디지털홈 환경에서의 보안 프레임워크 연구

김도우* · 한종욱*· 주홍일*· 이윤경*
*한국전자통신연구원

A Study on Security Framework in Digital Home Environments

Do-Woo Kim* · Jong-Wook Han*· Hong-Il Ju*· Yun-Kyung Lee*
*Electronics and Telecommunications Research Institute
E-mail : dwkim@etri.re.kr

요 약

네트워크 기술의 발전과 가전기기의 디지털화로 인하여 컴퓨터를 포함하는 댁내의 정보기기들은 물론 오디오/비디오, 냉장고, DTV 등을 하나의 네트워크로 연결함으로써 사용자가 집안 어디에 있든 모든 정보가전기기들을 제어할 수 있다. 이러한 홈네트워크 환경은 원격제어 및 홈 서비스 제공을 위하여 전화선을 포함한 다양한 유무선 네트워크에 연결될 수 있다. 이로 인하여 외부 네트워크에 연결된 정보가전기기들은 공격에 의한 보안 취약성을 가진다. 따라서 디지털홈 환경에서의 보안 프레임워크 구축을 위한 취약성 분석 및 보안 요구사항 연구가 필요하다.

ABSTRACT

With the development of modern communicatien and networking technology, more and more computing and communication facilities, automation equipments, home information appliances and different type of networking terminals come into home all over the world. The user can control information appliances in home environments. The home environment can communicate with the external network via phone line, wired LAN, wireless LAN, or mixed. However, home information appliances that are connected to the external network are under attack and need to be secured. So specifying suitable security requirements and policies for digital home environment is critical in home networking environments. This paper analyzes the possible vulnerability to home network, and specifies the security requirements derived from the vulnerability analysis for digital home environment

키워드
Home network, vulnerability, security, authentication

Ⅰ. 서 론

네트워크 기술의 발전과 가전기기의 디지털화로 인하여, 기업이나 공공기관의 사무실 중심으로 구축되던 네트워크 환경이 컴퓨터를 포함하는 댁내의 정보기기들은 물론 오디오/비디오, 냉장고, DTV 등을 하나의 네트워크로 연결함으로써 사용자가 집안 어디에 있든지 모든 정보가전기기들을 제어할 수 있는 환경으로 변화되고 있다. 댁내의 정보가전기기들은 HPNA, xDSL, PLC, Cable-Modem, IEEE 802.17 등과 같은 다양한 기술을 통하여 액세스망(Access Network)과 통신할 수 있다. 또한 HomePNA, PLC, WLAN, IEEE1394 등과 같은 다양한 댁내 유무선 네트워크 기술을 통하여 정보가전기기들 사이의 자원의 공유 및 서비스를 사용할 수 있다.

기업과 공공기관의 네트워크 환경은 침입차단시스템에서 암호기술에 이르기까지 다양한 정보보호 기술의 적용을 통해 안전하고 신뢰성 있는 서비스를 제공하고 있다. 이러한 네트워크 환경은 전문적인 보안 기술을 가진 관리자에 의해 관리되어진다. 이에 비해 홈네트워크 환경은 다양한 유무선 네트워크 기술의 사용, 미들웨어와 프로토콜의 혼재, 댁내 정보가전기기의 제한적인 시스템 자원, 댁내 사용자의 보안 인식 부족 등으로 인하여 기업과 공공기관의 네트워크 환경과 같은 정보보호기술을 그대로 적용하기가 쉽지 않다[1,3].

따라서 홈네트워크 환경에서 안전하고 신뢰성

있는 서비스를 제공하기 위해 보안 요구사항과 정책(policy)의 수립은 상당히 중요한 요소이다. 본 논문에서는 디지털홈 환경에서 발생할 수 있는 보안 취약성을 분석하고, 이를 바탕으로 보안 프레임워크 구축을 위해 필요한 요구사항 및 정책을 제시하고자 한다.

