韓國 컴퓨터情報學會 論文誌
第12卷 第5號, 2007. 11.

2007-12-5-2-3

해커의 유비쿼터스 홈 네트워크 공격에 대한 정보보호 기술

천 재 홍*, 박 대 우**

Information Protection against The Hacker's Attack of Ubiquitous Home Networks

Jae Hong Cheon*, Dea-Woo Park**

요 약

본 논문에서는 유비쿼터스 홈 네트워크에서의 개인정보보호를 위해 유비쿼터스와 홈 네트워크의 보안을 위협하는 다양한 보안 위협사항과 요구사항에 대해 분석하고 연구하였다. 보안기능을 강화한 유비쿼터스 홈 보안 게이트웨이를 설계를 통해 외부에서의 정당한 사용자 접근 시, 인증절차와 검증절차를 마련함으로써 홈 네트워크의 보호를 강화하였다. 또한 DoS, DDoS, IP Spoofing 공격을 실시하여 홈 네트워크 보안 게이트웨이에서의 방어실험을 함으로써 해커의 공격에 대한 보안이 이루어졌음을 확인하였다. 공격 실험을 통해 유비쿼터스 홈 네트워크에서의 기기와 사용자에 대한 보안을 강화하고, 외부 공격에 대한 방어를 확인함으로써 본 논문의 홈 네트워크 보안 모델을 유비쿼터스 홈 네트워크에서의 개인정보보호를 강화할 수 있는 방안으로 제시한다.

Abstract

Analyzed about a matter and requirements to intimidate security of ubiquitous and home network threatening various security for personal information protection in ubiquitous home networks at this paper, and studied. Got authentication procedures and verification procedures acid user approach to be reasonable through designs to the home security gateway which strengthened a security function in the outsides, and strengthened protection of a home network. Also, execute a DoS, DDoS, IP Spoofing attack protective at home network security gateways proved, and security regarding against the Hacker's attack was performed, and confirmed. Strengthen appliances and security regarding a user, and confirm a defense regarding an external attack and present a home network security model of this paper to the plans that can strengthen personal information protection in ubiquitous home networks in ubiquitous home networks through experiment.

▸ Keyword : ubiquitous security, hacker attack, home network security, vulnerability

• 제1저자 : 천재홍, 교신저자 : 박대우(prof1@paran.com)
• 접수일 : 2007. 9.11, 심사일 : 2007. 10.10, 심사완료일 : 2007. 11.10.
* 한국환경정책평가연구원, ** 호서대학교 벤처전문대학원 교수

Ⅰ. 서 론

유비쿼터스 컴퓨팅(Ubiquitous Computing)은 1988년 미국 제록스사의 마크 와이저 박사가 제안한 개념이다. 이는 일상생활과 다양한 컴퓨팅 시스템의 유기적 네트워크 구성을 통해 제공할 수 있는 지능화된 환경을 구축하는 것으로 제한 없이 접속하고 쉽게 서비스를 제공받을 수 있도록 계속적으로 발전하고 있으며, 빠른 기술발전에 따라 급속히 일상생활에 이용되고 있다.

유비쿼터스 컴퓨팅은 메인프레임 시대, 퍼스널 컴퓨터에 이은 제3의 물결이라 정의할 수 있으며, 미국, 일본, 유럽의 선진국 정부뿐만 아니라 많은 기업 및 연구소 등에서는 지식정보국가 건설과 자국의 정보산업 경쟁력 강화 및 세계 정보화산업을 선도 할 수 있는 핵심과제로 인식하여 유비쿼터스 관련 기술개발에 많은 자본과 인력을 경쟁적으로 투입하고 있다[1].

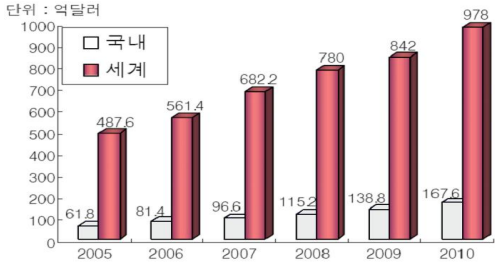

그림 1. 홈 네트워크 기기 국내·외 시장 예측
Fig. 1. Market research about a Home network Devices

그림 1에서 홈 네트워크의 국내·외 시장은 성장할 것이고 유비쿼터스 홈 네트워크로 발전되어 진화될 것이다.

본 논문에서는 유비쿼터스 홈 네트워크 환경에서 발생할 수 있는 보안 취약점과 보안 요구사항을 도출하여 제시하고, 사용자 인증 및 검증에 관한 인증기술을 연구하였다. 또한 유비쿼터스 홈 네트워크에 대한 외부에서의 접근제어와 DoS(Denial of Service), DDoS(Distributed Denial of Service), IP Spoofing공격[2]을 하여 방어기술을 실험하고, 실험결과로써 정보보호를 위한 사용자 인증과 검증 및 외부의 해커로부터의 공격을 방어하는 유비쿼터스 홈 보안 게이트웨이의 기술을 검증한다. 또한 유비쿼터스 홈 네트워크의 인증기술과 서비스 방향을 통한 유비쿼터스 보안 모델을 제안하고, 적용하여, 가정에서의 가정 댁내·외에서의 정보보호의 안정성을 확보할 수 있는 근거 자료를 마련한다.

Ⅱ. 관련 연구

2.1. 유비쿼터스 시스템

마크 와이저가 주장한 유비쿼터스 컴퓨팅은 기본적으로 네 가지 사상을 지닌 컴퓨팅 환경으로 정의할 수 있다.

첫째, 유비쿼터스 컴퓨팅은 인간친화적인 인터페이스로서 이용자가 지나치게 주의를 기울이지 않아야 한다.

