홈네트워크 보안 취약점에 대한 대응 방안

권성구* 황은영* 성윤종* 이준희* 송오영* 박세현*
*중앙대학교 전자전기공학부

A Solution for Home Network Security Weaknesses

Sunggu Kwon*, Eunyoung Hwang*, Yunjong Sung*, Junhee Lee*
Ohyoung Song*, Sehyun Park*
*School of Electrical & Electronics Engineering, Chung-ang University.

요 약

홈네트워크는 무궁한 발전 가능성을 가지고 있으면서 동시에 여러 분야의 기술들을 유기적으로 결합하여 사용하기 때문에 기존의 네트워크 서비스에서 가지고 있던 보안 취약성에 그대로 노출되어 있다. 또한 요소기술 및 환경 등의 특성으로 홈네트워크 정보기기에 대한 불법적인 공격이 빈번하게 발생할 수 있다. 홈네트워크 산업을 활성화시키기 위해서는 이기종 망간의 상호연동 기술은 물론 관리적 측면에서의 기술과 통합 측면에서의 기술 등이 필요하고 정보의 처리, 전달 및 저장을 안전하게 하기 위해서는 특히 보안 기술이 절실히 요구된다. 따라서 본 논문에서는 프라이버시, 네트워크, 서비스, 인프라, 미들웨어 및 디바이스의 측면으로 나누어서 홈네트워크에서의 보안 취약점을 분석하고, 홈네트워크 환경에서의 보안 요구사항을 도출함으로써 이와 같은 보안 위협으로부터의 대응방안을 제시한다.

I. 서론

현대 사회는 인터넷 사용에 대한 욕구 증가와 무선통신기술의 발달 과정을 통해 가정 내에서 통신망을 구축한다는 좁은 의미의 홈네트워크에서부터 시작되어, 현재는 다양한 분야가 결합되어 커다란 시너지를 창출하는 복합 멀티미디어 산업으로서의 홈네트워크로 의미가 확장되었다[1]. 홈네트워크는 홈 내부에 위치한 어떠한 정보 기기 간에도 네트워크로 연결이 가능하고 원격지로부터도 네트워크를 통하여 정보 기기의 제어 및 관리가 가능한 통신 서비스 환경을 구현하는 홈 정보제어시스템 및 서비스, 솔루션을 총칭하는 개념으로써, 네트워크를 통하여 기기·시간·장소에 구애받지 않고 다양한 홈 서비스가 제공되는 미래 가정환경인 디지털 홈을 구성하는 핵심요소이다. 홈네트워크는 IT839 전략에서도 8대 신규서비스 및 9대 신성장동력에 선정될 만큼 현재 가장 주목받고 있는 차세대 IT 기술로 손꼽히고 있다.

이러한 홈네트워크는 무궁한 발전 가능성을 내재함과 동시에 여러 분야의 기술들을 유기적으로 결합하여 사용하기 때문에 기존 보안 문제에 대한 취약성을 그대로 포함하고 있다. 또한 요소기술 및 환경 등의 특성으로 인해 홈네트워크 정보기기에 대한 불법적인 공격이 빈번하게 발생할 수 있으며, 이러한 공격은 개인의 프라이버시 침해 뿐만 아니라 개인의 생명 및 자산까지 직접적인 피해를 줄 수 있어 보안 취약성에 대한 대응책 마련이 매우 시급한 실정이다.

따라서 본 논문에서는 홈네트워크 환경에서의 보안 요구사항을 도출하고 홈네트워크 환경에서의 보안 취약점들을 분석함으로써, 이에 대한 대응 방안을 제시한다.