II. 디지털홈 환경에서 요구되는 보안 서비스

홈네트워크에서 요구되는 보안 서비스는 홈의 정의에 따라 달라질 수 있다. 그리고 댁내에 어떠한 홈네트워크 기술들이 포함될 것인가에 따라 달라진다. 댁내의 네트워크가 외부 액세스망과 연결되어 있지 않다고 가정하면, 안전한 홈네트워크 환경을 제공하는 것은 쉽다. 그러나 댁내의 망이 인터넷과 같은 외부의 액세스망과 연결되어 있다면, 안전한 네트워크 서비스를 제공하기 위해 고려해야 할 요소들은 많아진다. 또한 댁내에 한 명만이 거주하고 있다면, 안전한 홈네트워크 구축이 쉬울 수 있다. 하지만, 댁내에 여러 명의 구성원이 거주하면 한 명이 거주하는 형태와 비교해볼 때 훨씬 복잡한 보안 정책이 필요하다[2].

홈네트워크 환경에서 요구되는 정보보호 서비스는 기업과 공공기관의 네트워크 환경과 마찬가지로 다음과 같은 기능을 보장해야 한다[1,2].

- *인증(Authentication)* : 누구에게 디바이스와 홈서비스를 사용하도록 허락할 것인가?
- *기밀성(Confidentiality)* : 디바이스로 전달된 메시지를 누구에게 읽도록 허락할 것인가?
- *무결성(Integrity)* : 사용자와 디바이스나 홈서비스 사이에 전송되는 정보는 권한을 가진 사용자만이 정보를 수정할 수 있어야 한다.
- *가용성(Availability)* : 사용자가 필요할 때 디바이스나 홈서비스를 사용할 수 있도록 보장해야 한다.
- *인가(Authorization)* : 각 디바이스에서 제공하는 서비스나 정보에 대해 가족 구성원 각각에 대해 어느 정도의 접근권한을 주어야 하는가?

III. 홈네트워크 환경에서의 보안 취약성 분석

홈네트워크 환경에서의 보안 위협(threat)은 부정확한(incorrect) 홈네트워크 구축, 홈네트워크 구성요소들의 변화 혹은 악성코드와 같은 외부 공격을 포함한 다양한 요소들로부터 발생할 수 있다. 이러한 위협은 댁내 보안 취약성(Vulnerability)과 댁외 보안 취약성으로 분류할 수 있다[1]. 그림 1은 디지털홈 환경에서의 보안 취약성을 보여주고 있다.

댁내 보안 취약성은 불법적인 접근, 인증되지 않은 디바이스의 접속, 메시지의 유출 등으로 분류할 수 있다.

불법적인 접근(Unauthorized access) : 침입자(intruder)는 합법적인 홈 사용자를 가장(masquerade)하여 댁내 디바이스나 서비스를 사용하거나 정보를 얻기 위해 접근할 수 있다.

인증되지 않은 디바이스의 접근(Uncertified device access) : 인증되지 않은 디바이스를 홈네트워크 환경에 연결함으로써 홈네트워크 환경의 보안 정책을 변화시킬 수 있다. 또한 합법적인 시스템으로 가장하여 홈네트워크 환경에 연결함으로써 홈서비스를 이용하거나 중요한 정보를 얻을 수 있다.

메시지 유출(Release of message contents) : 해커가 홈네트워크 환경에서 무선을 통한 전송이 이루어지는 경우, 전송되는 내부 트래픽을 가로채 분석을 할 수도 있다.

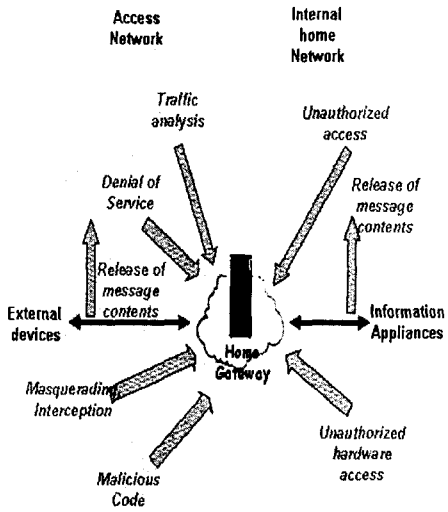

그림 1. 디지털홈 환경에서의 보안 취약성

댁외 보안 취약성은 악성코드, 가장(masquerading), 가로채기(interception), 메시지 유출, DoS, 트래픽 분석 등으로 분류할 수 있다.

트래픽 분석(traffic analysis) : 해커는 댁내와 댁외 사이에 전송되는 트랜잭션으로부터 중요한 정보를 가로채거나 시간, 양, 방향, 빈도 등 트래픽 흐름을 분석하여 홈 사용자나 외부 노드의 위치 등을 추측할 수 있다.