둘째, 유비쿼터스 컴퓨팅은 물리공간의 모든 컴퓨터뿐만 아니라 컴퓨팅 기능이 내재된 모든 사물들을 서로 연결한다.

셋째, 사용자가 컴퓨터의 사용이나 네트워크의 존재에 주의를 기울이지 않는 평온하고 고요한(calm) 기술을 구현하여야 한다.

넷째, 유비쿼터스 컴퓨팅은 현실 세계를 네트워크로 연결하는 것이며, 실존하지 않는 가상현상은 유비쿼터스 컴퓨팅에 속하지 않는다.

2.2. 유비쿼터스 홈 네트워크

인터넷의 발달과 IT 서비스 중 하나가 홈 네트워크 서비스이다. 홈 네트워크 서비스는 그림 2와 같이 네 가지의 분야로 표현된다.

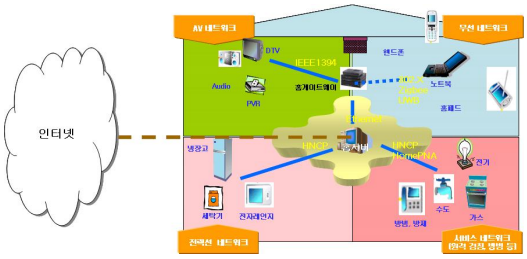

그림 2. 홈 네트워크 서비스 분야
Fig. 2. Service field in Home network

첫째, AV 네트워크는 집안의 가전제품 중 오디오, 비디오와 같은 종류의 기기들의 네트워크 구성을 위한 것으로 주로 IEEE1394 프로토콜을 이용하여 상용화되고 있다.

둘째, 전력선을 이용한 PLC 네트워크는 설치가 간단하고 간단한 제어 명령들을 전송할 수 있어 냉장고, 세탁기와 같은 명령체계를 가지는 장비들을 제어하는데 상용화되고 있다.

셋째, 서비스 네트워크로서 원격 검침 및 방범과 같이 외부에서 내부의 사용을 점검하는데 주로 구성된다.

넷째, 무선 네트워크는 설치가 어려운 홈 네트워크 장비 및 가전을 쉽게 연동할 수 있는 기술로서 향후 홈 네트워크를 연결하는 가장 중추적인 역할을 수행할 것이다.

현재 홈 네트워크의 가장 큰 현안은 인터넷 및 디지털 기기 간 통신에서 발생할 수 있는 보안문제와 개인정보보호 문제이다.

2.3. 홈 네트워크 RFID

홈 네트워크에 연결된 제품에 붙이는 태그(tag)에 생산, 유통, 보관, 소비 등 전 과정의 정보와 연동되는 식별자인 ID를 저장하고 자체 안테나를 갖추고 있으며, 리더기(Reader)를 이용하여 정보를 읽고, 인터넷과 이동통신망이나 인공위성 등의 다양한 네트워크 통신망을 통해 유비쿼터스 센서 네트워크[3]에 사용되는 RFID 시스템을 말한다.

RFID 시스템은 크게 태그와 리더기 및 RFID 미들웨어 서버 또는 네트워크로 구성되며[4] RFID의 주요 시스템은 다음과 같다.

- 태그 : 용도에 맞게 만들어진 리더와 통신을 제어하는 IC 칩이 있으며 칩 내의 기억장치에 관련 정보에 대한 데이터를 저장한다.
- 리더기 : 태그로부터 송·수신되는 신호를 처리하여 메모리에 저장하거나 향후 송신 할 수 있도록 마이크로프로세서를 내장한다.
- 미들웨어 : 리더기로부터 받은 정보를 처리하고 데이터를 필터링하여 Back End Server로 데이터를 전송한다.
- 서버/네트워크 : 기존 ERP(Enterprise Resource Planning), SCM(Supply Chain Management)시스템과의 연계를 통한 서비스 제공을 한다.

2.4. 무선 센서 네트워크 보안기술

2.4.1. 무선 센서 네트워크 보안기술 개요

무선 센서 네트워크는 일반 PC 컴퓨팅 환경과 비교해서 제한된 처리장치, 저장 공간, 대역폭, 전원 등의 제약 사항을 갖지만[5] 보안 요구사항은 일반적인 인터넷 환경에서 요구되는 수준을 만족시킬 수 있는 보안 기술이 이루어져야 한다. 센서 네트워크를 위한 센서 디바이스의 프로토타입은 CITRIS의 구성요소인 Smart Dust Program[6]에 의해 정의되어진다.

2.4.2. 무선 센서 네트워크 보안 요구사항

- 기밀성 (Confidentiality) : 센서 네트워크 환경에서는 노드 간 민감한 데이터의 교류가 빈번하게 발생하게 된다. 따라서 권한이 있는 노드 외에는 민감한 정보를 볼 수 없도록 하기위해 데이터를 암호화하여 데이터의 기밀성을 보장할 수 있다.
- 인증 (Authentication) : 무선 센서 네트워크 환경에서 비대면 접속이기 때문에 공격자는 쉽게 메시지를 삽입할 수 있어, 수신자는 수신된 데이터가 원래 작성자로부터 온 것인지를 확인해야만 한다.
- 무결성 (Integrity) : 수신자가 수신한 데이터가 송신자로부터 전달 시 위·변조 여부를 확인하여 SPINS (Security Protocols for Sensor Networks)[7]에서는 데이터 인증을 통해 데이터 무결성을 보장한다.
- 적시성(Freshness) : 예전에 보낸 데이터를 해커가 불법적으로 재사용하는 것을 방지하고, 가장 최근에 보낸 데이터임을 보장하는 보안 서비스이다.

