Home Network 환경에서의 보안 기술

임진우, 이옥연
고려대학교 정보보호대학원, 국민대학교

A Study on Security technology in the Home Network

JinWoo Lim, Okyeon Yi
Dept. of Information Security ,Korea University
Kookmin University

요 약

최근 유·무선 통신 기술이 고도화 성장함에 따라 정보 기기, 디지털 가전 기기, 홈 오토메이션 기기들을 하나의 통신망으로 묶어 언제, 어디서나, 임의의 장비를 사용하여 홈 기기들을 제어하고 관리할 수 있는 홈 네트워크를 구축하려는 움직임이 빠르게 진행되고 있다. 본 고에서는 홈 네트워크상에서 발생할 수 있는 보안 위협, 보안 요구사항 등에 대하여 정의하였으며, 무선의 특성상 보안이 취약한 무선 보안 기술의 응용에 대해 제시하였다.

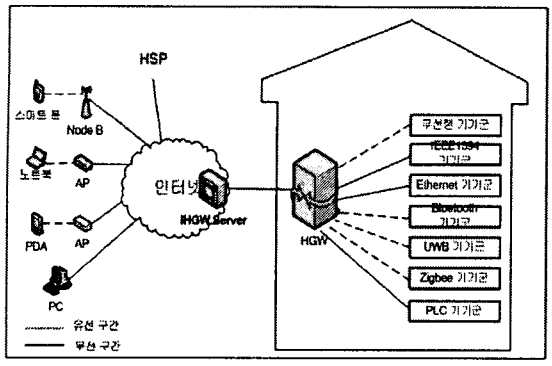
1. 서론

최근 가정내 정보기기, 디지털 가전기기, 홈오토메이션기기들에 통신 기능을 부여해 하나의 통신망으로 묶어 언제, 어디서나, 임의의 디바이스를 사용하여 가정내 각종 기기들을 제어, 관리할 수 있는 홈 네트워크를 구축하려는 시도가 활발히 진행되고 있는 상황이다. 이러한 홈 네트워크를 실현하기 위한 기술로는 유·무선 네트워크 기술, 이기종 네트워크의 상호 연동을 위한 기술, 홈 네트워크에서의 보안 기술 등이 있다. 유선 기반 네트워크 기술로는 기존의 전화 배선 선로를 이용해 고속의 가정내망을 구축하려는 HomePNA기술, 가정내 전력선을 이용하여 통신망을 구축하는 PLC기술, USB를 이용하여 여러 주변 장치와 통신망을 구성하는 기술, 근거리 통신망으로 현재 전 세계적으로 널리 사용되는 이더넷 기술, 고속 시리얼 전송이 가능하여 A/V 디지털 기기의 멀티 미디어 데이터를 전송할 수 있는 IEEE1394 기술 등이 있고, 무선 기반 네트워크 기술로는 Wireless LAN 기술, 무선 랜보다 전송거리가 가까운 곳에서 사용되는 Wireless PAN(Personal Area Netwrok) 기술로 Bluetooth, Zigbee, UWB 등이 있다. 이기종 네트워크의 상호 연동을 위한 기술로는 미들웨어와 홈 서버 기능을 수행하고 이기종 네트워크를 수용할 수 있는 통합형 홈 게이트웨이 기술이 있다. 홈 네트워크에서의 보안 기술로는 각 네트워크에서 제공하는 보안 기술과 보안 메커니즘을 연동하는 기술 등이 있다. 본 논문에서는 홈 네트워크에서의 보안 위협과 보안 요구사항들을 정의하고, 보안 취약성이 큰 무선 매체를 이용한 통신에서의 보안 구조에 대해 중심적으로 살펴본다 [5].

