유비쿼터스 환경에 적합한 홈네트워크 보안요구사항 및 대응 방안

류우권*, 이희조
*고려대학교 컴퓨터정보통신대학원
e-mail: rwk-1@korea.ac.kr

Home Network Security Requirements and Response for Ubiquitous Environment

Woo-Kwon Ryu*, Heejo Lee
*Graduate School of Computer and Information Technology, Korea University

요 약

최근 들어 언제 어디서나 컴퓨팅이 가능한 유비쿼터스 컴퓨팅(Ubiquitous Computing) 사회가 되면서 개인의 컴퓨팅 환경 의존도가 증가되었고, 따라서 사이버공격으로 인한 개인생활의 위협도 증가할 수밖에 없게 되었다. 더욱이 향후에는 원격진료와 같이 개인의 생명과 직결된 유비쿼터스 서비스가 활성화될 것이므로 사이버공격으로 인해 재산뿐 아니라 생명까지 위험에 처하는 경우가 늘어나게 될 것이다. 이로 인해 유비쿼터스 환경에 적합한 홈네트워크 보안(Home Network Secutity)의 중요성이 부각되게 되었다. 본 논문에서는 안전한 U-홈네트워크(Ubiquitous-Home Network) 구축에 필요한 기술들을 유·무선 기준으로 구분하고, U-홈네트워크 환경에서 발생할 수 있는 다양한 침해유형을 분석하여, 이를 막아낼 수 있는 대응방안을 수립하고, 안전한 U-홈네트워크 구축을 위해 필요한 기존의 보안요구사항들을 살펴본 후에 U-홈네트워크에 적합한 추가적 보안사항을 제안하고자 한다.

1. 서론

유비쿼터스 홈(Ubiquitous Home)이란 유·무선 통신 네트워크를 기반으로 가정 내의 다양한 가전기기 및 센서로 구성되는 네트워크의 상호 연동을 통해 다양한 서비스의 환경이 가능한 것을 의미한다.

현재 미국, 일본, 유럽 등 세계 각국은 국가기관, 유수 대학 연구소, 첨단 기업들을 앞세워 홈네트워크를 국가적 과제로 추진하고 있다. 국내 정보통신부에서도 IT839전략에 가치의 최정점에 있는 홈네트워크 서비스와 네트워크 기술과제를 내 놓고 있으며 2007년까지 전체인구의 약 60%인 1,000만 가구에 홈네트워크를 보급하고 국내외 통신·가전 업체들간의 표준화를 유도, 홈서버, 통합미들웨어 등 핵심기술의 개발을 지원하는 등 지원을 아끼지 않고 있다[1].

언제 어디서나 컴퓨팅이 가능한 유비쿼터스 컴퓨팅(Ubiquitous Computing) 사회에서는 개인의 컴퓨팅 환경 의존도가 증가함에 따라 사이버공격으로 인한 개인생활의 위협도 증가할 수밖에 없다. 더욱이 향후에는 원격진료와 같이 개인의 생명과 직결된 유비쿼터스 서비스가 활성화될 것이므로 사이버공격으로 인해 재산뿐 아니라 생명까지 위험에 처하는 경우가 늘어나게 될 것이다. 이로 인해 유비쿼터스 환경에 적합한 홈네트워크 보안의 중요성이 부각되게 되었다. 본 논문에서는 먼저 안전한 U-홈네트워크(Ubiquitous-Home Network) 구축에 필요한 기술들을 유·무선 기준으로 구분하고, U-홈네트워크 환경에서 발생할 수 있는 다양한 침해유형을 분석하여, 이를 막아낼 수 있는 대응방안을 수립하고, 안전한 U-홈네트워크 구축을 위해 필요한 기존의 보안요구사항들을 살펴본 후에 U-홈네트워크에 적합한 추가적 보안사항을 제안하고자 한다.