2.4.3. 센서 네트워크의 인증 및 검증

SNEP 프로토콜은 자료의 비밀성, 쌍방간 데이터 인증, 완전성, 적시성과 재전송 보호와 시멘틱 보안에 관한 안전함을 제공한다. 자료의 인증과 무결성은 MAC(Message Authentication Code)이 사용된다[8]. 센서는 멀티 홉(multi-hop) 라우팅[9] 토폴로지와 함께 자기 자신을 조직하는 무선 네트워크를 구성한다. 표준 네트워크는 한 쌍의 노드와 더욱 강력한 기본 스테이션을 포함한다. SPINS에서 제시하는 프로토타입은 소규모의 전력으로 구동되어지는 노드와 보다 강력한 자원을 갖는 Base Station으로 구성된다[10]. 기본 스테이션은 외부 네트워크에 연결된다. 센서의 작은 전지는 노드(node)가 동작하는데 필요하고, 노드가 스스로 작동을 할 수 있도록 하기위해 에너지를 소비하게 되므로, 센서 네트워크에서는 보안에서 사용하는 통신의 오버헤드(Overhead)가 에너지 소비를 최소한으로 하는 시스템을 적용한다.

센서의 노드는 기본 스테이션을 향해 메시지를 보내게 되고, 기본 스테이션으로부터 자신으로까지의 경로인 주소 패킷을 인식하여 인증 및 검증의 절차를 거친다. 인증과 검증 후에 모든 노드는 초기의 기본 스테이션을 신뢰하고 각각의 노드는 노드 자신을 신뢰한다[11].

2.5. 유비쿼터스 네트워크의 공격

유비쿼터스 네트워크의 공격유형에는 기존의 인터넷에서

의 TCP/IP의 버그와 취약점을 이용하는 DoS, DDoS, IP Spoofing, SYN Flood 같은 공격이 있다.

2.5.1. DoS, DDoS 공격

DoS 공격은 멀티태스킹을 지원하는 운영체제에서 발생할 수 있는 공격 방법으로서 사용자가 시스템의 리소스를 독점(Hogging)하거나, 모두 사용함으로써 이 시스템이 다른 사용자들에게 올바른 서비스를 제공하지 못하게 만드는 것이고, DDoS(분산 서비스 거부) 공격은 DoS공격을 보다 효과적이며 강력하게 공격하기 위한 방법으로 여러 대의 장비를 하위의 더미로 이용하여 일시에 공격을 하는 것이다.

이와 유사한 공격으로 SYN공격은 대상 시스템에 연속적인 SYN 패킷을 보내서 넘치게 만들어 공격자는 큐를 꽉 차게 만들어, 들어오는 모든 SYN 요구를 무시하고 시스템이 인증된 사용자들의 서비스를 할 수 없게 만든다.

2.5.2. IP Spoofing 공격

호스트나 라우터로 하여금 해커의 패킷이 인증된 네트워크로부터 온 것인 것처럼 IP를 Spoofing을 통해, 라우터나 방화벽에서 정상 패킷이 인증된 네트워크로부터 전송된 것으로 의심 없이 통과 하도록 만든 다음 해커가 원하는 공격을 한다.

III. 유비쿼터스 홈 네트워크의 정보보호 위협 및 요구사항 설계

3.1. 유비쿼터스 보안 위협 및 요구사항

3.1.1. 유비쿼터스 보안 위협 사항

유비쿼터스 컴퓨팅 환경은 무선 인터넷, 무선랜, 블루투스, 홈 네트워크 등의 분야를 통합하는 환경이라 할 수 있다. 이러한 유비쿼터스 컴퓨팅의 특성은 데이터의 보안이 취약할 경우 보안 문제를 발생시킬 수 있다. 또한 수집된 데이터가 오·남용될 경우 오히려 사용자에 대한 감시 시스템으로 동작할 수도 있다.

유비쿼터스 네트워크 환경에서 발생할 수 있는 보안 위협 사항으로는 장치의 절도 및 분실, IP Spoofing, DoS, DDoS 공격, 트로이목마, 웜, 바이러스 등이 있다.

(1) 장치의 절도 및 분실

장치의 절도 및 분실은 유비쿼터스 장치가 분실되어 공격자가 접근해서는 안 되는 정보를 접근 및 수신할 수 있어 비밀성이 손상될 수 있고, 유비쿼터스 장치에 저장된 인증 정보들을 사용하여 네트워크에 대한 접근 권한을 얻을 수 있으며 이는 네트워크 침해로 이어질 수 있다.

(2) IP 스푸핑

무선 신호는 건물의 벽을 통과할 수 있기 때문에 건물 외부로 전달될 수 있고, 적어도 무선 신호 범위 내에 존재하는 어느 누구나 무선 접속이 가능하기 때문에 전송되는 정보가 암호화되어 있지 않을 경우 공격자가 중요 정보를 도청할 위험이 항상 존재한다.

(3) DoS, DDoS 공격

유비쿼터스 네트워크 환경은 수시로 망구조가 변경되기 때문에 임시로 구성된 노드들 간에 데이터 교환을 위해서는 멀티 홉 라우팅 프로토콜에 의존하며 노드들은 인접한 노드의 패킷을 전송해 주어야 한다. 노드들 중 해커에 의해 가용성의 거부을 하는 DoS, DDoS 공격이 이루어진다.

(4) 트로이목마, 웜, 바이러스 등

트로이목마, 웜, 바이러스 등 역시 유비쿼터스 컴퓨팅 장치에 위협을 가하여 가용성에 영향을 미칠 수 있고, 비밀성과 무결성도 침해할 수 있다.

3.1.2. 유비쿼터스 보안 요구 사항

유비쿼터스 컴퓨팅 보안의 목적은 인가되지 않은 사용자가 공유된 정보에 불법적으로 접근하거나, 사용자 공유 정보를 노출 및 변경하지 못하도록 하는 것이다. 이를 위해서 고려되어야 할 보안의 요건은 인증, 기밀(비밀)성, 무결성, 가용성(Availability) 등이 있다.

