한국컴퓨터정보학회 동계학술대회 논문집 제23권 제1호 (2015. 1)

홈 네트워크를 위한 보안취약점 분석 및 고찰

박성준°, 윤희용*
°*성균관대학교 정보통신대학
e-mail: skoop89@gmail.com°, youn7147@skku.edu*

Security Vulnerability Analysis and Discussion for Home Network

SenogJoon Park°, Hee Yong Youn*
°*College of Information and Communication Engineering, Sungkyunkwan University

● 요 약 ●

홈 네트워크는 가정 내에서 여러 기기들을 유·무선으로 연결 후 네트워크를 구성하여 서로 데이터를 공유한다. 가정 내 기기들은 컴퓨팅 기능이 저하되기 때문에 보안취약점을 이용한 사이버 범죄에 노출되어 있다. 따라서 사이버 범죄 및 개인정보의 유출을 방지하기 위해 유·무선 보안취약점 및 대응방안을 파악할 필요가 있다. 본 논문은 홈 네트워크의 보안 개선을 위해 미들웨어의 보안기능 및 홈 네트워크의 보안취약요인을 분석하고, 보안취약점 개선 방안을 제안한다.

키워드: 홈 네트워크(Home Network), 보안취약점(Security Vulnerability), 보안 기능(Security Function), 미들웨어(Middleware)

I. 서 론

정보통신 기술의 발전으로 인간은 더욱 다양하고 편리한 서비스에 대한 관심이 높아지고 있다. 홈 네트워크는 가정에서 여러 기기들을 유·무선으로 연결 후 데이터 및 프린터, 인터넷 등을 공유할 수 있도록 가정 내 네트워크를 구성한다.

홈 네트워크에 적용되는 기술들은 Home RF, HomePNA, IEEE1394, HomeBluetooth, Ethernet 등이 있다. 그러나 가정 내 홈 네트워크 기기들은 컴퓨터 기능이 저하되기 때문에 강력한 보안 적용이 힘들어 보안취약점을 이용한 정보 유출, 변조 등의 사이버 범죄에 노출되어 있다.

사이버 범죄 및 개인정보유출을 방지하기 위해 유·무선 보안취약점과 대응방안에 대해 파악할 필요가 있다. 이에 홈 네트워크의 보안 개선을 위해 미들웨어의 보안기능 및 홈 네트워크의 보안취약요인을 분석하고, 보안취약점 개선방안을 제안한다.

본 논문은 2장에서 홈 네트워크의 미들웨어의 보안기능과 보안취약점을 파악하고, 3장에서 홈 네트워크의 보안을 위해 고려할 점과 개선 방법을 제안한다. 4장에서는 결론을 맺는다.

II. 본 론

1. 홈 네트워크 미들웨어의 특징

본 장에서는 미들웨어의 특징에 대해서 분석한다. 홈 네트워크의 정보가전기기간의 제어를 위해 필요한 미들웨어들은 기본적인 보안 기능이 제공되고 있으며, 관련 보안 기능에 대한 표준화 또한 이루어지고 있다. 미들웨어는 홈 서버에 탑재되어 홈 네트워크를 구성하는 소프트웨어로 홈 네트워크에 연결된 모든 기기들이 서로 제어 정보 및 각종 멀티미디어 정보를 교환할 수 있도록 중간 매개체 역할을 해준다. 홈 네트워크의 미들웨어별 보안 기능은 아래의 표 1과 같다.

표 1. 주요 홈 네트워크 미들웨어별 보안기능
Table 1. The Main Home Network Middleware Security Function

미들웨어	제공 보안 기능 현황
UPnP	-Ver 1.0에서는 보안 기능이 정의되어 있지 않음 -Ver 2.0에서 보안 기능이 추가될 예정 -제품 인증 기능 제공 -기기간 인증 기능 제공 -접근제어를 위한 Device가 자체적인 ACL 제공 -기밀성 제공
Jini	-Ver 1.0의 보안기능은 Java Security에 의존 -사용자 인증 기능 제공 -기기 간 인증 기능 제공 -메시지 무결성 및 기밀성 제공 -접근제어 기능 제공 -Ver 2.0에서 추가적으로 상호인증, 인가기능, 코드 무결성등에 대한 기능이 강화됨
Havi	-Havi 인증서를 이용한 인증기능 제공 -접근제어 기능 제공
LoneWorks	-기기 간 인증 기능 제공
HNCP	-보안기능 정의 안 되어 있음(Ver 1.0)

미들웨어는 일반적으로 OS(Operating System) 환경과 응용프로그램 사이에 위치하지만, 유비쿼터스 환경에서 요구사항을 만족시키기 위해 일반적인 미들웨어가 수행하는 주요한 기능은 표 2와 같다.

표 2. 미들웨어의 주요 수행 기능
Table 2. The main roles of the middleware functionality

기능	특징
Addressing	홈 네트워크에 연결된 각종 기기에 고유한 번호를 부여하여 식별
Discovery	홈 네트워크에 새로운 기기가 연결되거나 제거되었을 때 자동으로 인식
Event	기기의 상태나 정보가 변경되었을 때 변화를 인식
Control Device	해당 기기를 제어하고 관련 UI 제공
Resource Management	홈 네트워크에 연결된 기기의 부하 조절 및 자원 관리
Security	가정 내의 네트워크가 외부의 공격에 대해 안전하도록 관리

2. 홈 네트워크의 보안 취약점

홈 네트워크에는 다양한 보안기술이 사용가능하나 컴퓨팅 성능의 문제로 인해 보안취약점을 해결할 수 있는 강력한 보안 기능을 가지고 있지 못하다. 유·무선 홈 네트워크의 보안취약점은 아래의 표 3, 4와 같다[1].

표 3. 유선 홈 네트워크 기술의 보안취약점
Table 3. Wired home security Vulnerability in Network technology

기술	보안취약점
IEEE 1394	-데이터 송수신으로 인한 유출 및 변조
PLC	-제어정보/데이터 전송 시 유출 및 위변조
HomePNA	-SNMP 기능 내장 -인증과 프라이버시 서비스들을 제공 -서비스 거부와 트래픽 분석의 보안 취약성 존재
USB	-오류발생시 재전송 불가 -키보드나 마우스 등 저속 전송 모드에 적용 -대역 보증이 없어 제어정보/데이터 전송 시 유출 및 위변조에 취약성 존재

표 4. 무선 홈 네트워크 기술의 보안취약점
Table 4. Security vulnerabilities in wireless home networking technology

기술	보안취약점
WLAN	-실시간 공격과 도청으로 인한 평문의 노출 -DoS 공격의 위험 존재
초광대역 통신	-무선기반 시스템의 개방성 때문에 정보의 유출 위험 존재 -WEP 암호화 기술을 보안하기 위한 연구 필요
무선랜	-높은 전송속도 지원이 필요할 뿐만 아니라 seamless connection 지원을 위한 안정적인 제어와 통신이 가능한 MAC 개발이 필요
무선1394	-잠재적으로 유해한 클라이언트가 이용자로 가장하여 정보의 유출을 유도할 수 있는 위험 존재
Zigbee	-블루스키핑, 블루버깅, 블루재킹

3. 홈 네트워크 보안 요구사항

보안취약점을 해결하려면 홈 네트워크의 종류에 따라서 보안 요구사항을 충족해야 한다. 본 절에서는 무결성, 기밀성, 가용성에 대해 다룸으로서 보안을 충족시킬 수 있는 최소한의 요구사항에 대해 제시한다.

3.1 무결성

무결성은 변조로부터의 보호방법이며, 정보의 저장과 전달시 비인가 된 방식으로 정보가 변경, 파괴되지 않도록 정확성과 안전성을 보호한다. 즉, 메시지가 통신 중간에 변질이 되지 않도록 한다. 이는 시스템의 하드웨어 및 소프트웨어의 안전성을 유지하기 위한 작용으로 데이터의 저장이나 전송 시 암호화, 전송기술, 바이러스 백신 설치, 보안정책, 논리적/물리적 접근 통제에 의해서 해결한다. 인증 및 키 교환 과정을 알고 있을시, 메시지 인증 코드와 같은 메커니즘을 사용하여 메시지의 변조를 막는다. 홈 네트워크 환경에서도 이러한 방법들과 같이 각 가구별로 암호화/복호화 알고리즘, 전자서명, 키 교환 및 키 분배 메커니즘을 이용한 인증방법과 홈 네트워크 환경에 적합한 접근통제 기술을 사용하여 무결성을 보장한다.

3.2 기밀성

기밀성은 공개로부터의 보호방법이며, 허가되지 않은 개인, 단체로부터 중요한 정보를 보호하며, 정보 소유자의 인가를 받은 사람만이 정보 접근이 가능하다. 주고받는 메시지에 대한 내용을 비밀로 하는 것으로, 거래 당사자 외의 다른 사람이 비밀메시지를 알아볼 수 없도록 하는 것, 즉, 도청을 방지한다. 또한 데이터 보안 분류체계에 의해 통제가 가능하다. 홈 네트워크 환경에서 홈 구성원이 아닌 다른 사람들로부터 댁내의 중요한 정보를 보호하고, 전송하는 메시지를 중간에서 누군가 침입하여 훔쳐볼 수 없도록 할 때 기밀성이 유지된다. 따라서 인증이 허가된 한 가구의 홈 네트워크 구성원들에게만 권한을 부여함으로써 외부사용자들로부터 중요한 정보들을 보호한다.

3.3 가용성

가용성은 파괴, 지체로부터의 보호이며 인가된 사용자가 정보나 서비스를 요구할 때 언제든지 사용한다. 즉, 많은 데이터 유입에 대하여 어떤 방법으로 시스템의 서비스를 제공할 것인지에 대해 홈 네트워크 서비스 요청 시 언제든지 사용하는 것이다. 홈 네트워크 환경에서 유선을 사용한 서비스 요청은 언제든지 처리가 가능하도록 할 수 있지만 무선에서는 필요시에만 접속이 되고 불 필요시에는 휴먼 상태에 접어들게 하는 방법을 사용한다.

이외에도 홈 네트워크의 보안 필요사항은 다음 표 5와 같다.

표 5. 홈 네트워크 보안 요구사항
Table 5. Home Network Security Requirements

구분	보안 요구사항
프라이버시	-개인 정보 유출 방지 -불법 위치 추적 방지
유·무선 네트워크	-상호 인증 -분산형 인증 시스템 -효율적인 키관리 -강력한 암호 알고리즘 -접근 제어 및 정책 -전파 방해 문제
서비스	-보안에 대한 QoS 보장
인프라	-센서신호의 Jamming 방지 기술 -과다 트래픽 탐지 기술 -도청 방지 기술 -이동 IPv6 인증/인가/접근제어 기술
미들웨어	-지능적 상황인지 기반 초경량의 통합 인증 서비스 구축
디바이스	-디바이스 인증 -디바이스 분실 방지 -단말 해킹 방지
통합관리	-통합 인증 기술

4. 홈 네트워크 보안 요구사항 대응 방안

본 절에서는 앞 절에서 보안취약점 해결을 위해 분석한 보안 요구사항에 대한 대응 방안을 제시한다.

4.1 암호화

데이터의 암호화는 가장 광범위하게 적용되어야 하는 기능이다. 기본적으로 사용자의 사생활 보호라는 측면에서 본다면 거의 모든 데이터는 암호화되어 처리되어야 한다. 홈 네트워크는 특성상 많은 가구가 하나의 네트워크에서 분기하여 서비스를 받는다. 홈 네트워크의 경우 다른 가구로부터 반드시 보호받아야 하므로 아파트 단지와 같은 경우 단지 내의 트랜잭션에 대한 암호화가 반드시 제공되어야 한다.

4.2 식별 및 인증

식별 및 인증을 위해서는 기본적인 ID/비밀번호 방식과 함께 공인인증서, 생체 인증 등이 사용될 수 있다. ID/비밀번호 방식의 경우 구현상 가장 간단하지만 사용자가 ID와 비밀번호를 입력하여야 하므로 불편하며 보안성이 낮다는 것이 단점이다.

공인인증서의 경우 인증서 이동성 기능 제공 및 각 플랫폼상에서 구현 등이 어려우나 비밀번호만을 입력하며 전자서명, T-Commerce, T-Banking에의 활용과 높은 보안성 제공이 장점이다.

생체인증의 경우 사용자의 입력이 필요 없으므로 편리하지만 지문인식기 등의 장치를 요구하는 점이 단점이다. ID/비밀번호 방식과 지문 인증 방식에서는 사용자 인증 정보의 등록과 저장이 안전하게 구현되어야 한다.

4.3 전자서명

전자서명은 사용자 인증, 부인 방지 및 코드 서명에도 사용된다. 전자서명을 사용하는 것은 성능 및 자원의 소요가 필요하므로 업무에 따라 적절히 적용하되, 만일의 경우를 대비할 수 있도록 업무의 성격을 충분히 분석하여 설계할 필요가 있다.

코드 서명은 기기의 모듈을 갱신하거나 추가 할 때 등록된 인증서로 검증 성공한 모듈만을 설치하도록 하여 불법적인 접근을 막는다.

인증서는 공인인증서와 사설 인증서를 사용할 수 있으며 용도에 따라 선택하여 사용한다.

4.4 플랫폼

홈 네트워크는 기존 서비스와는 달리 매우 다양한 기기를 함께 사용하는 서비스로서 사용되는 플랫폼도 다양하다. 홈 게이트웨이, 셋톱박스(Set Top Box) 등의 장비는 임베디드 리눅스 또는 윈도우 CE 등을 주 OS로 사용하고 있으며 향후 다양한 임베디드 OS가 사용될 수 있다. 방송용 셋톱박스의 경우에는 ACAP/OCAP 이라는 브라우저에 대응 되는 플랫폼을 사용한다. 또한 외부에서 사용자가 휴대폰을 통한 접속으로 사용할 수 있으며 내부에서 PC를 사용한 제어를 할 수 있다. 이 외에 홈 네트워크의 보안 요구사항에 따른 보안 대응 방안은 다음 표 6과 같다[2].

표 6. 홈 네트워크 보안 요구사항에 따른 대응 방안
Table 6. Countermeasures according to the home network security requirements

구분	보안 요구사항 대응 방안
프라이버시	-프라이버시 정보 프로파일 구체화 -권한, 역할에 따른 개인정보조회를 위한 context modeling과 ontology화 -Privilege or Role Delegation Service -위치 보호 및 인증 기술
유·무선 네트워크	-타원곡선 알고리즘 -AP인증 기술 -802.11i 키관리 기술 -Rogue Bridge 관리 -유·무선 연동 보안 기술
서비스	-보안에 대한 QoS 제어 기술 -프로파일 기반의 보안 정책 -유해정보 판단 및 분류 기술
인프라	-USN 보안 취약성에 대한 대책 -IPv6 지원 기술 마련 -BcN망에서의 보안 관리 기술
미들웨어	-상호 단일 인증 지원 미들웨어 기술 -자가 치료 및 자가 방어 기능을 탑재한 고도화된 보안 미들웨어 기술
디바이스	-통합 디바이스 관리 미들웨어 보안 기술 -불법 디바이스에 대한 고성능 자동 선별, 차단 기술
통합관리	-통합 관리 미들웨어 보안 기술

Ⅳ. 결 과

본 연구에서는 홈 네트워크에서의 보안취약점과 문제점 개선을 보안 요구사항을 분석하고 그에 대한 대응 방안을 제시하였다. 아직까지 미들웨어별로 보안취약점이 상당함에도 통합 홈 네트워크를 구성하여 대응 방안을 논의하고 있지 않다. 공통되게 만족하는 보안 기준을 마련하여 보안취약점을 해결하고, 언제든지 발생 가능한 사이버 범죄

및 개인정보 유출에 대응해야 한다.

ACKNOWLEDGMENT

본 연구는 BK21+사업, 한국연구재단 기초연구사업 (2012R1A1A2040257), (2013R1A1A2060398), 삼성전자(S-2014-0700-000), 미래창조과학부 및 정보통신기술연구진흥센터의 정보통신·방송 연구개발사업 (1391105003)의 일환으로 수행하였음.

참고문헌

[1] Hoon Ko , “Home Network Vulnerability Assessment and Certification Analysis”, Korea Institute of Information Security and Cryptology, Vol. 16 No.6, pp. 42-47, 2006.

[2] Jae-Hak Jung,“Security Requirements Analysis in a Home Network”, Electronics and Telecommunications Trends, Vol. 14 No.5 pp. 19-22, 2004