본 논문의 구성은 2장에서 U-홈네트워크 기술을 분류를 하고, 3장에서는 U-홈네트워크 환경에서 발생할 수 있는 침해유형을 분석하고, 대응방안을 제안하고, 4장에서는 U-홈네트워크 보안의 목적과 기존의 보안요구사항과의 비교를 통해 U-홈네트워크에 필요한 추가적 보안사항을 제안하고, 5장은 결론 및 향후과제를 제시한다.

2. U-홈네트워크 기술

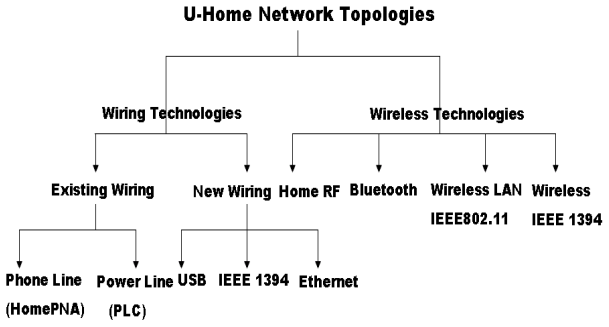
U-홈네트워크의 기본개념은 집안의 정보가전기기를 네트워크로 묶고 이를 외부의 인터넷 망과도 연결하여 집 내부 및 외부 어디서나 사용자의 위치에 관계없이 정보가전기기를 제어할 수 있도록 하고 각종 편의를 위한 홈서비스를 제공하겠다는 것이다[2].

U-홈네트워크의 기술분류는 보는 시각에 따라 다소 차이가 있으나, 표 1에서 보듯이 크게 유·무선 홈네트워킹, 정보가전, 지능형미들웨어 등 4개의 분야로 나눌 수 있다[3].

<표 1> U-홈네트워크 구성 요소별 분류

1단계	2단계	3단계
U-홈네트워크 기술	홈플랫폼 기술	홈서버/홈게이트웨이 기술
		홈네트워크 보안
		개방형 서버 기술
	유·무선 홈네트워킹 기술	유선홈네트워킹 기술 (Ethernet, PLC, IEEE1394)
		무선 홈네트워킹 기술 (WLAN(802.11a/b/g/n),WPAN(UWB,ZigBee))
	정보가전기술	지능형 정보가전
		홈센서 기술(센서,RFID)
	지능형 미들웨어 기술	홈네트워킹 미들웨어 기술
		상황적응형 미들웨어 기술
		멀티 모달 인터페이스 기술

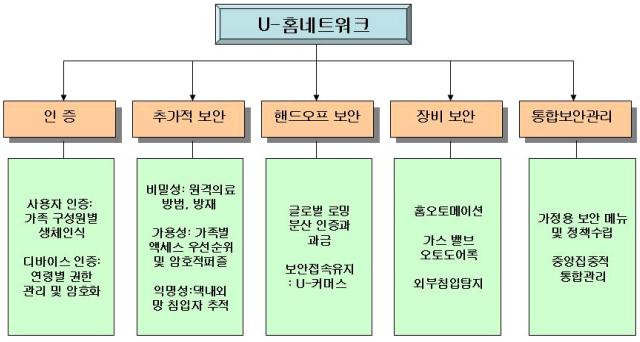
그리고, 이러한 기술들을 다시 유선 기반 기술과 무선 기반 기술로 구분을 해서 토폴로지를 작성해 보면 그림 1과 같다[4].



(그림1) U-홈네트워크 유·무선망 기술 분류도

3. U-홈네트워크 침해 유형 분석과 대응 방안

U-홈네트워크에서는 이종의 유·무선 네트워크와 다양한 프로토콜 등의 혼재로 기존 인터넷 등에서 발생되던 보안취약성 외에도 추가적으로 고려해야할 보안취약성이 많이 존재한다[5]. U-홈네트워크의 다양한 정보가전기기들은 인터넷과의 연결로 사이버공격의 대상이 될 수 있으며, 더욱이 U-홈네트워크 내의 정보기기의 다양성과 기기간의 자원의 공유 등으로, 보안측면에서 고려해야할 보안요구사항은 더욱 복잡해지고 다양화되고 있으며, 이를 정리하면 그림 2와 같다.