3.2. 홈 네트워크 보안 위협 및 요구사항

3.2.1. 홈 네트워크 보안 위협 사항

(1) 접근망 취약성

접근망은 홈 보안 게이트웨이를 기준으로 외부서비스 사업자와 연동되는 망을 말하며, 내부망 접속지점에 대한 네트워크 패킷 수집을 통하여 사용자 ID 및 그 밖의 중요정보 등이 노출될 수 있다[12].

(2) 댁내망 취약성

댁내망에는 댁내에서 처리하고 관리하기 위하여 기존 홈 기술을 이용하는 방식과 새로운 선로를 설치하는 방식으로 나눌 수 있고, 여기에 유선과 무선이 혼용되어 사용된다. 유선에는 Home PLC와 같은 기존기술과 USB, IEEE 1394, Ethernet과 같은 기술들과, 무선에는 Home RF, Bluetooth, Wireless LAN IEEE 802.11, Wireless

IEEE 1394, IEEE 802.15 등과 같은 기술이 있는데, 네트워크와 댁내 기기와 연동하여 서비스를 제공하는 이러한 연동의 취약점과 기술자체의 취약점으로 많은 보안위협[13]이 노출되게 된다.

3.2.2. 홈 네트워크 보안요소 및 요구 사항

(1) 보안요소

- 데이터 기원 인증 : 메시지를 인증하기 위하여 특정한 소스로부터 왔다는 것을 확립하여야 함. 관용 암호화와 디지털 서명을 이용한 공개키 방법 사용.
- 명령권한 검증 : 어떤 사용자가 어떤 일을 수행하기 위한 명령에 대해 정당한 권한이 있는지 검증.
- 메시지 무결성 보호 : 입력 메시지에 대해 정당하지 않은 데이터 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.

(2) 요구사항

홈 네트워크에서는 홈 서버와 홈 보안 게이트웨이를 통해서 전달되는 사용자와 서비스 제공자 및 집안의 정보가 부정한 사용자 및 위험으로부터 보호되고, 침입, 해킹, 바이러스 등과 같은 외부침입 행위에 대한 방어기능도 필요하다.

3.3. 홈 네트워크 보안 설계

3.3.1. 센서 네트워크 설계

센서 네트워크는 여러 개의 센서 네트워크 필드가 게이트웨이를 통해 외부 네트워크에 연결되는 구조를 갖는다. 센서 노드들은 가까운 싱크(Sink) 노드로 데이터를 전송하고 센서 노드로 집적된 데이터는 게이트웨이로 전송된다. 게이트웨이에서 관리자에게 전달되는 데이터는 위성통신, 유무선 인터넷 등을 통해 전송될 수 있으며, 이런 액세스 네트워크는 기존 인프라를 이용한다. 전체적인 센서 네트워크의 아키텍처는 그림 4와 같다. 센서 네트워크는 네트워크를 구성하는 일정 지역에 크기가 1㎟ 정도의 작은 노드들이 수 백 개에서 수 천 개까지 설치하여 통신하는 구조를 갖는다. 노드의 메모리가 너무 작기 때문에 많은 데이터를 저장하고 있을 수 없다. 따라서 네트워크나 라우팅 정보들을 필수적인 것들만 저장하여 이용하도록 간단한 프로토콜이 요구된다.

3.3.2. RFID 시스템 네트워크 설계

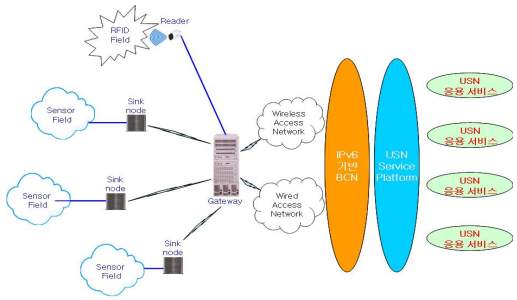

그림 3. 센서 네트워크 구조
Fig. 3. System Architecture of Sensor Network

RFID 시스템은 적은 기반시설과 낮은 비용으로 구축할 수 있는 위치 인식 시스템이다. RFID 시스템은 그림 5처럼 신체, 사물, 건물 등에 부착된 측정기, 센서, RFID 태그는 RFID 리더의 호출에 의해 대상체의 식별번호를 RFID 리더에게 전송하며, 이를 데이터 처리시스템에 보내 필요한 정보를 사용자가 이용할 수 있는 리소스, 즉 단말이나 주변 장치에 표시해 준다.

태그는 리더의 호출이 있을 때만 통신을 하고 리더기는 RF 모듈, 제어 유닛, 커플링 소자로 구성된다. 모든 리더기는 데이터 처리 시스템에 연결되어 있다. 대상체에 부착된 RFID 태그에 ID를 저장하고, 이를 포인터로 이용하여 대

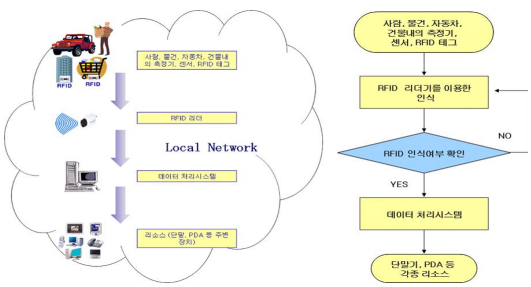

그림 4. RFID 시스템 구조
Fig. 4. System Architecture of RFID

상체에 대한 정보를 네트워크에 연결된 데이터 처리 시스템으로부터 얻는다.

3.4. 홈 네트워크의 인증 및 검증 설계

홈 네트워크에는 액세스 망과 홈 네트워크를 연결하기 위한 홈 서버, 홈 보안 게이트웨이 기술, 가정정보화 인프라 구축을 위한 유무선 홈 네트워크 기술, 오디오, 비디오 등 AV 기기들의 지능화에 따른 정보가전 기술, 사용자의 편의성 제공을 위한 미들웨어 기술 등이 포함한다.