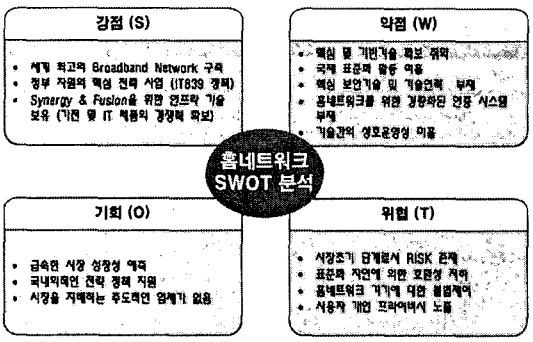
본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터(중앙대학교 홈네트워크 연구센터) 지원 사업의 연구결과로 수행되었음

II. 본론

1. 홈네트워크 환경에서 보안의 필요성

홈네트워크는 홈 내부에 위치한 어떠한 정보기기 간에도 네트워크가 가능하고, 원격지로부터도 네트워크를 통하여 기기의 제어 및 관리가 가능한 통신 서비스 환경을 구축하기 위한 것이다. 홈네트워크 산업을 활성화시키기 위해서는 이기종 유, 무선 네트워크 망간의 상호 연동 기술은 물론 관리적 측면에서의 기술과 통합 측면에서의 기술 등이 필요하고, 또한 정보의 처리, 전달 및 저장을 안전하게 하기 위해서는 특히 보안 기술이 절실하게 요구된다.

다음 <그림 1>의 홈네트워크에 대한 SWOT 분석으로부터, 홈네트워크 환경에서 여가가지 취약점들이 산재해 있으므로 안전한 홈네트워크 환경을 구축하기 위해서는 특히 보안에 대한 대책 마련이 시급하다는 것을 알 수 있다.

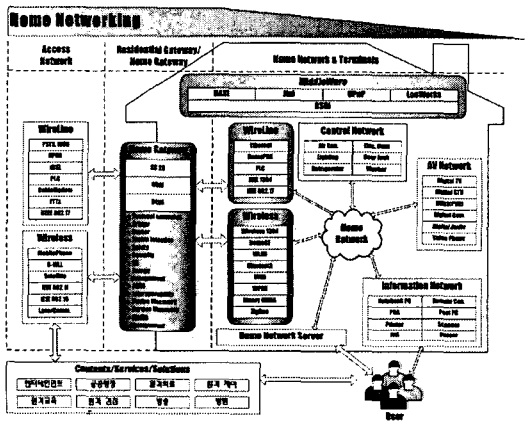


<그림 1> 홈네트워크에 대한 SWOT 분석

<그림 1>과 같이, 홈네트워크는 무궁한 발전 가능성을 내재함과 동시에 여러 분야의 기술들을 유기적으로 결합하여 사용하기 때문에 기존의 유·무선 네트워크에서의 보안 취약성을 그대로 포함하고 있다. 또한 홈네트워크는 요소기술 및 환경 등의 특성으로 인해 홈네트워크 정보기기에 대한 불법적인 공격이 빈번하게 발생할 수 있으며 이로 인한 개인의 프라이버시 침해는 물론 자산까지 직접적인 피해를 줄 수 있으므로 이에 대한 대응책 마련이 필요하다.

2. 홈네트워크 환경에서의 보안 취약점

다음 <그림 2>는 홈네트워크 환경 및 구성요소를 도시한 것이다. 홈네트워크 기술은 외부의 인터넷과 접속을 가능하게 해 주는 유·무선 외부 네트워크, 내·외부 네트워크간 인터페이스 역할을 하는 홈게이트웨이, 홈서버, 이더넷, 전화선, 전력선, 무선 등으로 내부 네트워크를 연결하는 홈네트워킹, 홈네트워킹 기능이 추가된 정보기기 및 정보가전들을 제어하며 상호연동을 위한 미들웨어로 나뉜다[2].



<그림 2> 홈네트워크 전체 기술 구조도

현재의 홈네트워크 환경은 상호연동적인 측면, 컨버전스적인 측면, 관리적인 측면에서 중요한 보안상의 취약점들이 있다. 본 논문에서는 이러한 홈네트워크 환경에서의 보안상의 취약점들을 프라이버시, 네트워크, 서비스, 인프라, 디바이스 및 미들웨어의 측면으로 나누어서 분석하였으며, 이에 대한 내용은 다음의 <표 1>과 같다[3].

<표 1> 홈네트워크 환경에서의 보안 취약점

프라이버시
• 이기종 네트워크 연동시 발생할 수 있는 프라이버시 정보 유출 위험 증가 • 세분화된 context로 인한 사용자의 프로파일에 대한 데이터 유출 가능성

• 카메라의 네트워크화로 인한 개인 프라이버시 침해 가능성 • 홈네트워크의 지능적 맞춤형 서비스로 인한 개인의 등급화 초래
유·무선 네트워크
• 여러 회사의 가전기기간 상호 운용 기술 부족 • 다양한 무선 기기들간의 전파 간섭 • 다양한 네트워크 간 로밍시 원활한 인증 체계 부족 • 유·무선 네트워크 연동시 유선 수준의 seamless한 보안 유지의 어려움 • 무선 네트워크에서의 최소 전달 지연 보장의 어려움
서비스
• 다양한 서비스를 위한 context 기반의 다양한 보안 서비스 정책 부족 • 컨텐츠 불법 복제 및 재배포 방지 기술 미비 • 다양한 서비스를 위한 context 기반의 다양한 처리 능력 부족 • 통합망에서 발생할 수 있는 불법 컨텐츠 접근 제어 기술 부족
인프라
• 광대역화로 인한 악성코드 등의 전파 속도 증가 문제 • 통합망 관리 및 제어를 위한 신호의 보안 기술 미비 • 기존의 네트워크 망으로의 외부 공격 확산 문제 • 통합망과 IPv6 지원으로 더욱 복잡하고 다양한 형태의 단말 공격 가능성
디바이스 및 미들웨어
• 디바이스 인증 및 접근 권한 제어에 대한 통합적인 관리가 취약 • 다양한 디바이스 인증을 위한 미들웨어 기술 취약 • 미들웨어간 상호 연동성 부족으로 보안 관리의 어려움

보안의 위협은 단순한 정보 유출로부터 서비스 공격, 인프라 공격, 융합 공격의 형태로 그 공격 형태가 날로 복잡해지고 또한 보안에 대한 위협의 정도도 날로 증가하고 있다. 따라서 정보보호 기술의 패러다임 역시 단일 보안 기술에서 통합 보안 기술의 형태를 거쳐서 convergence 보안 기술의 형태로 발전해 가고 있으며, 요구되는 정보보호에 대한 보안기술 또한 더욱 더 고도화되고 지능화 되는 추세를 보이고 있다[4][5].

3. 홈네트워크 환경에서의 보안 요구사항

홈네트워크 보안은 일상생활과 밀접하게 연관된 정보 가전기들에 내장되어야 하므로 경제적이고 높은 신뢰성을 제공해야 한다. 이와 동시에 침입을 실시간으로 차단할 수 있는 침입방지 시스템, 사용자/정보 가전기기 인증 기술과 메시지/데이터 암호화 기술들이 유비쿼터스 홈네트워크 환경으로의 효과적 적용이 요구된다. 또한, 최근 홈네트워크 환경은 이동성과 편리성, 보안성이 차지하는 부분이 점차 커짐에 따라 디렉토리 서비스(directory service)를 기반으로 각각의 조직과 사용자의 필요에 따라 네트워크 사용 권한을 부여하는 인증 중심의 통합 보안 솔루션 도입도 고려해야 한다[6].

기존의 홈네트워크 보안 기술들과 앞에서 분석한 보안 취약점들을 바탕으로 보다 안전한 홈네트워크 환경 구축을 위해서 프라이버시, 네트워크, 서비스, 인프라, 디바이스 및 미들웨어의 측면에서 홈네트워크 환경에서의 보안 요구사항은 다음과 같다.

<표 2> 홈네트워크 환경에서의 보안 요구사항

프라이버시
• 이기종 네트워크 연동시 발생할 수 있는 프라이버시 정보 유출 방지 • 권한 및 역할에 따른 정책적인 개인정보조회 방안 • RFID 태그와 리더간 전파 도청으로 인한 프라이버시 정보 유출 방지
유·무선 네트워크
• 유·무선 네트워크 간의 상호 연동성 보장 • 홈네트워크와 외부 통합망과의 안전한 로밍 기술 • 원격 제어 등의 홈네트워크 사용자에 적합한 접속 메커니즘