2. 홈 네트워크 구조

홈 네트워크에서 네트워킹을 위한 기술로는 유무선 네트워크 기술, 가정내 정보전자 가전들이 상호 통신하기 위한 액세스망 기술, 외부 액세스망과 홈을 연동시키기 위한 게이트웨이 기술이 있고, 네트워크 구성 장비로 살펴보면 댁내 정보기기, 전자 기기, 홈오토메이션 기기, 이들을 연결하는 홈 게이트웨이 장비, 외부망에서 홈 게이트웨이에 접근을 위한 장치로 PDA, Smart Phone, 노트북, PC 등이 있다. [그림 1]은 이러한 기술과 장비를 이용하여 구성되는 홈 네트워크의 구조를 보여 준다 [2].

1) HSP(Home Service Provider) : 홈 네트워크 서비스를 제공하는 사업자로 서비스를 원하는 User에게 네트워크 설계 및 컨설팅에서부터 인터넷 접속 서비스, 웹 사이트 건설 및



[그림 1] 홈 네트워크 구조

웹 서비스 등을 제공한다. 이를 위해 HSP는 인터넷 접속에 필요한 장비 및 통신회선 등을 갖추고 있다.

2) **HGW**(Home Gateway) : 외부망과의 인터페이스와 가정내 정보가전기기들에 대한 인터페이스를 수용하고, 대용량의 저장장치가 있어 가정내의 멀티미디어 데이터의 저장, 관리 및 분배의 역할을 하는 홈 서버 [3] 기능을 포함한다. 또한 홈 네트워크를 이루는 장비에 대한 인증을 수행하고 가정내 서비스 사용자에 대한 권한 부여 기능을 수행한다. 이를 위해 다양한 기기간에 정보를 교환하고 관리, 제어할 수 있는 미들웨어 기술을 탑재하는 형태의 통합형 홈 게이트웨이이다.

3) **IHGW Server**(Integration HGW Server) : 인터넷을 사용할 수 있는 여러 기기에 대한 인터페이스를 가지고 있고, HGW와 통신을 한다. 또한 AAA(Authentication, Authority, Accounting)의 기능으로 홈 네트워크 사용자에 대한 인증, 권한부여, 과금 결정 등을 수행하고, 과금에 대한 정보를 HSP에게 넘겨준다.

4) **유·무선 통신 기기군** : 가정내 유·무선 통신 기술에 의해 HGW와 통신을 한다. 유무선 통신 기술의 선정은 가격, 효율성, 신뢰성 등의 고려사항을 가지고 사용자가 선택할 수 있고, 좀 더 효과적으로 홈 네트워크를 구성하기 위해 HSP에게 컨설팅 요구를 함으로써 이루어 질 수 있다. [표 1]은 가정내 망을 구축할 때 고려할 필요가 있는 무선통신 기술을 비교한 표이다 [1].

3. 홈 네트워크에서의 보안 위협 및 보안 요구

홈 네트워크상에서의 정보 보안에 대한 위협은 인증, 기밀성, 무결성, 부인 봉쇄, 접근제어와 같은 보안 서비스 요구사항을 충족하지 못하는 것이다. 즉, 지금까지 유·무선 네트워크에서의 보안에 대한 개념을 홈 네트워크에도 그대로 적용하면 된다. 그러나 그 적용범위가 기존 유·무선 통신시스템에 비해 더 확장됨으로써 다양한 공격 유형과 예측하기 힘든 공격자가 나올 것이다.

3.1 홈 네트워크에서 공격자

공격자 유형은 크게 수동적 공격자, 능동적 공격자로 나누어 볼 수 있다. 수동적 공격자는 단지 송·수신되는 데이터를 관찰하고, 데이터를 분석함으로써 통신하는 주체의 키를 획득하기 위해 노력한다. 이렇게 해서 획득한 키를 통해 수동적 공격자는 통신을 하는 사용자가 어떤 메시지를 주고받는지 알 수 있다. 즉, 수동적 공격자는 송·수신 데이터에 대한 분석은 하는데, 어떠한 악의적인 행동을 가하지 않는다. 반면에 능동적 공격자는 키를 획득하여 송수신 메시지에 대한 위·변조를 가함으로써 어떤 이익을 취하려고 하거나, 통신을 방해하는 악의적인 행동을 한다.