홈 보안 게이트웨이에는 사용자 인증 서버 기능, 접근제어 서버 기능, 보안관리 서버 기능 또는 에이전트 기능이 탑재되고, 댁내 및 댁외 클라이언트에는 사용자 인증 클라이언트 모듈이 탑재되어 홈 네트워크를 위한 인증 및 검증을 통해 접근권한 제어 서비스가 이루어진다.

3.4.1. 사용자 인증 기능

안전한 홈 네트워크 환경 구축을 위해서는 홈 구성원에 대한 인증과정이 필요하며, 현재까지 많이 사용되고 있는 사용자 인증수단으로는 아이디(ID), 패스워드, 공인인증서, 생체인식기술 등을 사용한다.

3.4.2. 접근제어 기능

홈 네트워크 접근제어 기능은 댁내, 댁외에서의 홈서비스 및 홈 기기에 대한 불법 접근을 차단할 뿐만 아니라, 비록 정당한 사용자라 할지라도 불필요한 서비스 접근을 허용하지 않게 하는 실시간 권한 제어 기능을 제공하여야 한다.

3.4.3. 보안관리 기능

보안관리 기술은 홈 보안관리자(Home Security Manager)가 설정한 정책이 홈 보안 게이트웨이로 전송되어 홈서비스를 수행할 때 인증 및 접근 제어 정책이 반영되게 하는 것이다. 관리자가 설정한 보안 정책은 GUI (Graphical User Interface)를 통하여 정책으로 생성되며, 생성된 정책을 전달하여 보안기능이 탑재된 홈 보안 게이트웨이로 전달되어 수행하게 한다.

3.5. 홈 네트워크 보안 게이트웨이 설계

홈 네트워크는 일반 네트워크처럼 필요한 선로를 추가로 설비하는 것이 힘들기 때문에 기존의 가정에 설비되어 있는 통신선로(전화선), 전력선을 이용하여 구축한다. 기존에 구축된 외부 네트워크(인터넷)와 연결하기 위해서는 홈 네트워크를 하나의 서브 네트워크로 하여 이를 외부 네트워크에 연결할 수 있는 홈 보안 게이트웨이가 필수적이다[14]. 또한 홈 보안 게이트웨이는 각종 기기와 ADSL, Ethernet 전용선 등에 연결하기 위해서 기존의 게이트웨이와 마찬가지로 상호 프로토콜의 변환을 하는 동시에 한 서브 네트워크를 대표하는 라우터 역할을 수행한다.

3.5.1. 홈 보안 게이트웨이 환경 설계

(1) 기기 일반 및 표준

홈 보안 게이트웨이는 인터넷의 라우터 역할과 같이 접근망(Access Network)과 댁내망(Home Network)을 연결하는 역할을 수행한다. 접근 네트워크란 외부에서 인터넷을 통해 홈 보안 게이트웨이까지 이르는 통신 선로를 말하고, 댁내 네트워크란 홈 보안 게이트웨이를 기점으로 집안에서 홈 기기 사이의 연결된 내부 네트워크를 말한다. 또한 홈 보안 게이트웨이는 방화벽(Firewall)과 마찬가지로 IP 패킷 필터링을 이용하여 네트워크를 보호하며, 부가적으로 VPN과 같이 외부 접근에 대한 인증을 요구한다.

(2) 적용기술 설계

홈 보안 게이트웨이에 필요한 기본적인 기술은 홈 보안 게이트웨이가 현재 인터넷 인프라의 라우터적인 역할과 방화벽적인 역할을 하기 때문에 이 두 가지 동작을 바탕으로 하여, 접근제어 등의 기본적인 관리기능 및 부가적인 기능(프로토콜 변환)이 필요하다.

가. 라우팅(Routing) 기반 설계

홈 보안 게이트웨이에서 라우터 기능을 가지며, 패킷 필터링 기능은 발신 IP주소, 발신 포트, 수신 IP 주소, 수신 포트, 프로토콜 조류 등을 기반으로 하여 네트워크 간 데이터 전송을 제어한다. 이를 처리하기 위해 라우터는 네트워크의 보안정책을 가지고 특정 프로토콜과 서비스를 허가하거나 차단한다.

나. 방화벽(Firewall) 기반 설계

홈 네트워크를 보호하기 위해서는 외부에서의 불법적인 트래픽이 들어오는 것을 막고, 허가하거나 인증된 트래픽만 허용하는 적극적인 방어 대책인데, 홈 네트워크에서는 홈 보안 게이트웨이가 이러한 역할을 수행한다.

다. 접근제어(Access Control) 설계

홈 네트워크 서비스에 대한 접근을 제어하기 위한 기능이 필요하다. 현재 접근제어와 관련된 관리 기법들은 DAC, MAC, RBAC 등으로 구분될 수 있다. 그 중에서 RBAC는 사용자 대 역할매핑, 역할 대 접근허가 매핑의 2-Tier 방식을 지원함으로써, 다양한 접근제어 도메인에 적용할 수 있는 유연성을 가지도록 적용할 수 있다.

3.5.2. 홈 보안 게이트웨이 위협 및 대응 설계

(1) 침해 위협 설계

홈 네트워크는 기존의 유선망과 무선망의 통합된 형태로 구성되기 때문에 유·무선망에서의 도청 및 신분위장이 가능하고, 서비스 거부와 같은 공격으로 홈 보안 게이트웨이를 무력화 시킬 수 있다. 특히 무선망의 경우 특성상 네트워크에 접속하려는 기기에 대해서 계속적인 연결요청을 수행하게 되며 이러한 요청이 하나의 AP에 가상으로 다수가

요청될 경우 신규로 접속을 요구하거나, 현재 접속한 기기에서도 서비스가 불가능한 경우가 생길 수 있다.

