈네트워크가 새로운 패러다임이 아니라는 것을 숙지하여 기존의 취약점에 대해서도 방지할 필요가 있다. 또한 다양한 기술과 기기가 혼재되어 있는 홈네트워크에서는 이기종 프로토콜간의 침해가 일어날 수 있고, 좀더 복잡한 유형의 공격이 발생될 수 있기 때문에 이에 대한 대응 방안도 고려해야 한다. 추가적으로 홈네트워크에 가장 중요한 것이 개인정보 보호일 것이다. 가장 많이 산재되어 있는 개인정보를 보호하기 위해서 홈네트워크 특성이 고려된 접근제어 및 인증 기술이 연구되어야 할 것이다.

[참고 문헌]

[1] "홈게이트웨이 정보통신 표준(Home Gateway Standard)", 정보통신단체표준, TTAS_KO-04_0015, 2001년 12월 3일.

[2] IEEE802.11, http://grouper.ieee.org/groups/802/11

[3] HomeRF Specification, Revision 2.01, 1 July 2002, HomeRF Working Group, Inc.,

[4] ZigBee Technology: Wireless Control that Simply Works, Patrick Kinney, Kinney Consulting LLC, Chair of IEEE 802.15.4 Task Group, Secretary of ZigBee BoD, Chair of ZigBee BuildingAutomation Profile WG, 2 Octorber 2003,

[5] Wireless Security, Bluetooth Special Interest Group (SIG), 2003