3.1.1 홈 네트워크에서의 수동적 공격자

[표 1] 무선 통신 기술 비교

분 류	HomeRF	IrDA	무선 1394	무선 LAN	블루투스	UWB	Zigbee
표준	SWAP	IrDA v2.0	None	802.11	802.15.1	802.15.3a	802.15.4
전송 속도	1,2,10 Mbps	4 Mbps	54 Mbps	11, 55 Mbps	2~10 Mbps	100 Mbps 이상	20~250 Kbps
최대전송거리	50m	3.8m	4.5m	50~100m	10m	10m	10m
응용 분야	PC centre	이동 단말	정보가전기기	office 환경	전자 가전	통신 및 레이더	전등, VCR 제어
비용	중·저	저	고	고	중	저	저
장점	높은 유연성	높은 유연성	네트워크간의 연동	높은 유연성	높은 유연성	높은 대역폭	초저전력 소비
단점	전송 속도	기기간 배치 문제	전송 거리	간섭	호환성과 편의성 문제	기술 기준 제정	전송 속도

1) 트래픽 분석 : 송·수신되는 데이터의 트래픽을 분석할 수 있다.

2) 홈 기기간 송·수신 데이터 분석 : 기기간 무선으로 연결된 경우 홈 외부에서 기기간 통신 데이터 분석을 통해 가정에서 어떤 일을 수행 하는지 알 수 있다.

3) 프라이버시 침해 : 공격자는 유·무선 구간에서 송·수신되는 데이터를 관찰하여 서비스 사용자의 프라이버시를 침해할 수 있다.

3.1.2 홈 네트워크에서의 능동적 공격자

1) 데이터 위·변조 : 통신 데이터를 변조함으로써 정당한 서비스를 받지 못하게 한다. 또한 데이터를 위조해서 전송함으로써 서비스 사용자가 예기치 않은 결과를 초래한다.

2) 가정내 기기에 접근 : 가정내 기기가 무선으로 연결된 경우 데이터 분석을 통한 키 획득을 통해 가정내 기기에 접근하여 기기를 제어할 수 있다.

3) 프라이버시 침해 : 가정내 기기에 접근하여 웹 카메라를 통해 홈 내부를 들여다 볼 수 있고, 각종 기기들의 정보를 획득할 수 있다. 무선 매체를 사용하는 access control 및 암호화 등의 보안 구조가 요구된다.

3.2 홈 네트워크에서의 보안 요구사항

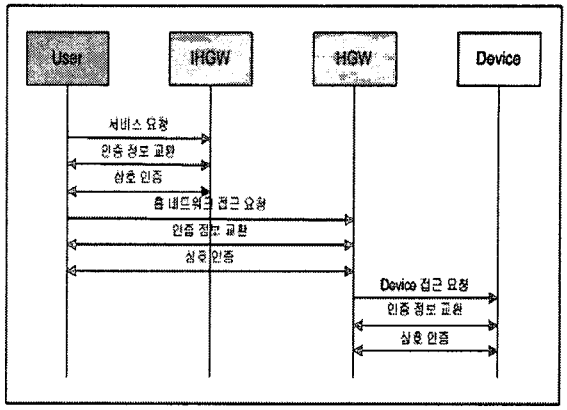
홈 네트워크에서 보안위협은 위에서 나열한 것 외에도 DoS 공격이나 Man-in-the-middle attack 등을 통한 수많은 보안 위협이 존재하고, 발생한다. 이절에서는 보안 위협에 대비한 홈 네트워크에서 여러 보안 요구사항에 대해 살펴본다.

1) 인증(Authentication)

홈 네트워크에서의 인증은 정당한 사용자인지 확인하는 사용자에 대한 인증과 기기간 통신에서 홈 네트워크를 구성하는 디바이스인지 확인하는 디바이스에 대한 인증으로 나누어 볼 수 있다. [그림 2]는 User가 외부망에 있는 경우 Device에 접근하기 위한 인증 구조적 기능 에 대해 보여 준다. 외부망에 있는 사용자가 디바이스에 접근하기 위해서는 User-IHGW, User-HGW, HGW-Device 간 최소 3번의 상호 인증과정이 필요하다.