(2) 보안 요구 및 대응 설계

홈 보안 게이트웨이에 대한 보안요구를 분석하기 위해서는 홈 보안 게이트웨이의 내부에 사용하는 프로토콜, 게이트웨이 운영체제에 대한 분석과 내·외부망에 대한 연관 관계를 분석이 선행되어야 한다.

Ⅳ. 유비쿼터스 홈 네트워크의 보안 구축 후 공격과 방어 실험

4.1. 유비쿼터스 홈 네트워크 보안 모델 구축

유비쿼터스 홈 네트워크시스템의 보안을 위해 본 논문에서는 유비쿼터스 홈 네트워크의 가용성을 저해할 수 있는 Dos, DDoS공격 등과 같은 외부의 공격을 차단할 수 있는 홈 보안 게이트웨이와 공인인증서를 이용하여 댁내의 홈 네트워크 구성 기기들에 접근에 대한 인증과 검증을 실시하고, RFID를 이용한 댁내 장비의 외부 입·출입 시 인증 절차를 구축함으로써 그림 5와 같은 보안이 강화된 유비쿼터스 홈 네트워크시스템 보안 모델을 구축한다.

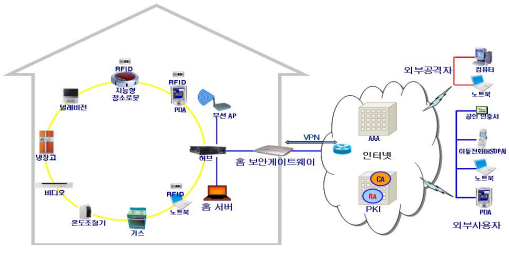

그림 5. 홈 보안 게이트웨이 실험 환경
Fig. 5. Simulation Environment of Home Security Gateway

4.1.1. 홈 네트워크 보안실험 구축 환경

- ❖ 홈 보안 게이트웨이 시스템 사양 : Linux RedHat 9.0(OS), Intel Pentium 3.0GHz (CPU), 1024MB RAM(Memory), 120GB(HDD)
- ❖ 홈 서버 : Windows XP Pro(OS), Intel Pentium 3.0GHz (CPU), 2048MB RAM (Memory), 200GB(HDD)
- ❖ 네트워크 : KT Megapass
- ❖ HUB : 24 Port Switching HUB
- ❖ 무선 AP : IEEE802.11, 5GHz, 54Mbps
- ❖ RFID : 18000-6, UHF 860 0 930MHz
- ❖ 냉장고, 비디오, 온도조절기, 가스, 노트북, PDA, 지능형청소로봇, 텔레비전, 창문, 전등 등

4.2. 홈 네트워크에서의 RFID 센서 감지 및 차단

홈 네트워크를 구성하는 다양한 디지털 기기 중 지능형 청소로봇, PDA 등에 RFID 센서를 설치하였다. RFID 리더기는 PDA의 RFID에 저장된 사용자 인증정보를 확인하여 인증 및 검증을 거쳐 홈 네트워크에 서 접속하여 작동하도록 설정한다. 댁내에서 홈 네트워크에 접속되어 사용하던 PDA나 지능형 청소로봇의 RFID 홈 네트워크의 범위를 벗

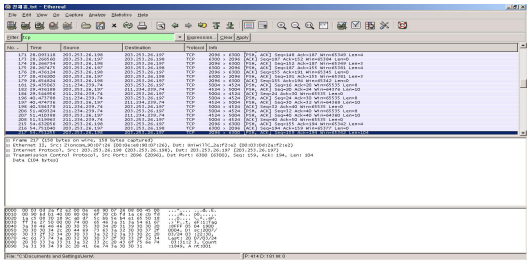

그림 6. RFID 헤더정보의 플래그가 1일 경우
Fig. 6. Flag's value 1 in RFID head

어날 경우 그림 6, 그림 7과 같이 홈 서버에서 무선 AP를 통한 RFID의 헤더 정보에 수록된 플래그를 0으로 변경시킨다. 이 때 플래그가 0으로 변환된 RFID는 댁내의 정보가 외부로 유출되지 않도록 관련 정보를 감추게 된다.

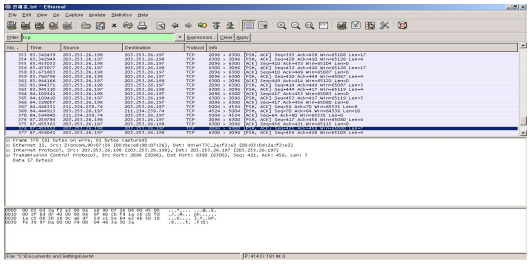

그림 7. RFID 헤더정보의 플래그가 0일 경우
Fig. 7. Flag's value 0 in RFID head

또한 지능형 청소로봇은 댁내에 들어오는 경우에 RFID의 인증을 위한 등록과 검증을 받아서 활동하며 스스로 집안을 움직이면서 댁내를 청소한다. 만약 RFID 센서 홈 네

트워크의 범위를 벗어나면 작동이 중지되도록 RFID 헤더정보에 수록된 마스킹에 의해 0으로 처리된다. 이 결과로 댁내의 장비가 외부로 반출되었을 때 댁내의 정보 유출을 방지하고, 유출된 장비의 남용을 차단할 수 있게 된다.

마스킹이 0으로 된 지능형 청소로봇을 재사용 하려면 홈 서버에서 관리자의 인증과 검증절차를 다시 거쳐 유비쿼터스 홈 네트워크에 재접속을 한다.

