홈네트워크 환경에서의 보안공격에 따른 보안강화 연구

김여진*, 송오영*, 박세현*
*중앙대학교 전자전기공학부

Strengthen the Security as a result of Attack in Home Network Environment

Yeo-Jin Kim*, Oh-Young Song*, Se-Hyun Park*
*School of electrical & electronics engineering, Chung-ang University.

요 약

홈네트워크 시스템을 구성하기 위해서는 유무선 네트워크 기술과 미들웨어 기술, 홈게이트웨이 기술 등의 다양한 기술들을 필요로 한다. 이러한 홈네트워크 환경에서 공격에 대한 가능성이 점차 증대할 것이고, 따라서 홈네트워크 보안에 대한 연구 및 개발에 대한 필요성 또한 증대되고 있다. 따라서 본 논문에서는 홈네트워크 보안의 필요성과 이에 저해되는 요소 및 그에 대한 대응책을 기술하고자 한다.

I. 서론

언제, 어디서나 컴퓨팅이 가능하다는 유비쿼터스 컴퓨팅시대에서 개인의 컴퓨팅 환경의존도가 증가함에 따라 각종 공격에 의한 개인생활의 위협 또한 증가할 수 밖에 없다. 더욱이 앞으로 유비쿼터스 서비스가 활성화되면서 이러한 공격으로부터 개인의 재산뿐만 아니라, 생명까지도 위협에 처할 수 있는 상황이 생길 수 있다. 이런 관점에서 볼 때, 유비쿼터스 컴퓨팅 환경으로 가는 시작점이라 할 수 있는 홈네트워크의 활성화에 있어 이러한 공격의 증가는 장애물로서 대두될 것이 틀림없으므로 이에 대한 대응책 마련이 시급하다고 할 수 있다.

홈네트워크는 인터넷 가전제품을 손쉽게 연결, 사용할 수 있게 함과 동시에 사생활, 개인정보보호대책 또한 제공해야 한다. 최근 들어 인터넷을 통한 가정내 불법침입, 유무선 통신감청 등의 위험을 막기위해 가입자망, 유무선 댁내망, 홈게이터웨이, 응용서비스 등에 대한 보안대책이 필요하다는 지적이 나오고 있다.

본 논문에서는 현재의 홈네트워크 시스템에서의 취약점과 개발동향 및 보안서비스의 전망에 대해 기술해보고자 한다.

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터(중앙대학교 홈네트워크 연구센터) 지원 사업의 연구결과로 수행되었음

II. 본론

1. 홈네트워크 보안기술 동향

1.1 홈네트워크 동향

홈네트워크 서비스가 편리하고 안전하게 제공되기 위해서는 홈네트워크 환경에서의 보안 요구사항 및 구현방안에 대한 중요도는 매우 높으나, 기업의 정보보호 구현 시스템이나 정책에 비해 상대적으로 연구가 활발치 못하다. 특

히 홈네트워크는 컨텐츠, 활용기술, 구현솔루션 등이 외부 네트워크 환경인 인터넷망과의 연동이 불가피하므로 공중망에서 발생할 수 있는 해킹이나 바이러스 침투 등의 위험에 노출되어 있다.

1.2 홈네트워크 보안의 필요성

현재 홈네트워크 서비스를 추진하고 있는 모습을 살펴보면, 단순하게 기존의 홈오토메이션(Automation) 확장 차원을 넘어서, IT인프라와의 컨버전스를 모색하고 있다. 이에 따라 우리가 현재까지 발견하지 못한 보안문제를 그대로 홈네트워크 시스템에서도 지니고 있고, 홈네트워크 신규기기에서 발생될 수도 있는 보안문제 또한 드러날 수 있다.

2. 홈네트워크의 취약성

2.1 접근망 취약성

접근망의 홈게이트웨이를 기준으로 외부서비스 사업자와 연동되는 망을 말하며, 댁내망 접속지점에 대한 네트워크 패킷수집을 통하여 사용자 ID 및 그 밖의 중요정보 등이 노출될 수 있다. 현재 홈네트워크에서 사용자정보는 홈네트워크 시범사업자에 의한 암호화채널을 제공하는 형태로 보호하고 있으나, 그 외의 개별 사업자들의 서비스제공방식은 잘 알려지지 않고 있는 실정이다.