2) 권한 위임(Delegation)

홈 네트워크 환경에서 인증의 구조적 기능을 살펴보면 User는 HGW와 상호 인증하여 성공적이면 홈 네트워크 기기제어 권한을 HGW에게 위임함을 알 수 있다. 따라서 권한



[그림 2] 홈 네트환경에서 인증의 구조적 기능

위임 기능은 상호 인증을 통해 이루어진다.

3) 권한 부여(Authority)

홈 네트워크 서비스 권한이 있는 Super User(ex-아버지)는 User(ex-아내, 자식, 손님)들에게 어느 정도 서비스를 사용할 수 있는 권한을 부여할 수 있다. 권한 부여 기능은 Super User가 HGW에 접근해서 HGW에게 권한 부여 서비스 명령을 내림으로써 이루어진다.

4) 이기종 네트워크 보안 솔루션의 연동

홈 네트워크는 이기종 네트워크들로 이루어져 있기 때문에 네트워크는 각각의 보안 솔루션을 가지고 있다. 따라서 보안 솔루션 모두는 대체 할 수 없지만 보안 솔루션의 매핑을 제공해야 한다. 이 기능은 HGW에서 수행 할 것이다.

5) 기밀성/무결성(Confidentiality, Integrity)

각 시스템을 안전하게 컨트롤하고, 공격자로부터 송수신되는 데이터에 대한 보호를 위해서 기밀성/무결성 서비스가 제공되어야 한다. 특히 무결성 서비스는 키가 있는 MAC (Message Authenticaion Code) 함수를 사용함으로써 가정내 기기 및 사용자 인증하는 역할도 한다.

4. 홈 네트워크 환경에서의 무선 보안 기술

홈 네트워크를 구성하는데 무선통신 기술은 설치하는데 유용할 뿐만 아니라 저속의 전송 속도를 요하는 센서 기술에서부터 고속의 전송 속도를 요하는 멀티미디어에 이르기 까지 많이 사용될 것이다. 그러나 무선 통신 기술은 전파를 사용하기 때문에 전파의 특성상 누구에게나 노출되어져 있다는 단점이 있다. 따라서 무선 구간에서의 보안은 매우 중요하다고 하겠다. 이절에서는 무선 기술 중 이동 통신 기술을 이용

한 홈 네트워크 환경에서의 보안 구조에 대해서 살펴본다.

4.1 이동 통신 보안 기술

3세대 이동 통신은 크게 주로 유럽에서 상용화 되는 비동기식 UMTS(3Gpp), 북남미 위주로 개발된 동기식 CDMA (3Gpp2)로 구분된다. 인증 및 키일치 메커니즘은 Millenage 알고리즘을 사용하고, 암호 알고리즘으로는 KASUMI 기반의 f8을 사용한다 [6,7].

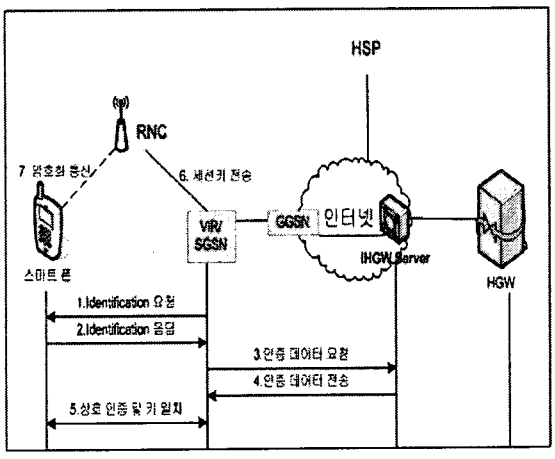
4.2 외부 이동망을 이용한 홈 네트워크의 보안 구조

이동 통신 기술과 무선랜 기술은 홈 네트워크 환경에서 서비스 사용자가 언제, 어디서나 가정내 기기를 제어하는데 중요한 역할을 한다. [그림 3]은 이동망에서 홈 네트워크에 접근하기 위한 보안 구조에 대하여 설명한다. 그림에서 알 수 있듯이 핸드폰과 HGW 사이에서 End-to-End Security를 보장하지 못한다. end-to-end Security를 보장하기 위해 어플리케이션 레벨에서의 보안 메커니즘을 제시한다.

1) 홈 네트워크 서비스 가입자인 Super User는 HGW를 제어 할 수 있기 때문에 키 갱신 주기를 정해서 대칭키 K 를 공유한다.

2) 스마트폰 -> HGW : E_K (Pnounce, r1)
: 스마트폰은 Pnounce(Phone nounce) 와 random number r1을 생성해서 대칭키를 이용해서 HGW에게 보낸후 키 갱신을 위해 K 대신 K+r1로 대체한다.

3) HGW -> 스마트폰 : E_{K+r1} (Pnounce , Hnounce , r2)
: HGW는 D_K (E_K (Pnounce, r1))을 이용하여 Pnounce와 r을 획득하고, K를 K+r1로 대체한후 K+r1을 이용하여 Pnounce와 Hnounce(HGW nounce)를 전송한다. 전송이 끝나면 세션키를 K+r1+r2로 대체 한다.



[그림 3] 이동망에서 HGW 접근 구조

4) 스마트폰 -> HGW : $E_{K+r1+r2}$ (Hnounce)
: 스마트폰은 D_{K+r1} (E_{K+r1} (Pnounce , Hnounce , r2))을 이용하여 Pnounce를 확인함으로써 HGW를 인증한다. 또한 자신이 정당한 사용자임을 확인시키기 위해 세션키를 K+r1+r2를 대체한후 Hnounce 를 보낸다. HGW는 Hnounce가 자신이 보낸 값과 같은지 확인함으로써 스마트폰을 인증한다.

5. 결 론

홈 네트워크가 실현되기 되기 위해서는 유무선 통신 기술, 이기종 네트워크를 연동하는 기술, 디바이스 제어 기술 등 다양한 기술이 필요하다. 그러나 실질적인 서비스를 제공하기 위해서는 보안 서비스가 뒷받침 되지 않으면 여러 가지 문제를 야기할 수 있다. 이에 따라 홈 네트워크에서 보안 공격 유형과, 보안 위협, 보안 요구사항을 정의 하였고, 무선 통신 기술 중 외부망에서 홈망으로 접근을 위한 이동 통신에서의 보안 메커니즘에 대해 제시하였다. 홈 네트워크 구성에서 무선 기술 특히 무선 PAN 기술은 수요자 측면이나 공급자 측면에서 많은 이점이 있는 반면에 보안에 있어 취약점이 많기 때문에 이 부분에 대한 더 많은 연구가 필요하겠다.

[참고문헌]

[1] 임승옥, 윤찬수, 정광모, " 유비쿼터스 통신 실현을 위한 홈 네트워크 프로토콜 구조", 정보처리학회지 제10권 제4호, 2003.7

[2] 박영충, 최광순, 정광모 "U-Home 시대를 향한 Digital Concergence 기반의 홈 스테이션 구조" 전자부품연구원, 2003

[3] 배창석, 이전우, 김채규, "홈서버 기술 현황 및 기술개발 방향" 정보처리학회 제8권 제1호, 2001

[4] 구필영, 박원배, 박종태 Home Network에서의 통합 Protocol Architecture에 관한 연구" 대한전자공학회 제24권 제1호, 2001

[5]최광순, 정광모 "국내외 홈 네트워킹 기술 표준화 동향 및 발전 전망" 전자부품연구원 전자정보센터, 2003

[6] 3Gpp TS 33.102 V5.1.0, "Security Architecture",

[7] 3Goo TS 23.002 V5.90, "Network architecture"

[8] IEEE 802.11i/D9.0 "Specification for Robust Security on WLAN", 2004

[9]IEEE 802.15 "Wireless Access Control(MAC) and Physical Layer(PHY) Specification for Wireless Personal Area Networks(WPANs), 2002