(그림2) U-홈네트워크 보안프레임

3.1 침해 유형 분석

현재까지는 U-홈네트워크 환경에서 발생할 수 있는 구체적인 침해 유형의 사례를 찾기가 쉽지는 않다. 왜냐하면, 지금의 현실은 완전한 유비쿼터스의 환경이 아니고 초기단계의 유비쿼터스 환경과 유·무선 네트워크의 혼합 환경이기 때문이다. 그러므로, 기존의 유·무선 네트워크 환경과 지금까지 이루어진 유비쿼터스 환경에서 발생하고 있는 침해 유형 분석을 기초하여[6], U-홈네트워크 환경에서 발생하게 될 침해유형들을 예측할 수밖에 없으며, 이를 정리하면 표2와 같이 기술할 수 있다.

<표 2> U-홈네트워크 침해 유형

침해유형	보안위협
기존의 침해 유형	
인 증	공개키 암호시스템
비밀성	IP Spoofing
무결성	트로이목마, 웜 바이러스
가용성	DOS 공격(서비스거부공격)
추가적 침해 유형	
인 증	유비쿼터스 장치의 분실 및 도난
	Rouge AP
비밀성	IP Spoofing/댁내망 도청, 트래픽 분석 공격
	가족 구성의 신원정보 및 의료정보
무결성	가정용 유비쿼터스 기기에 대한 바이러스
가용성	댁내 단말기기에 대한 DOS 공격
	신호방해 공격
	배터리소진 공격
익명성	댁내·외 망에서 발생하는 불법사용자
핸드오프 시큐리티	핸드오프과정에서 보안 접속 유지와 보안(U-커머스 거래 활성화, 글로벌 로밍의 분산 인증과 실시간 패킷 과금 문제)
장비보안	홈오토메이션기기 공격(가스, 홈뷰어, 도어록)

3.2 보안 위협별 대응 방안

○**인증**: 통신에 참여하는 송신자와 수신자는 상대방의 신원을 직접 확인할 수 있어야 한다는 것

- 장치의 분실 및 도난에 대비한 인증방법: 장치의 절도 및 분실은 비밀성에 대한 위협으로 유비쿼터스 장치를 소유한 사람은 장치에 저장된 MAC(Media주소와 Access Code), WEP(Wireless Equivalent Privacy)키 등의 인증정보를 소유하게 되기 때문에 접근권한을 얻게 하므로 이를 해결하기 위해서 장치 독립적인 사용자 인증, 암호화를 해야 한다.
- Rouge AP: 무선랜의 경우 단방향 인증만을 제공하므로, Rouge AP가 무선에 위치하면 공격자는 AP에 대한 인증 없이 네트워크에 접근이 가능하게 되어 DOS 공격의 거점이 될 수 있게 되므로 이를 해결하기 위해 양방향 인증을 해야 한다.
- 적용분야: 가정내 다양한 유비쿼터스 기기들에 대해 가족 구성원의 연령별 권한 관리, 가족별 개체식별과 검증(생체인식), 사용자 정보 접근 제어(홈스마트카드, RFID)

○**비밀성**: 안전한 비밀 통신 채널을 통한 비밀성 보장

- IP Spoofing: 비밀성에 대한 공격으로 무선 신호는 벽을 통과하여 외부로 전달이 될 수 있고, 신호 범위 내에 존재하는 누구나 접속이 가능하므로 전송되는 정보가 암호화 되어 있지 않으면 도청의 위험이 존재하므로 정보의 암호화를 해야 한다.
- 신원정보 및 위치 정보 노출: 메시지에 대한 비밀성은 메시지 내용에 대한 비밀 유지를 가능하게 한다. 그러나, 언제 누가 어디로 전달되는지는 메시지 비밀성만으로는 유지할 수 없다. 이러한 정보는 공격자의 관심의 대상인 동시에 사용자의 프라이버시 문제이기도 하므로 익명성이 요구 된다.
- 적용분야: 가정내 원격의료 관련 개인 의료정보, 개인 신상 및 각종 금융관련 서비스에 대한 정보 누출 위협(신용카드, 공인 인증서 등)