4.3. 홈 네트워크에서의 사용자 정보의 공인인증 및 검증

외부에서 홈 네트워크의 내부에 접속하여 댁내의 유비쿼터스 홈 네트워크 기기들을 관리하기 위해서는 홈 네트워크의 보안 게이트웨이에서 인증된 사용자임을 증명할 수 있는 그림 8과 같은 아이디 및 비밀번호가 필요하며, 아이디와 비밀번호의 사용자가 인증된 사용자임을 검증할 수 있는 방법으로 그림 9와 같은 공인인증기관에서 발급한 공인인증서를 통한 검증이 필요하다.

또한 홈 네트워크용 기기를 관리하기 위한 인증서 프로

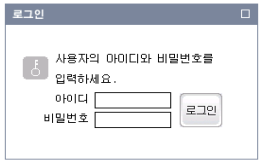

그림 8. 사용자 ID 및 비밀번호
Fig. 8. User ID & Password

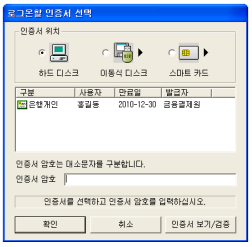

그림 9. 사용자 검증
Fig. 9. User Authentication

파일 표준안은 ITU-T SG17에 의한 기기 인증서 프로파일을 실행한다. 표준안에 따라 실험실에서는 그림 10과 같이 기기 인증서 프로파일의 기본 필드는 기존 X.509 V3를 준용하여 사용하며, 확장 필드는 Authority Key Identifier, Subject Key Identifier, Key Usage, Basic Constraint 등 네 가지 확장을 사용한다.

4.4. DoS, DDoS, IP Spoofing 공격과 방어

유비쿼터스 홈 네트워크에서 그림 11처럼 외부 공격자가 홈 보안게이트웨이에 대한 공격을 실험실환경에서 실시한다.

❖ 공격용 노트북 사양 : Windows XP Pro(OS),

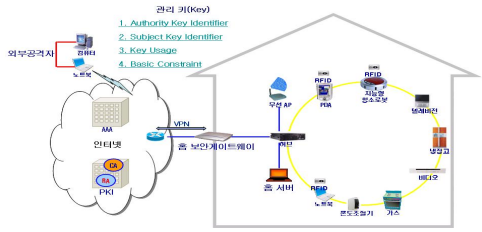

그림 10. 기기 인증 모델
Fig. 10. A Model in Authentication devices

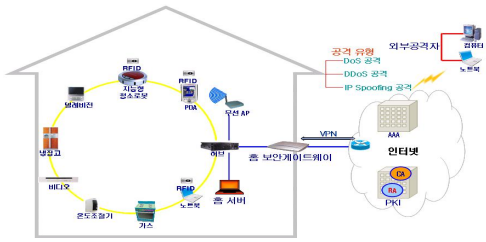

그림 11. 홈 보안 게이트웨이 구성
Fig. 11. Composition of Home Security gateway

Intel Pentium 2.0GHz (CPU), 1024MB RAM(Memory), 200GB(HDD)

❖ 공격 사용 툴 : TFN, SuperKoD

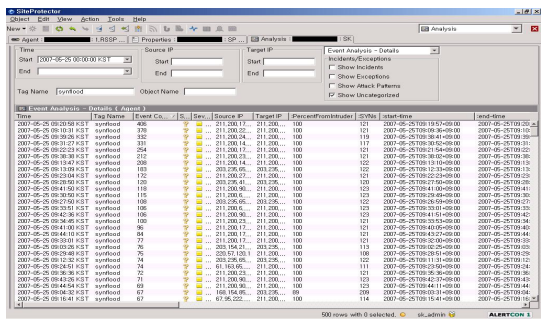

그림 12. DoS 공격 및 방어 로그
Fig. 12. Logs of DoS Attack and protection

공격을 한 결과에 대한 홈 보안 게이트웨이의 방어는 UDP, ICMP, Echo, TCP Syn 패킷 등을 조작한 SYN Flooding 방법 등으로 공격하여 DoS 공격을 유발한 첫 번째 공격은 그림 12처럼 성공적으로 차단하는 모습을 보여주고 있으며, 그림 13에서 TCP/UDP 포트 번호 기반으로 정의된 네트워크 어플리케이션을 통한 DDoS 공격을 차단하는 모습을 보여주었다. 그림 15에서 IP Source Address Spoofing과 Smurf을 이용한 공격에서는 처음에는 정상적

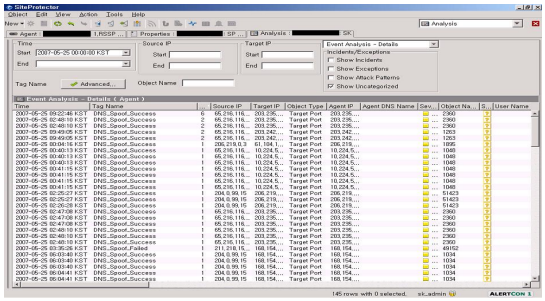

그림 13. DDoS 공격 및 방어 로그
Fig. 13. Logs of DDoS Attack and protection

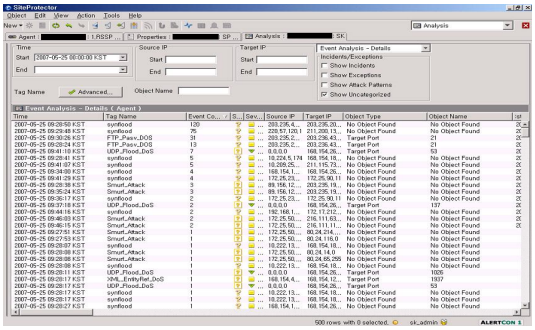

그림 14. IP Spoofing 공격 및 방어 로그
Fig. 14. Logs of IP Spoofing Attack and protection

인 인증 패킷으로 인하여 공격에 따른 트래픽이 증가 하였으나, 트래픽의 임계치에 이르자 홈 보안 게이트웨이가 공격으로 판단하여 공격 차단이 이루어지는 것을 확인하였다.