가장(Masquerading) : 해커가 합법적인 홈 사용자를 가장하여 홈네트워크 환경에 원격 접속하여

디바이스나 홈서비스를 사용하거나 중요한 정보를 얻을 수 있다.

DoS(Denial of Service) : 침입자는 서비스의 가용성을 줄이거나 서비스 거부를 초래할 수 있는 다양한 방법으로 홈서비스나 트래픽을 방해할 수 있다. 침입자는 홈게이트웨이나 홈서버로 엄청난 양의 패킷을 보내어 공격할 수 있다. 이로 인해 시스템 자원이 고갈되고, 권한을 가진 사용자가 홈네트워크 서비스를 사용할 수 없게 될 것이다.

정보 추론(Information inference) : 해커가 질의나 시그널을 홈네트워크 환경으로 보내거나 직접적으로 댁내의 정보가전기기로 보내어 홈네트워크으로부터 전송되는 응답을 관찰해서 해커가 필요로 하는 정보를 추론할 수 있다.

정보 누출(Information leakage) : 침입자는 원격으로 홈네트워크 환경에 합법적인 접근을 해서 홈네트워크 시스템에 저장된 중요한 정보들을 유출시킬 수 있다.

악성 코드(malicious code) : 홈네트워크 환경에서는 악성 코드로 인한 위협이 정보보호 요소 및 인식 부족 때문에 기업과 공공기관의 네트워크 환경과 비교해 훨씬 더 파급 효과가 크다. 현재 악성 코드는 소프트웨어 핏폴(pitfall), 전자우편, 웹 페이지 등을 통해서 전파된다. 악성 코드들은 홈네트워크 시스템 자원을 크게 소모하고, 홈네트워크 시스템을 심각하게 파손하고, 홈네트워크를 통해 급속도로 빠르게 전파될 수 있다.

IV. 홈네트워크 설계 시 필요한 보안 요구사항

홈네트워크 환경에서 보안 정책은 댁내의 디바이스와 홈서비스를 안전하게 사용하기 위한 규칙(rule)을 명시해야 한다. 이 규칙은 시스템 자원의 사용, 정보의 저장 및 수정, 사용자에 대한 권한과 책임, 인증과 접근권한 제어 등으로 구성되어야 한다.

이 절에서는 3절의 보안 취약성 분석을 통하여 안전한 홈네트워크 환경 설계 시 요구되어지는 정보보호 요소들을 기술할 것이다.

인증(authentication) : 홈네트워크 환경에 불법적인 접근을 시도하여 댁내의 디바이스와 홈서비스의 불법 사용은 댁내·외를 통하여 발생할 수 있다. 홈네트워크 환경에 접근을 시도하는 사용자나 디바이스를 식별하는 기능은 보안 단계의 가장 첫 번째이며 가장 중요한 단계이다. 또한 인증 기능을 수행하기 위해 네트워크를 통하여 전송되는 인증 데이터는 합법적인 사용자를 가장한 침입자에 의해 유출될 수 있기 때문에 암호에 기반 한 인증 기술을 사용함으로써 침입자로 하여금 네트워크를 통해 정보를 얻을 수 없도록 해야 한다.

인가(Authorization) : 댁내·외에서 디바이스나 홈서비스 사용은 단지 인증만으로 이루어질 수 없다. 홈네트워크 환경에서 접근권한 제어를 사용하여 가족 구성원에 대해 미리 설정된 규칙에 기반하여 사용자가 디바이스나 홈서비스에 접근이 이루어질 수 있도록 하여야 한다. 이를 위해 디바이스나 홈서비스는 가족 구성원 각각에 대해 혹은 방문객에 대해 디바이스나 홈서비스의 어떤 기능을 제공해야 되는지에 관한 접근권한 정보를 알고 있어야 한다.

암호화(Encryption) : 중요한 트래픽 데이터의 무결성과 기밀성을 보장하기 위하여 유무선 네트워크를 통해 전송되는 제어 메시지와 같은 중요한 데이터는 트래픽 분석이나 도·감청과 같은 위험성을 줄이기 위해 암호화되어져야 한다. 또한 패스워드, PIN과 같은 사용자 인증과 관련한 데이터도 디바이스나 홈서비스에 대한 불법적인 접근에 노출되는 위험성을 줄이기 위해 암호화되어져야 한다.