○**무결성**: 인증되지 않은 사용자가 중요 정보를 변경하는 것을 방지하는 것

- 바이러스: 트로이목마, 웜 바이러스 등 바이러스는 기존의 컴퓨터 네트워크에서도 많은 영향을 주고 있지만, 가정용 유비쿼터스 장치들에는 더 큰 위협이 될 것이다. 대응방안으로 무결성을 보장해 주도록 백신프로그램을 사용한다.
- 적용분야: 가정용 유비쿼터스 관련 기기 오작동(지능형청소로봇, 홈뷰어, 통합리모콘, 홈서버)

○**가용성**: 시스템이 요구되는 수준의 일정한 기능을 수행할 수 있도록 하는 것

- DOS 공격: 댁내 단말기기에 대한 DOS 공격으로 노드들 중 하나가 협력을 거부할 경우 DOS 공격으로 이루어지게 되므로, 중요한 사용을 위해 액세스에 등급을 두어서 가용성을 보장해줘야 한다.
- 신호방해공격: 신호방해 공격은 장치의 가용성을 침해하는 것으로 무선 시스템에 대한 고전적인 공격방법으로 통신 채널을 혼선시켜서 정상적인 서비스를 제공하지 못하게 하는 공격으로 이를 막기 위해서 확산대역 주파수 호핑을 사용한다.
- 배터리소진공격: 배터리 소진 공격은 유비쿼터스 장치의 배터리를 짧은 시간 내에 방출시켜서 장치를 더 이상 사용하지 못하게 하는 공격으로, 이를 막기 위해서는 DOS 공격에서처럼 서비스 액세스에 우선 순위를 두어서 가용성을 보장한다.
- 적용분야: 가정내 방범·방재와 원격 감시·제어 그리고, 각종 의료기기 사용이 불가능하게 되어 재산의 손실은 물론 소중한 가족의 생명에 위협 가능

○**시큐리티**: 핸드오프과정에서 보안 접속 유지·보안과 댁내망에서의 장비보안

- 장비보안: 댁내망에서 이루어지는 홈오토메이션기기와 관련된 장비들에 대한 공격
- 적용분야: 핸드오프 시큐리티, U-커머스 거래 활성화, 글로벌 로밍의 분산 인증과 실시간 패킷 과금 문제, 홈오토메이션 기기와 연결된 방범, 방재, 홈 의료기기 위험노출(가스, 홈뷰어, 도어록)

4. 기존 보안 요구 사항과 추가적 보안 사항

U-홈네트워크 환경에서의 보안의 목적은 인가되지 않은 사용자가 공유된 정보에 불법적으로 접근하거나 사용자 공유정보를 노출 및 변경하지 못하도록 하는 것이다. 이를 위해서 고려되어야 할 보안의 요건은 인증(authentication), 비밀성(confidentiality), 무결성(integrity), 가용성(availability)외에도[7] 기

밀성, 권한관리, 익명성, 핸드오프 시큐리티, 장비보안, 통합보안관리 등의 추가적인 보안요구 사항이 제공되어야 하며 표3, 표4와 같이 정리할 수 있다.

