유비쿼터스 환경에서의 홈네트워크 시스템 침해 위협 및 대응 방안

오대균* · 정진영**

요 약

최근 초고속 인터넷의 확산과 댁내 가전기기들의 지능화에 따라, 홈 네트워크(Home Network)에 대한 사회적인 관심이 높아지고 있다. 언제 어디서나 컴퓨팅이 가능한 유비쿼터스 컴퓨팅 사회에서는 개인의 컴퓨터환경 의존도가 증가함에 따라 사이버공격으로 인한 개인생활의 위협도 증가할 수 밖에 없다. 홈네트워크는 유비쿼터스 컴퓨팅 환경으로 가는 시작점이라고 할 수 있으므로 인터넷을 통한 사이버공격의 증가는 눈앞에 현실로 다가오고 있는 홈네트워크의 활성화를 방해하는 장해물로 대두될 것이 틀림없으므로 이에 대한 대응책 마련이 시급하다고 할 수 있다. 이와 같은 다양한 환경에서는 현재보다도 복잡한 위협이 존재할 것이다. 따라서 본 논문에서는 현재의 홈네트워크 시스템 환경을 분석하고 이에 따른 보안 위협과 향후 다가올 유비쿼터스 환경의 침해 유형에 대해서 살펴보고자 한다.

Response and Threat of Home Network System in Ubiquitous Environment

Dae-Gyun Oh* · Jin-Young Jeong**

ABSTRACT

Recently The social interest regarding is coming to be high about Home Network accordong to intelligence anger of diffusions and the family home appliance machineries and tools of the superhigh speed Internet In the ubiquitous computing socioty, only neither the threat of the private life which is caused by in cyber attack will be able to increase according to the computer environment dependence degree of the individual increases In the ubiquitous computing socioty, only neither the threat of the private life which is caused by in cyber attack will be able to increase according to the computer environment dependence degree of the individual increases Beacaues of Home network is starting point to go ubiquitous computing enviorment, The Increase of Cyber attack through Internet will raise its head with the obstacle to disrupt the activation of the groove network. So there is a possibility of saying that the counter-measure preparation is urgent, In the various environment like this, It means the threat which present time than is complicated will exist. So it will analyze the Home network system environment of present time and observe the Security threat and attack type in the ubiquitous computing enviorment. So it will analyze the Home network system environment of present time and observe the Security threat and attack type in the ubiquitous computing enviorment.

Key words : Ubiquitous, Home Network, Response, Security

* 한국에너지기술연구원 창업보육센터 센터장

** 대전보건대학 멀티미디어과 조교수

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 서비스의 하나로 홈네트워크를 선정하고 이에 따르는 시범사업 추진 및 관련 산업 육성을 하고 있다. 하지만 홈네트워크를 사용할 사용자들은 서비스에 대한 편리성만을 요구하고, 이에 따르는 침해 위협에 대해서는 무관심한 상황이다.

홈 네트워크 서비스는 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 방법과 같이 외부에서 댁내의 사용량을 점검하는데 주로 구성된다. 마지막으로 무선 네트워크는 설치가 어려운 홈네트워크 장비및 가전을 쉽게 연동할 수 있는 기술로서 향후 홈 네트워크를 연결하는 가정 중추적인 역할을 수행할 것이다.

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.

본 논문은 2장에서는 유비쿼터스, 홈네트워크 서비스 기술에 대한 관련연구를 살펴본 후 3장에서는 홈네트워크 시스템 보안환경에 대하여 논의한 후 4장에서는 유비쿼터스 환경에서의 홈네트워크 시스템 침해위협 및 대응방안에 대해 기술하고, 끝으로 5장에서 결론 및 향후 연구방향을 제시한다.

2. 관련 연구

2.1 유비쿼터스(Ubiqitous)

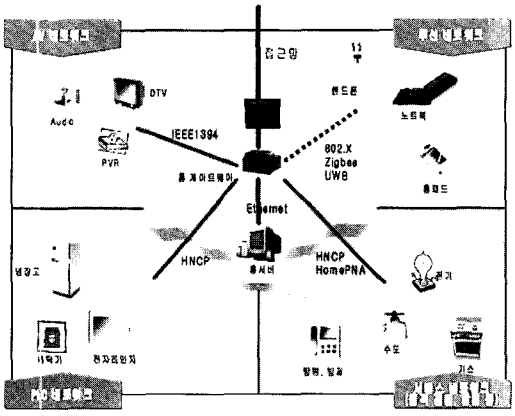
유비쿼터스(Ubiqitous)사용자가 네트워크나 컴퓨터를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 정보통신 환경이다.