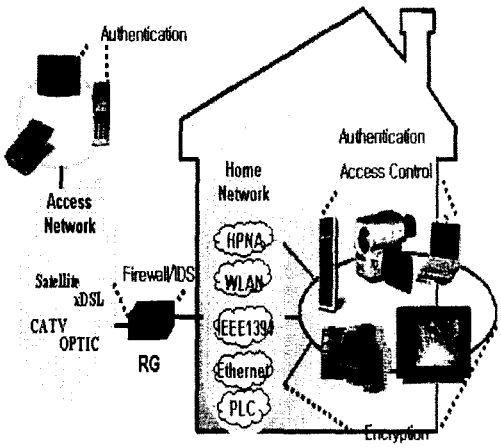

그림 2. 디지털홈 환경에서의 보안 요구사항

침입차단시스템(Firewall) : 침입자는 노출된 보안 취약성을 통해 지속적으로 홈네트워크 시스템을 스캐닝(scanning)한다. 침입차단시스템은 인터넷과 같은 외부 네트워크에 연결되어 있는 홈네트워크의 중요한 정보 및 자원을 외부 네트워크를 통한 불법적인 침입으로부터 안전하게 보호할 수 있다. 침입차단시스템은 외부에서 홈네트워크 내부로의 공격이나 침입을 시도한다 할지라도 댁내망에 접근하려면 침입차단시스템을 반드시 거쳐야 하기 때문에 이를 탐지하고 방어할 수 있는 기능을 제공함으로써 어느 정도의 외부 공격으로부터 댁내를 보호할 수 있다.

침입탐지시스템(Intrusion Detection System) : 방화벽의 경우 침입이 발생하지 않도록 홈네트워크의 출입구를 제어하는 기능을 수행하므로 인증을 받지 않은 외부의 접근 시도는 차단할 수 있지만 이미 인증된 사용자나 이를 가장한 침입자에 의한 공격에는 취약하다. 특히 댁내 사용자 혹은 허가된 외부 사용자에 의해 자주 발생하는 홈네트

워크 시스템 침입을 다룰 때에는 침입을 즉각적으로 탐지하고 대처하는 기술이 필요하다. 침입탐지 시스템은 침입을 탐지하여 이를 홈네트워크 관리 시스템에게 관련 정보를 전달하고 관리 시스템에서는 정해진 대응방침에 따라 연동되는 침입차단 시스템, 바이러스 백신 프로그램 및 자체 보안기능 등을 통해 다양한 방법을 수행할 수 있다.

V. 결 론

본 논문에서는 홈네트워크 환경에서 발생 가능한 보안 취약성을 분석하고, 이를 바탕으로 보안요구사항들을 제시하였다.

기업과 공공기관의 네트워크 환경과 비교해서 홈네트워크 환경은 네트워크를 구성하는 요소들과 사용자측면에서 상당히 많이 달랐다. 네트워크 구성요소 측면은 다양한 유무선 네트워크, 미들웨어와 프로토콜들이 존재하고, 사용자 측면은 댁내 사용자들의 보안 인식 수준 낮다는 것이다. 이러한 요소들은 홈네트워크 서비스 활성화의 저해 요인으로 작용할 수 있다.

따라서 홈네트워크 환경 설계 시, 적합한 정보보호 기술의 고려는 안전하고 신뢰성 있는 홈서비스 제공을 위해 반드시 필요하고, 중요한 요소이다.

참고문헌

[1] Guoyou He, "Requirements for Security in Home Environments", Residential and Virtual Home Environments Seminar on Internetworking, Spring 2002.

[2] Carl M. Ellison, "Home Network Security", Intel Technology Journal, 2002.

[3] Cert Coordination Center, Home Network Security, 2001.

[4] Gollmann Dieter, ComputerSecurity, John Wiley & Sons, England, 1999.

[5] Cooper Frederic J., Coggans Chris, etc., Implementing Internet Security, New Riders Publishing, 1995.

[6] Hayes Keith, Active Security Monitoring and Containment with Cross Technology Correlation: The Next Generation in Computer Security Technology, 2002.

[7] Matthew J. Brodeur, Security Concerns In Home Automation Technologies, 2001.

[8] Patria Leath, Addressing and Implementing Computer Security for a Small Branch Office, 2001