2.2 댁내망 취약성

댁내망에는 댁내에서 처리하고 관리하기 위하여 기존 홈에 설치되어있는 기술을 이용하여 구축하는 방식과 새로운 선로를 설치하여 구축하는 방식으로 나눌 수 있고, 여기에 유선과 무선이 혼용되어 사용된다. 유선에는 Home PNA와 PLC와 같은 기존기술과 USB, IEEE 1394, Ethernet과 같이 새로운 구축을 필요로하는 기술들이 있고, 무선에는 Home RF, Bluetooth, Wireless LAN IEEE 802.11, Wireless IEEE 1394, IEEE 802.15 등과 같은 기술이 있다. 이러한 네트워크 기술이 궁극적으로 댁내 홈기기와 연동하여 서비스를 제공하는 이러한 연동의 취약점과 기술자체의 취약점으로 인해 많은 보안위협이 노출되게 된다.

<표 1> 보안 취약점 및 요구사항

구분		보안 취약점	보안 요구사항
홈게이트웨이(홈서버)		- 외부망으로부터의 해킹, 악성코드, 웜 및 바이러스 차단, DOS, 유무선통신의 도청(sniffering) 차단 등의 외부 보안 침입 - 내부 정보가전기기 간 메시지/데이터유출, 비인증기기의 연결	- 사용자와 기기간 인증기능 - 접근제어 - 디바이스 보안기능 관리 - 침입방지(차단, 탐지) 기능 - VPN기능 - 전송데이터/제어정보의 무결성 - 서비스정보에 대한 기밀성
네트워크	외부망	- 외부인터넷망으로부터의 보안침해	- 사용자 인증 및 기기간 인증기능 - 접근제어 기능 - 무결성 및 기밀성 - VPN기능 - 서비스 정보에 대한 기밀성
	내부 유선망	- 망연결 장비의 DOS공격 위험 - 데이터 송수신시 제어정보/데이터의 유출과 위변조 위험 - 인증 및 개인 프라이버시 침해	
	내부 무선망	- 망개방에 따른 도청 등의 정보유출 위험 존재 - 인증기술 미적용에 따른 위험 - 망연결 장비의 DOS공격 위험	
정보가전기기		- 웜 및 바이러스에 노출 위험 - 통신선로상의 데이터 유출 - 데이터 손실 - 기기의 물리적 손상 - 해킹 및 불법침입 등의 사생활 침해 위험 - 지불관련 데이터 유출 및 사용자인증, 개인프라이버시 유출	

3. 보안요소 및 고려사항

3.1 보안요소

- 데이터 기원 인증: 메시지를 인증하기 위하여 특정한 소스로부터 왔다는 것을 확립하여야 한다. 점검값을 이용한 관용 암호화와 디지털 서명을 이용한 공개키 방법이 사용
- 명령권한 검증: 어떤 사용자가 어떤 일을 수행하기 위한 명령에 대해 정당한 권한이 있는지 검증
- 메시지 무결성 보호: 입력 메시지에 대해 정당하지 않은 데이터의 변경이 없음을 보증하는 기능
- 메시지 재생 방지: 임의의 메시지를 공격자가 중간에서 가로채 나중에 재사용되는 것을 방지
- 데이터 비밀성: 메시지 내용을 암호화
- 키 분배: 완전한 보안혜택을 위한 키 분배

3.2 홈네트워크 보안 고려사항

홈네트워크에서는 이종의 유무선 네트워크와 다양한 프로토콜 등의 혼재로 기존 인터넷 등에서 발생하던 보안취약성 외에도 다양한 취약성에 대한 보완이 대두되고 있다.

- 권한 검증(authentication): 각 장치에서 무슨 조치를 취하고, 데이터를 접근하기 위하여 어떤 것이 허용되는가?
- 기밀성(confidentiality): 어떤 것이 장치로 전달되는 메시지를 읽도록 허용되는가?

홈 서버/ 게이트웨이를 통해서 전달되는 사용자와 서비스제공자의 정보가 부정한 사용자 및 위험으로부터 보호되어야 하며, 동시에 사용자와 집안의 정보에 대한 프라이버시가 보호되어야 한다. 또한 침입, 해킹, 바이러스 등과 같은 외부침입 행위에 대한 방어기능도 필요하다.

이를 위해서는 홈네트워크를 구성하는 다양한 통신매체나 프로토콜 등과는 관계없이 요구되는 보안기능을 만족할 수 있는 프레임워크가 정립되어야하며, 홈네트워크의 발전전망을 고려하여 현재 추진 중인 시범서비스에서 연동가능한 보안기술과 향후 유비쿼터스 컴퓨팅 환경에 근접한 홈네트워크 모델에서 활용될 수 있는 보안기술에 대한 검증이 이루어져야 한다.

3.3 보안대책

위에서 명시한 홈네트워크 보안 공격 유형들은 기존의 유,무선망을 그대로 수용하여 홈네트워크의 인프라를 구축하고, 부가적으로 홈네트워크에 필요한 부분만을 통합하는 형태로 서비스가 구축된 것이 그 원인이다. 그러므로 현재 우리가 대응하고 있는 각종 네트워크 공격에 대한 대응방법을 이용한다면 일반적인 공격에 대해서는 대응할 수 있을 것이다.

<표 2> 대응방안

대책	보안 매커니즘
인증	- 최소의 패스워드 기반 인증 - 인증서 기반의 인증
접근통제	- 사용자 권한 기반의 접근제어 - 접근통제목록, 사용자 및 가용목록 이용
데이터 비밀성	- 메시지 암호화 - 패킷필터링 라우팅/방화벽 기능 이용
모니터링	- 접근제어 정보의 변경에 대한 로그 - 감사 도구의 사용

III. 결론

홈네트워크 서비스를 창출하는데 있어 기술의 진보와 사용자의 편리성을 고려하는 것은 당연하다. 하지만 사용자에게 발생될 여러 가지 불편사항을 무시하는 서비스는 결코 성공할 수 없으며, 이러한 불편사항 중 서비스 장애를 통한 불편은 단순한 서비스 복구를 통해 해결되지만, 보안관리 부재로 인한 불편은 심각한 문제를 초래할 수 있다. 홈네트워크 해킹을 통한 사용자의 개인정보나 금융정보는 단순히 타인이 그 정보를 습득하는 것으로 그치지 않고, 이를 악용하려는 의도가 많기 때문에 사고발생 후 손실비용이 만만치 않다.

현재 국내 홈네트워크 서비스는 각 홈네트워크 산업분야의 기술개발에 치우쳐있다. 이러한 개발주도의 서비스는 사용자의 편의성만을 강조하고 사용자의 정보보호에는 무관심해질 수 있다. 그러나 홈네트워크 산업이 활성화되면서

홈네트워크 보안과 관련하여 기존의 인프라들이 갖고있는 취약성뿐만 아니라, 다양한 기술과 기기의 혼재에서 발생하는 이기종 프로토콜간의 침해와 좀 더 복잡한 유형의 공격에 대한 대응방안을 마련해야 한다. 또한 산재되어있는 개인정보를 보호하기위한 접근제어 및 인증기술에 대한 연구가 시급하다.

아울러 좀더 나은 서비스를 제공하기위해 차별화된 보안서비스를 개발하여 사용자들에게 보안의 필요성을 인지시키고, 서비스 수준에 따라 안전이 보장된다는 인식의 전환 또한 필요하다.

[참고문헌]

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

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

[3] Interopertable Home Infrastructure Home Network Security, Intel Technology Journal, Carl M.Ellison, 2002

[4] 홈네트워크 관련정책 및 기술 취약성, 제1회 홈네트워크 시큐리티 워크샵, 김태근 정보통신연구진흥원, 2004

[5] 유비쿼터스 홈네트워크 환경에서의 침해위협 및 대응방안, 유동영, 김영태, 노병규 한국정보보호진흥원, 2004 학술발표논문집 한국정보과학회

[6] 홈네트워크 서비스에서 정보보호 필요성 및 고려사항, 유동영, 한국정보보호진흥원, 2005