물이나 공기처럼 시공을 초월해 '언제 어디에나 존재한다'는 뜻의 라틴어(語)로, 사용자가 컴퓨터나 네트워크를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 환경을 말한다. 1988년 미국의 사무용 복사기 제조회사인 제록스의 와이저(Mark Weiser)가 '유비쿼터스 컴퓨팅'이라는 용어를 사용하면서 처음으로 등장하였다. 와이저는 유비쿼터스 컴퓨팅을 메인프레임과 퍼스널컴퓨터(PC)에 이어 제3의 정보혁명을 이끌 것이라고 주장하였는데, 단독으로 쓰이지는 않고 유비쿼터스 통신, 유비쿼터스 네트워크 등과 같은 형태로 쓰인다. 곧 컴퓨터에 어떠한 기능을 추가하는 것이 아니라 자동차·냉장고·안경·시계·스테레오장비 등과 같이 어떤 기기나 사물에 컴퓨터를 집어넣어 커뮤니케이션이 가능하도록 해 주는 정보기술(IT) 환경 또는 정보기술 패러다임을 뜻한다. 유비쿼터스화가 이루어지면 가정·자동차는 물론, 심지어 산 꼭대기에서도 정보기술을 활용할 수 있고, 네트워크에 연결되는 컴퓨터 사용자의 수도 늘어나 정보기술산업의 규모와 범위도 그만큼 커지게 된다. 그러나 유비쿼터스 네트워크가 이루어지기 위해서는 광대역통신과 컨버전스 기술의 일반화, 정보기술 기기의 저가격화 등 정보기술의 고도화가 전제되어야 한다. 이러한 제약들로 인해 현재 일반화되어 있지는 않지만, 휴대성과 편의성뿐 아니라 시간과 장소에 구애받지 않

고도 네트워크에 접속할 수 있는 장점들 때문에 세계적인 개발 경쟁이 일고 있다.

2.2 홈네트워크(Home Network)

홈네트워크란 TV, 냉장고, 에어컨 등 집안의 가전제품과 안방, 부엌, 거실, 현관 등 집안의 각 공간을 인터넷을 통해 연결, 정보를 전달해 휴대전화 등을 통해서도 작동이 가능토록 하는 미래형 가전 시스템을 말한다. 홈네트워크는 가정 내의 정보가전기기가 네트워크로 연결돼 기기, 시간, 장소에 구애받지 않고 서비스가 이뤄지는 미래 가정환경인 '디지털 홈'을 구성하는 것이다. 초고속 인프라를 기반으로 다양한 IT(정보기술) 기기를 활용해 원격교육, 엔터테인먼트, 헬스케어, 정보가전 제어 등을 할 수 있는 '디지털 컨버전스(융합)'의 대표적인 서비스인 꿈의 테크널러지라고 할 수 있다.



(그림 1) 홈네트워크 서비스 개요

홈네트워크를 설치하면 방에 앉아서 초인종을 누른 사람과 세탁 종료 여부를 확인 할 수 있다. 홈네트워크 체제에서 이용자는 PDA나 휴대폰으로 집에서 리모콘으로 TV를 조정하듯 외부에서 자신의 집을 모니터링 할 수 있고 퇴근 전에 사무실에서 집안 온도를 조정하고 바깥에서 신호를 통해 밥을 지을 수 있고 건강 검진도 자동으로 받아볼 수 있게 된다.

3. 홈 네트워크 보안환경

네트워크에는 홈패드, 홈서버, 홈게이트웨이 등 많은 수의 기기들이 존재하는데, 그 중에서 현재 상용화되고 있는 것이 홈 게이트웨이 분야이다. 홈서버의 경우도 홈게이트웨이의 보조 역할을 할 것으로 기대하고 있지만 단독으로 홈서버 제품을 출시하지는 않고 있다. 현재 홈게이트웨이 홈서버 제품을 출시하지는 않고 있다. 현재 홈게이트웨이는 2001년 12월에 정보통신표준협회를 통하여 표준을 제정하였다. 하지만 최근에 홈게이트웨이에는 이더넷(Etherner), PLC, IEEE1394등의 많은 프로토콜과 서비스 등이 탑재되고 있어 좀 더 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 AAA인증과 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 주건공간엔 이미 배선이 돼 있어서 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 뒷받침해 줄 필요가 있다.

HomePNA는 기존의 구축된 전화망을 이용하여 고속의 댁내 망을 구축하기 위한 기술로서 현

재 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.