• 기존 네트워크와 동등한 수준의 홈네트워크 환경에서의 정보 암호화 기술
서비스
• 홈네트워크에서의 다양한 보안 인증 서비스의 QoS 보장 • context 기반의 다양한 보안 서비스 정책 • 컨텐츠의 적법한 사용을 위한 라이센스 및 키 관리 기술 • 전체 서비스 통합 및 관리를 위한 홈 게이트웨이 기술
인프라
• 통합망과의 연동시 홈네트워크 인터페이스에서 발생할 수 있는 병목현상 및 지연 방지 • 통합망에서의 보안 피해에 대한 홈네트워크로의 확산 방지 • IPv6로의 전환 및 BcN 통합을 위한 보안 정책 표준화
디바이스 및 미들웨어
• 홈네트워크 디바이스에 적합한 암호화 메커니즘 • 디바이스 인증, 접근 권한 제어의 통합 관리 플랫폼 필요 • context-aware 미들웨어 보안 기술 • 홈네트워크 환경에 적합한 보안 프레임워크 및 미들웨어 기술 • 미들웨어 기반 지능적 보안 인증 체계

4. 홈네트워크 보안 취약점에 대한 대응방안

홈네트워크 환경에서는 다양한 이기종 네트워크의 통합 및 이기종 기기간의 연동으로 다양한 보안 취약점들이 존재하고 이로 인해 많은 위험에 노출될 수 있다. 또한 보안 취약성에 대응하는 다양한 보안 기술이 개발, 적용되고 있으나 몇몇의 기술과 장비만으로는 모든 공격에 대응하는 것은 현실적으로 불가능하다는 것은 이미 잘 알려진 사실이다. 이에 따라 홈네트워크 구축 및 사용에 있어서 최신 보안기술의 사용이나 환경 설정 등을 비롯해서 많은 주의를 필요로 한다[7]. 따라서 본 절에서는 홈네트워크 환경에서 발생할 수 있는 보안 취약점에 대한 대응방안을 다음과 같이 제시한다.

<표 3> 홈네트워크 보안 취약점 대응방안

고도화된 지식기반 미들웨어 기반의 홈네트워크 보안 통합 관리 지원
• Intelligent Automation Service에 대한 보안 인증 및 서비스의 QoS 보장 • Multi-user Context-aware Service에 대한 지원으로 다중 사용자 환경에서 발생할 수 있는 conflict에 대한 문제 해결 및 상황인지 기반의 통합 인증 서비스 지원 • 원격 검침과 제어 등 과금 시스템과 관리 시스템간의 보안 기술 연동
유, 무선 네트워크 및 BcN, IPv6 기반 인프라와의 상호 연동성 보장
• 유, 무선망에서의 상호 연동성을 보장하며 이기종망 간의 통합 인증에 대한 보안을 지원하고 안전한 로밍에 대한 보안 기술을 제공 • Wireless LAN, Bluetooth, UWB, ZigBee, Binary CDMA, 무선 IEEE1394, HomeRF 등의 상호연동에 대한 표준화 작업을 지원 • 홈네트워크 환경에서 사용되는 다양한 이기종 네트워크 망간의 상호 연동을 지원함으로써 Seamless한 서비스 제공 및 QoS 보장 • IPv6로의 전환 및 BcN 통합 정책을 마련하여 네트워크에서 발생할 수 있는 병목현상 및 지연에 대한 방지 대책을 수립하고 BcN망으로의 통합 네트워크 환경에서 더욱 급격하게 퍼질 수 있는 보안 피해에 대한 확산 방지 기술 제공 • 각종 무선 태그 및 센서간 통합 보안 관리 기술 제공
네트워크, 미들웨어 등 요소 기술간 컨버전스 지원
• 컨버전스 환경으로 발전함에 따른 홈네트워크 환경에서의 개인 프라이버시 침해에 대한 대응책 마련 • 네트워크 및 미들웨어의 통합 관리 정책 및 표준 마련 • 기술의 Layer별 보안 방식을 통합적으로 관리하는 표준 convergence 방식 제안 • 디바이스 보안 프로파일링 및 관리에 대한 표준화 방안 마련 • 강력한 암호화 메커니즘을 제공함으로써 개인의 프라이버시 및 보다 안전한 홈네트워크 서비스 제공을 위한 보안 강화