<표 3> 기존의 보안 요구 사항

유 형	기존 보안 요구 사항
인 증	- 상호인증 - 동적키 사용 - 무선 구간 키 교환 기반제공 - 장치 독립적인 사용자 인증 - PKI오버헤드 감소 - 안전 전이 협약
비밀성	- 트래픽 데이터 암호화 - 키 관리 기법 제공 - 이동형/서버 장치 내 정보를 암호화 - 저 전력 암호 알고리즘
무결성	- 유비쿼터스 기기에 맞는 무결성 보장을 위한 암호화적 메커니즘
가용성	- DOS 공격에 대해 사용자 접근 우선 순위

<표 4> 추가적 보안 사항

유 형	추가적 보안 사항
인 증	- 가족 구성원의 연령별 권한 관리 - 가족별 개체식별과 검증(생체인식) - 사용자 정보 접근 제어(홈스마트카드,RFID)
비밀성	- 통신 당사자간의 비밀정보를 공격자로부터 보호(원격의료: 개인 신상 정보 누출) - 도청, 트래픽 분석 등의 공격으로부터 보호(방범, 방재, 홈 의료기기 위험노출)
가용성	- 댁내 단말기기에 대한 DOS 공격 - 가족 구성원별 서비스 액세스 우선순위 - 암호적인 퍼즐(cryptographic puzzle) 사용
익명성	- 익명성에 대한 사용자의 추적권한(댁내·외망에서 발생한 불법사용자 추적)
핸드오프 시큐리티	- 동일한 서비스 네트워크 내의 안전한 핸드오프 보안(글로벌 로밍의 분산 인증과 실시간 패킷 과금 문제) - 핸드오프과정에서 보안 접속 유지와 보안(U-커머스 거래 활성화)
장비보안	- 홈오토메이션기기 보안 - 가스 밸브/ 자동 도어록 시스템 보안 - 외부침입자 탐지시 경찰서 및 경비업체 자동연계
통합보안 관리	- 간단하며 효율적인 보안 메뉴와 정책수립 - 편리성과 안전성을 동시에 제공하는 중앙집중적인 통합관리(홈기기 사용자는 보안전문가가 아니다)

이상에서 살펴본 보안 요구 사항은 기존의 유·무선 홈네트워크 환경과 일반적인 유비쿼터스 환경에서 발생할 수 있는 보안요구사항들의 분석을 통해서, 앞으로 U-홈네트워크 환경에서 새롭게 추가적으로 요구될 수 있는 보안요구사항들을 일곱 가지로 제안하였다.

5. 결론 및 향후 과제

정부의 IT839전략에 따라 부가가치의 최정점에 있는 홈네트워크 서비스는 구축될 것이다. 그러나, 안정성이 확보되지 않은 홈서비스는 프라이버시 침해에서부터 생명에까지 위협을 줄 수 있게 될 것이다.

따라서, 본 논문에서 제시한 U-홈네트워크에 적합한 침해유형분석과 그에 따른 대응방안에 적절한 보안요구사항을 유비쿼터스 신도시 주택 건설시 적용토록 함으로서 안전한 유비쿼터스 환경을 구축하는데 큰 기여를 할 것이며, 또한 향후에 발생하게 될 U-홈네트워크 관련 사이버 범죄의 위협을 사전에 예측하여 대응할 수도 있을 것이다.

향후 연구 과제로는 U-홈네트워크 기기들에 효율적인 보안정책 수립 및 적용을 통한 보안관리대책을 정립함으로써 유비쿼터스 컴퓨팅 상황에 능동적으로 대처할 수 있을 것이다.

참고문헌

[1] 박세현, “유비쿼터스 홈을 위한 상황인지 서비스”, 2005.05

[2] 한종욱 외, “안전한 홈네트워크 구축을 위한 보안요구사항”, 2004.05

[3] 장동현 외, “홈네트워크 국내·외 동향 및 발전전망”, 2004.05

[4] 한치문 외, “디지털 홈네트워크 기술표준개론”, 진한멤엔비, 2004.02

[5] 한국전자통신연구원, “유비쿼터스 홈네트워크 침입대응 기술”, 2005.05

[6] 유동영 외, “홈네트워크 침해 위협에 대한 홈게이트웨이 보안 요구 및 대응방안”, 2004.11

[7] 한종수 외, “유비쿼터스기술”(RFID와 홈네트워킹), 도서출판세화, 2005.02