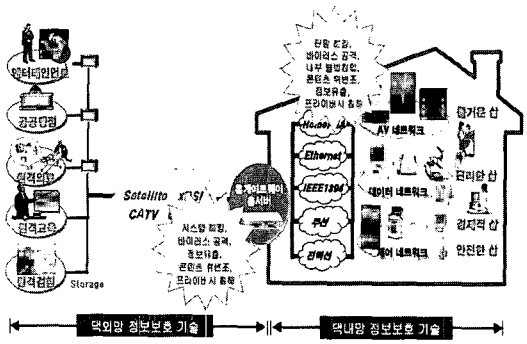
PLC 기술은 전력선을 이용한 통신기술로서 가스 검침·원격 제어·보안(CCTV)·오디오(AV) 등 다양한 분야의 애플리케이션이 최근에 출시되고 있다. 무선망의 경우 현재 속도 부분에서는 많은 개선이 이루어지어 802.11X 계열의 경우 54Mbps(802.11g)까지 개발되었지만, 보안성 검토를 해보면 802.11b를 사용해야 최소의 보안성을 보장하고 있고, 좀 더 나은 보안성으로 유지하기 위해서는 802.11i 수준이 필요하다. 무선망에서는 2Mbps이내의 전송이 가능한 HomeRF 2.01을 발표하였다. 발표 스펙에서는 시큐리티 요소와 관련하여 보안 구조(Security architecture) 부분을 명시하고 있다. 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.

블루투스(Bluetooth)는 블루투스 SIG에서는 3가지 보안 모드를 제공하는데, 신뢰받은 단말기(trusted device)에 대해서는 무제한으로 모든 서비스가 사용이 가능해 보안상의 취약점을 내포하고 있다. 필란드의 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 노출됐는지조차 확인할 수 없는 실정이다.

홈 네트워크에서는 다양한 유·무선 네트워크와 프로토콜 등의 혼재로 기존 인터넷 등에서 발생되던 보안취약성외에도 추가적으로 고려해야할 보안 취약성이 존재하고 있다. 즉, 홈 네트워크 내의 정보기기의 다양성과 기기간 자원의 공유 등으로 보안측면에서 고려해야할 요구사항은 더욱 복잡하고 다양한 특성을 지니게 된다. 더욱이 홈네트워크의 정보가 전기기들은 상대적으로 컴퓨팅 능력이 낮아 강력한 보안기능의 탑재가 어려우므로 사이버공격에 이용되거나 목표가 될 가능성이 더욱 높다고 할 수 있다.

홈 네트워크에는 Ethernet, HomePNA, PLC, IEEE802.1x, Bluetooth, UWB(Ultra Wide Band) 등 다양한 홈네트워킹 기술이 사용 가능하나 홈네트워크 측면에서 매체의 보안취약성을 해결 할 수 있는 대응 기술을 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.

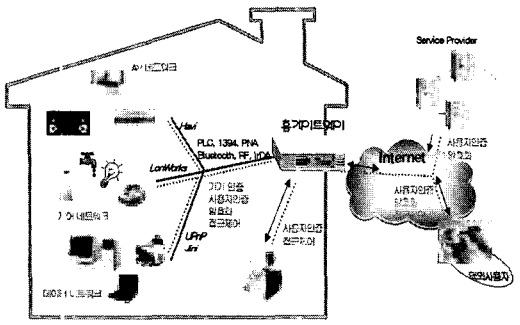
(그림 2)는 홈 네트워크에서 발생될 수 있는 보안 취약성을 정리한 그림이다. 인터넷 등에서 발생되던 취약성이 홈 네트워크 내부망에서도 그대로 발생됨을 알 수 있으며, 내부망의 복잡함을 고려할 때 우선적으로 종합적인 보안프레임워크를 정립하는 것이 필요하겠다.



(그림 2) 홈 네트워크의 보안 취약성

(그림 3)은 홈네트워크에서 발생될 수 있는 보안 취약성을 해결하기 위해 요구되는 보안기능을 정리한 그림이다.

홈 네트워크를 구성하는 다양한 통신매체나 프로토콜 등과 관계없이 요구되는 보안기능을 만족할 수 있는 보안프레임워크가 정립되어야 하며, 홈 네트워크의 발전전망을 고려하여 현재 추진 중인 시범서비스에서 연동될 수 있는 수준의 보안기술과 향후 유비쿼터스 컴퓨팅환경에 근접한 홈 네트워크 모델에서 활용될 수 있는 보안기술로 나누어 실질 적인 기술개발을 추진하는게 효율적이겠다.



(그림 3) 홈네트워크 보안 취약성 대응을 위한 보안기능

4. 침해 위협 및 대응방안

유선망에서는 도청 및 신분 위장이 계속해서 존재하고 서비스 거부와 같이 홈 게이트웨이를 무력화 시킬 수 있는 부분이 존재한다. 특히 홈 네트워크에서는 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 형태의 서비스 거부(Denial of Service) 공격에 노출될 수 있다. 무선망의 특성상 네트워크에 접속하려는 단말에 대해서는 계속해서 연결 요청을 하려고 하는데, 이러한 연결요청이 하나의 AP에 가상(Virtual)으로 다수가 요청될 경우 신규로 접속을 요구하거나, 현재 접속한 단말에서도 서비스가 불가한 경우가 생길 수 있다. 이상에서 살펴본 홈 네트워크 환경을 바탕으로 기본적인 침해 유형을 살펴보면 다음과 같다.

〈표 1〉 홈 네트워크 침해 유형

공격유형	공격내용	대 상
도청	중요데이터, 특정 서비스의 기능 등에 대한 정보수집	접근망 패킷 댁내망 패킷
신분위장	홈 네트워크 프로토콜의 취약점을 이용(IP spoofing, Prediction 등) 하여 정당한 사용자나 시스템으로 위장	홈게이트웨이 댁내망
서비스거부공격	네트워크 사용량 초과, 메일폭탄 대량의 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 대응방법을 이용한다면 일반적인 공격에 대해서는 대응 할 수 있을 것이다. <표 2>는 홈네트워크의 개념적 대응 방안을 명시하였다.

〈표 2〉 개념적 대응방안

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

5. 결론 및 향후 연구방향

현재 국내 홈 네트워크 서비스는 정보통신부에서는 "디지털 라이프 홈 구축계획"을 발표하면서 가정을 누구나 기기, 시간, 장소에 구애받지 않고 다양한 홈서비스를 제공받을 수 있는 디지털 생활 공간으로 전환하고, 2007년까지 천만가구에 디지털 홈 구현을 위한 홈 네트워크를 구축할 것이라는 비전을 제시했다. 이와 같이 정부의 산업육성 정책과 산업체들의 적극적인 시장참여로 홈 네트워크 분야 활성화를 통한 경제적, 사회적 기대가 높아만 가고 있지만 안전성이 확보되지 않은 홈서비스는 사용자로부터 외면 받을 수밖에 없고 더욱이 홈서비스에 따라 개인의 경제손실뿐 아니라 생명까지도 위협받을 수도 있으므로 홈서비스 활성화에 있어 보안기술이 차지하는 중요성은 매우 크다고 할 수 있다.

향후 홈 네트워크에서 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 프레임워크를 개발하고, 이를 적용한다면 최소한의 사용자 정보보호가 이루어 질 것이다.

일차적으로 홈 네트워크 사용자들은 홈 네트워크가 새로운 패러다임이 아니라는 것을 숙지하여 기존의 취약점에 대해서라도 방지할 필요가 있다. 또한 다양한 기술과 기기가 혼재되어 있는 홈 네트워크에서는 이기종 프로토콜간의 침해가 일어날 수 있고, 좀 더 복잡한 유형의 공격이 발생될 수 있기 때문에 이에 대한 대응 방안도 고려해야 한다. 추가적으로 홈 네트워크에 가장 중요한 것이 개인 정보 보호일 것이다. 가장 많이 산재되어 있는 개인정보를 보호하기 위해서 홈 네트워크 특성이 고려된 접근제어 및 인증 기술이 연구되어야 할 것이다.

참 고 문 헌

[1] CEO Information, "가정의 디지털 혁명, 홈 네트워크", 삼성경제연구소, 2003. 12.

[2] 유동영 외, "홈 네트워크 침해 위협에 대한 홈 게이트웨이 보안 요구 및 대응 방안", 한국정보처리학회, 추계학술 발표대회 논문집, 2004.

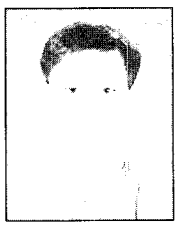
[3] 이윤철, "최근의 홈네트워크 기술동향 및 시장 전망", 주간기술동향, 제1098호, pp. 22-33, 2003.

[4] 한종수, 유비쿼터스 기술(RFID와 홈네트워킹), 세화, 2005.

[5] 양재수, 유비쿼터스 홈 네트워킹 서비스, 전자신문사, 2004.

오 대 균

1984년 한남대학교 경영학과 (경영학사)
1992년 한남대학교 대학원 컴퓨터공학과(공학석사)
2003년 한남대학교 대학원 컴퓨터공학과(공학박사)
1979년~현재 한국 에너지 기술연구원 창업보육센터 센터장
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 모바일 컴퓨팅, 정보보호



정 진 영

1992년 한남대학교 전자계산학과 (공학사)
1994년 한남대학교 대학원 컴퓨터공학과(공학석사)
2002년 한남대학교 대학원 컴퓨터공학과(공학박사)
2004년~현재 대전보건대학 멀티미디어과 조교수
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 모바일 컴퓨팅, 정보보호