홈 네트워크 기술은 많은 기술적 요소의 집합체로 시장선점을 위한 뜨거운 경쟁이 이미 시작되었다. 각 업체와 단체들은 보다 유리한 위치를 선점하기 위해 표준화에까지 신경전을 펼치고 있는 실정이다. 그러나 이러한 상황 속에서 각 기술에 대한 보안기술은 상대적으로 많은 관심을 받지 못하고 있다. 그러나 홈 네트워크를 사용하는 사용자에 대한 개인 프라이버시와 보안 서비스 제공이야 말로 궁극적인 홈 네트워크 기술의 완성이라고 할 수 있기 때문에 보안 취약성과 보다 안전한 보안기술에 대한 연구는 계속될 것으로 전망된다.

III. 결론

홈네트워크를 구축할 때 가장 먼저 해야 할 일은 각각의 가정에 제공할 서비스 레벨을 먼저 정의하는 것이다. 예를 들어 가전 기기의 제어만을 지원하는 단순한 홈 오토메이션 수준의 홈 네트워킹을 구현할 것인지, 혹은 댁내에 오디어·비디오 신호의 실시간 전송을 위한 광대역 네트워크를 지원할 것인지에 대해 먼저 결정을 해야 하는 것이다. 그래야만 이러한 서비스를 제공해 줄 수 있는 홈 네트워킹 아키텍처를 결정할 수 있기 때문이다. 여기에 특히 고려해야 할 핵심기술로 홈네트워크를 위한 정보보호 기술의 접목을 들 수 있다. 임의의 사용자의 집 안에 있는 가전 기기들을 디지털화하고 이들을 홈네트워크로 연결하려면 네트워크의 전문 지식이 없는 일반 사용자들을 고려한 Plug & Play 기능은 필수적이지만, 만일 그 사용자의 집을 방문한 외부인들 조차도 아무런 인증절차없이 모든 정보를 노출시킬 수는 없다. 따라서 본 논문에서는 이러한 홈네트워크 환경에서의 보안 취약점에 대해서 분석하였으며, 이를 바탕으로 보안 요구사항을 도출하여 홈네트워크 환경에서의 보안 취약점에 대한 대응방안을 제시하였다.

기간 망을 위한 훌륭한 네트워크 인프라로부터 가입자 망에서부터 홈네트워크에 이르기까지 초고속 인터넷 서비스 환경을 위한 요구가 변하고 있으며, 이에 따라 정보통신부에서도 IT839 정책에서 홈네트워크 산업을 신성장 동력 산업 중의 하나로 선정하였으며, 관련 산업의 집중 육성에 대한 기대가 커지고 있다. 홈네트워크는 네트워크, 정보가전, 컴퓨터업계 등에 기술적 및 경제적 등의 엄청난 성장의 기회를 제공할 뿐만 아니라 관련 부품업체까지 연관되어 있기 때문에 큰 폭의 새로운 시장창출이 가능할 것으로 기대된다.

따라서 본 논문은 거대한 시장이 창출될 것으로 예상되는 홈네트워크 분야에 대한 보안 취약점을 분석하여 보안 요구사항을 도출하고, 이에 대한 대응방안을 제시했다는 측면에서, 개발 초기단계에 있는 홈네트워크 분야에서의 국제적인 경쟁력을 갖출 수 있는 매우 중요한 연구가 될 것으로 기대된다.

[참고문헌]

[1] 이전우, 배창석, "디지털 홈 기술동향", 한국전자통신연구원, 2003.8.

[2] 전호인, "홈네트워킹 기술(I)", ITFIND 주간 기술동향 통권 1191호, 2005. 4.

[3] 박준희, 손영성, "홈네트워크 미들웨어 기술 및 표준화 동향", 전자통신동향분석 제19권 제 5호, 2004. 10.

[4] 이성몽, "유비쿼터스 컴퓨팅 환경에서 개인정보보호 방법", IITA 기술정책정보단, 2005. 5.

[5] 남택용, 장종수, "유비쿼터스 환경에서의 개인정보 보호 기술", 한국전자통신연구원, 2005. 2.

[6] Steven G. Ungar, "Home Network Security", Telcordia Technologies, Inc.

[7] "Information Security Guidelines for NSW Government Agencies - Information Security Risk Management", 2001. 1.