따라서 유비쿼터스 홈 네트워크에 대한 외부 공격자의 공격에 대한 보안이 안정적으로 이루어지는 것으로 판명되었다.

V. 결론

본 논문을 통해 유비쿼터스 보안과 유비쿼터스 홈 네트워크를 위협할 수 있는 여러 취약점 및 DoS, DDoS, IP Spoofing 공격 내용과 홈 보안 게이트웨이, 외부망, 댁내망, 각종 댁내 기기 등에 대한 보안 위협 사항 및 보안 요구사항에 대하여 연구하고, 외부에서 DoS, DDoS, IP Spoofing 공격을 실시하고 보안이 작동하는지를 실험하였다.

우선 유비쿼터스 네트워크의 구성을 위한 RFID와 센서 네트워크를 이용한 홈 네트워크 보안과 사용자와 댁내 각종 기기에 대한 인증과 검증방안을 설계하여 실험실 환경에서 적용해 보았다. 또한 홈 네트워크 보안에서의 핵심인 홈 네트워크 보안 게이트웨이를 실험실에서 설계 하였다.

설계한 유비쿼터스 홈 보안 네트워크 모델 시스템을 실험실에서 구축하여 홈 네트워크에서의 RFID 센서 감지를 이용해서 댁내의 기기들이 외부로 유출된 경우와 외부의 기기가 댁내로 반입되는 경우에 대한 기기의 PKI 공인인증 및 검증을 통해 보안이 강화된 것을 실험하였다. 또한 정당한 사용자임을 확인할 수 있는 인증과 검증절차를 설계 · 적용하여 모델을 구성함으로써 외부의 불법적인 접근을 방지하고 내부 사용자의 원활한 접근을 보장하였다.

이와 함께 외부의 DoS, DDoS, IP Spoofing 공격에 대해 방어 할 수 있도록 홈 보안 게이트웨이의 설계와 구성을 한 후 외부의 공격자의 DoS, DDoS, IP Spoofing공격에 대해 방어하는 실험을 통해 유비쿼터스 홈 네트워크 및 시스템에 대한 보안이 이루어 졌음을 증명하였다.

향후 연구로는 가용성과 무결성을 훼손할 수 있는 무선 분야의 보안과 댁내 유비쿼터스 홈 네트워크 기기간의 호환 문제에 따른 보안 취약점을 제거하기 위한 보안연구와 표준화 연구가 진행되어야 할 것이다. 이러한 유비쿼터스 홈 네트워크에 대한 보안 연구가 충분히 이루어졌을 때 유비쿼터스 시대가 우리들 생활에 전개될 수 있을 것이다.

참고문헌

[1] 김수지. “유비쿼터스 컴퓨팅 시스템의 보안 요구사항에 관한 연구.” 성균관대학교, 석사논문, 2006. 06.

[2] 박대우, 서정만. “TCP/IP 공격에 대한 보안 방법 연구.” 한국컴퓨터정보학회논문지, 제10권 제5호, pp 217-226, 2005. 11. 30.

[3] 이재용. “유비쿼터스 센서 네트워킹 기술.” 한국정보통신기술협회, TTA저널, 제95호, pp 78-83, 2004. 10.

[4] RFID White Paper, accenture, 2001.

[5] Ian F.Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, “A Survey on Sensor Networks”, IEEE Communications Magazine, August 2002.

[6] K. S. J. Pister, J. M Kahn, and B. E. Boser. Smart dust : Wireless network of millimeter-

scale sensor nodes, 1999.
〔7〕 박용수, 김일희, 김희문. "USN 환경에서의 분산형 인증체계 연구." 한양대학교 산학협력단, 한국정보보호진흥원, 2006. 11.
〔8〕 W. Ye, H Heidemann, and D. Estrin, "An Energy-efficient MAC protocol for wireless sensor networks", In 21st conference of the IEEE computer and Communications Societies (INFOCOM), volume 3, pages 1657-1576, June 2002.
〔9〕 C. Karlog and D. Wagner, "Secure Routing in Wireless First IEEE International Workshop on Sensor Networks & Application (WSNA'03), San Diego, CA, Sep, 2003.
〔10〕 서운석, 신순자, 구자동, 임진수. "유비쿼터스 컴퓨팅 환경에서 보안 및 인증 서비스 방향연구." 한국전산원, 2004. 09.
〔11〕 B.j.Bonfils, P. Bonnet, "Adaptive and Decentralized Operator Placement for In-Network Query Processing", IPSN'03, LNCS 2634. April, 2003,
〔12〕 김여진, 송오영, 박세현. "홈 네트워크 환경에서의 보안공격에 따른 보안강화 연구." 한국정보보호학회, 하계정보보호학술대회 논문집 제16권 제1호, pp431-434 2006.
〔13〕 전용희. "홈네트워크 보안 관련 기술." 한국통신학회, 제21권 제3호, pp81-95. 2004.03.
〔14〕 권진혁, 정재윤, 김학배. "홈 네트워크 환경에서 홈 게이트웨이와 관리 서버 개발." 한국정보처리학회, 제12권 제2호, pp261-266, 2005. 04.

저 자 소 개

천 재 홍

2002년 한국방송통신대학교 경영학과 (경영학사)
2007년 숭실대학교 정보과학대학원 정보보안학과 졸업(공학석사)
1997년~ 한국환경정책·평가연구원 환경정보센터 구원(정보보안담당)
관심분야 : 네트워크 보안, VoIP 보안, WEB 보안

박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)
2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006년 정보보호진흥원 선임연구원
2007년 호서대학교 벤처전문대학원 정보보호전공 조교수
〈관심분야〉 정보보호, 유비쿼터스 네트워크 및 보안, 보안 시스템, CERT/CC, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality