主題

홈네트워크 보안 관련 기술

대구가톨릭대학교 컴퓨터정보통신공학부 교수 진 용 희

차 례

1. 서 론

기간망을 위한 훌륭한 네트워크 인프라로부터 가입자 망, 홈네트워크에 이르기까지 초고속 인터넷 서비스 환경을 위한 요구가 변하고 있다. 이에 따라 정보통신부에서는 홈네트워크 산업을 신성장 동력 산업 중의 하나로 선정하였으며, 관련 산업의 집중 육성에 대한 기대가 커지고 있다.

홈네트워크는 홈 내부에 위치한 어떤 기기 간에도 네트워크가 가능하고, 원격지로부터도 네트워크를 통하여 기기의 제어 및 관리가 가능한 통신 서비스 환경을 구축하기 위한 것이다[3,7,9]. 홈네트워크 산업을 활성화하기 위하여 WAN 및 LAN 접속, 라우팅, 프로토콜 변환 기술 등이 필요하고, 또한 정보의 처리, 전달 및 저장을 안전하게 하기 위하여 특히 보안 기술이 절실히 요구된다.

이러한 요구에 따라, 국내에서도 2003년 10월에 홈네트워크 시큐리티 포럼 창립총회를 가지고 향후 추진될 중점 과제를 다음과 같이 확정한 바 있다[14].

- 홈네트워크 보안 취약점 분석
- 홈네트워크 보안 대책 및 모델 개발
- 홈네트워크 기술개발 및 표준화 로드맵 작성

홈네트워크를 구성하기 위하여 다양한 기술들이 있으며, 크게 유무선 네트워크 기술, 미들웨어 기술과 홈게이트웨이 기술 등이 있다. 이러한 홈네트워크 환경에서는 공격에 대한 가능성이 증대될 것이고, 따라서 홈네트워크 보안에 대한 연구와 제품 개발에 대한 필요성이 증대되고 있다. 본 논문에서는 이러한 새로운 환경에서의 보안 서비스 제공을 위하여 관련 표준화 기술과 동향을 알아보고, 특히 홈네트워크에서 다양한 네트워킹 토폴로지에서 서비스를 가능하게 해 줄 UPnP의 보안 기능에 대해서 기술하고자 한다.

본 고에서는 홈네트워크에 연결되어 있는 컴퓨터 자체의 보안에 대하여는 따로 기술하지 않는다. 이를 위하여 다른 자료와 그 안에 포함된 참고문헌들을 참고할 수 있다[6,12,17].

2. 관련 기술

홈네트워크 관련 기술은 크게 유선과 무선 네트워킹 기술, 미들웨어 기술, 그리고 홈게이트웨이 기술로 구분할 수 있다.

2.1 유선 네트워킹 기술

유선 홈네트워크 기술로는 IEEE 802.3 LAN 표준에 따른 네트워킹 기술로 오랫동안 사용되어 오고 있는 이더넷, 기존의 댁내 전화선로를 이용한 홈네트워크의 백본 기술로 대두되고 있는 HomePNA(Home Phoneline Network Alliance), 별도의 통신선로가 필요 없는 전력선을 이용한 PLC(Power Line Carrier), 고속의 실시간 데이터 전송을 가능하게 하는 고성능 직렬 버스를 이용한 IEEE 1394, 그리고 주변 장치와의 쉬운 연결이 장점인 USB(Universal Serial Bus) 등이 있다[5,8,21].

2.2 무선 네트워킹 기술

무선 홈네트워크 기술로는 IEEE802.11b, 802.11g, 802.11a, 802.11i 등 다양한 무선기술 표준을 가지고 있는 IEEE802.11x, RF(radio frequency)방식을 사용하여 홈 전체를 서비스 범위로 하고, SWAP(Shared Wireless Access Protocol)이라고 하는 표준 프로토콜을 가지고 있는 HomeRF, 블루투스(Bluetooth), 주로 군용 레이더나 원격 탐지 등의 특수목적으로 이용되다가 최근 가정용으로 개발되고 있는 UWB(Ultra-WideBand) 등이 있다[2,20].

2.2.1 무선 LAN 기술

무선 LAN은 크게 무선 LAN 단말과 엑세스 포인트(AP: Access Point)로 구성될 수 있다. 엑세스포인트는 여러 개의 무선 단말을 접속시켜주는 기능, 무선데이터를 유선인터넷으로 연결시켜주는 허브/브리지 역할을 수행하는 장치이다[1].

무선 LAN에서의 핵심기술로는 암호화 및 인증 기술을 포함하여, RF 전송기술, 기저대역 변복조 모뎀, 매체 접근제어(MAC: Medium Access Control) 설계 기술, AP(Access Point) 제어 소프트웨어 기술 등이 있다[2].

무선 LAN이 홈네트워크 뿐만 아니라 기업 내부망과 공중망 서비스로 확대되고 있는 이유 중의 하나는, 무선 LAN 사용자의 안전한 통신을 보장할 수 있도록 무선 LAN 보안 시스템의 보안 기술 개발이 활발하게 전개되고 있는 것이다[1].

2.2.2 무선 PAN 기술

비교적 단거리(10m 이내)에 위치하고 있는 홈네트워크 내의 기기들을 무선으로 연결하여 양방향 통신을 통한 여러 가지 응용들을 지원하기 위한 기술이다. 표준화 작업은 블루투스 SIG(Special Interest Group)와 IEEE 802.15 그룹을 통하여 진행 중이다[19].

2.2.3 UWB 기술

현재 UWB에 대한 표준화 작업은 미국에서만 진행 중이며 유럽이나 아시아에서는 미국의 진행 과정을 관심을 가지고 지켜보는 정도이다[2].

2.2.4 무선 1394 기술

IEEE 1394 유선기술은 멀티미디어 신호를 전송할 수 있는 최대 도달거리가 4.5m로 한계를 가지기 때문에, 이를 극복하기 위한 기술이 무선 1394 기술이다. 무선 1394 기술은 각 나라마다

표준이 조금씩 다른 것이 특징이다. 미국은 1394TA(Trade Association)를 중심으로 IEEE802.11aPHY와 IEEE802.11eMAC을 기반으로 1394PAL(Protocol Adaptation Layer) 및 Bridge Management & Internal Fabric(P1394.1) 규격을 만들고 있으며, 유럽에서는 BRAN(Broadband Radio Access Networks)을 중심으로 IEEE1394외에 ATM과 IP 등을 지원하는 것을 제안하였고, 일본은 5GHz와 60 GHz 두 가지 방식을 사용하는 것으로 진행되고 있다.

2.3 미들웨어 기술

2.3.1 UPnP(Universal Plug and Play)

UPnP는 마이크로소프트사가 제안하였으며, 특정 운영체제, 프로그래밍 언어, 매체와는 관계없이 IP, TCP, UDP, HTTP, XML과 같은 기존의 프로토콜을 이용하여 홈 네트워크 기기 간에 제어와 명령을 가능하게 한다. 홈네트워크 기기들을 피어 대 피어 방식으로 연결시켜 주는 미들웨어 구조로써, 기기 사이의 정보는 XML로 표현되며, HTTP 프로토콜을 이용하여 통신한다[8].

1999년 10월에 가전, 컴퓨터, 가정 자동화, 모바일 디바이스 등 업체를 중심으로 설립된 UPnP 포럼은 산하에 여러 개의 작업 위원회를 가지고 있는데, UPnP 디바이스 구조를 위한 보안 솔루션을 정의하기위한 보안 작업 위원회가 있다. 이 위원회에서는 모든 UPnP 디바이스에 적용될 접근제어(access control)를 다룬다. 이 위원회에서 다루고 있는 세 가지의 주요 사항은 다음과 같다[11].

- 장치 보안(device security) 서비스: 접근 제어 설정을 허용하기 위하여 신뢰 장치가 구현해야 할 조치사항들을 정의한다.
- 보안 콘솔(security console) 서비스: 다른 장치에 대한 보안을 설정하는 장치가 구현할 서비스를 정의한다.
- 신뢰 장치(secure device): 승인된 제어점에게만 실제 ID와 특성을 보여주는 일반적인 장치 형태로 사용되는 장치의 정의.

2.3.2 기타 기술

IEEE1394 기술을 채택하여 AV 기기간의 실시간 데이터 전송과 상호 호환성을 목표로 하는, Sony가 제안한 위한 미들웨어 기술인 HAVi(Home Audio Video interoperability) 그리고 LAN, xDSL, 전력선, 모뎀, 무선 등 다양한 통신 방식으로 접속된 가정 내 디지털 장비나 소프트웨어를 동적으로 상호 작용하도록 하는, Sun Micro systems 사가 제안한 Java 기반의 Jini가 있다.

2.4 게이트웨이 기술

홈네트워크 구현에서 가장 중요한 요소기술 중의 하나이다. 홈게이트웨이는 여러 가지 유무선 홈네트워크 기술 중에서 한개 이상의 홈네트워킹 기술과 xDSL, 케이블, 혹은 광전송 장치들 중에서 한 개 이상의 액세스망 기술을 상호 접속하거나 중계하기 위하여, 모뎀, 라우터와 스위치 기능을 통합시켜 놓은 장치이다. 외부와의 통신을 가능하게 하는 라우터 기능, 개별 홈네트워크 기술 간의 차이를 해결하기 위하여 필요한 프로토콜 변환 기능, 외부 네트워크와의 트래픽 분리를 통한 보안 기능, 홈오토메이션 기능 등을 수행할 수 있어야 한다[8].

표준화 단체로는 ISO/IEC 산하 JTC1의 SC25 WG1, OSGi(Open Services Gateway initiative)와 UPnP 포럼이 있다. 국내에서도 2000년 7월에 산학연 전문가들이 홈게이트웨이 표준화 전략 수립을 위한 워크숍을 개최한 이후, 기술 개발과 아울러 표준화 작업이 진행되고 있으며, 2001년 12월 홈게이트웨이 정보통신 표준안이 제정된 바 있다[4].

UPnP의 인터넷 게이트웨이 작업 위원회는 인터넷 게이트웨이 1.0 표준을 완성하였고, 2.0 표준화 작업을 진행 중이다. UPnP 인터넷 게이트웨이에 포함될 새로운 기능 중에서 보안 관련 기능은 다음과 같다[11,23]: TCP, UDP 외의 프로토콜 지원을 위한 NAT 정의 개선, 방화벽 기능 지원, VPN 설정 지원, UPnP 보안 서비스 지원, 대역폭 관리 및 QoS 지원.

홈게이트웨이는 기존의 모뎀형태의 가장 간단한 형태로부터 음성, 영상 및 데이터의 통합 서비스를 제공할 수 있는 지능형 홈게이트웨이로 진화될 전망이다.

3. 보안 요소 및 요구사항

3.1 보안 요소

홈네트워크 보안을 위하여 다음과 같은 일반적인 보안 요소를 열거 할 수 있다[13,16].

- 데이터 기원 인증: 메시지를 인증하기 위하여, 특정한 소스로부터 왔다는 것을 확립하여야 한다. 점검값을 이용한 관용 암호화와 디지털 서명을 이용한 공개키 방법이 사용될 수 있다.
- 명령 권한 검증: 어떤 사용자가 어떤 일을 수행하기 위한 명령에 대하여 정당한 권한이 있는지를 검정하는 것이다.
- 메시지 무결성 보호: 입력 메시지에 대하여 정당하지 않은 데이터의 변경이 없음을 보증하는 기능이며, 보통 인증과 관련된다.
- 메시지 재생 방지: 임의의 메시지를 공격자가 중간에서 가로채서 나중에 재사용하는 것을 방지하는 것이다.
- 데이터 비밀성: 메시지의 내용을 암호화함으로써 보통 이루어진다.
- 키 분배: 완전한 보안 혜택을 위하여 키 분배과정이 조심스럽게 설계되어야 한다.

3.2 홈네트워크 보안 요구사항

[13]에서는 홈의 정의에 따라서 다른 보안 요구사항을 제시하고 있다. 우리나라에서도 원룸, 투룸, 핵가족, 대가족, 공동 주택 등 다양한 주거 형태에 따라서 비슷한 요구사항이 적용될 수도 있을 것 같다.

여러 가지 보안 요소 중에서 홈네트워크 장치는 다음과 같은 두 가지 문제에 대하여 특히 관심을 가질 필요가 있다.

- 권한 검증(authorization): 각 장치에서 무슨 조치를 취하고 데이터를 접근하기 위하여 어떤 것이 허용되는가?
- 기밀성(confidentiality): 어떤 것이 장치로 전달되는 메시지를 읽도록 허용되는가?

여기서 어떤 것은 특정한 사람에 의하여 운영되는 네트워크 장치나 애플리케이션일 수 있다. UPnP는 이런 것들을 제어점(CP: Control Points)이라고 한다.

보안 도메인(security domain)과 정책(policy)도 결정되어야 한다. 여기서 보안 도메인은 서로 간에 상호작용이 허용되는 객체들의 집합으로 정의할 수 있다. 특정 개인키에 대한 접근권한을 가지고 있고 특정인에 의하여만 수행되는 애플리케이션으로 네트워크 상에서 대표되지만, 사람도 하나의 객체에 속한다. 보안 정책은 보안 도메인 내의 객체들이 상호작용이 허용되는 방법에 대한 명세이다. 도메인 내의 객체들은 모두 네트워크로 연결되어 있으나, 그러나 모두가 네트워크 컴포넌트는 아니다. 예를 들어, 네트워크 홈 경보 시스템이 단지 한 사람에 의하여만 접근될 수 있는 가족 PC 상의 특정 제어 애플리케이션을 가

진 보안 도메인 내에 있을 수 있다. 이 경우에는 그 PC 상의 다른 사용자나 애플리케이션은 접근이 허용되지 않는다. 다른 예로 단일 거주자 홈의 PC가 재정 파일 디렉터리를 가지고 있다고 가정하자. 이 파일은 홈 소유주 뿐 만 아니라 인터넷을 통하여 홈 소유주의 세무 회계사에 의하여 접근될 수 있다. 이 경우, 해당 특정 디렉터리, 회계사의 애플리케이션 및 홈 소유주의 어떤 애플리케이션을 포함하는 보안 도메인이 정의될 필요가 있다. 이와 같이, 보안 도메인의 사실상의 명세는 보호되는 자원의 소유주에 달려있다. 따라서 홈네트워크 제품 설계자나 연구자들은 이런 도메인들이 네트워크 노드보다 훨씬 더 세밀한 객체를 포함할 것이며, 자원 소유주가 파일 폴더를 정의하는 것처럼 많은 보안 도메인을 정의할 수 있다는 것을 알 필요가 있다[13].

4. UPnP 보안

4.1 배경

UPnP에서는 세리모니(ceremony)란 용어를 사용하는데, 이 용어는 인텔의 Jesse Walker에 의하여 만들어졌다. 네트워크 프로토콜과 같은 것을 의미하는데, 네트워크 프로토콜은 컴퓨터나 일반적인 네트워크 노드사이의 메시지를 의미한다. 반면에 세리모니는 컴퓨터, 사람과 아마도 환경사이의 메시지를 의미한다. 세리모니는 UPnP 보안 프로토콜과 같은 보안 프로토콜을 위하여 제일 먼저 만들어졌다. 이것은 모든 보안 프로토콜이 인간 상호작용을 필요로 하기 때문이다. 보안 프로토콜에서는 보안 정책(security policy)이란 데이터에 기초하여 네트워크 노드에서 결정이 만들어 진다. 정책은 인간으로부터 네트워크 노드로 통신되어야 한다. 그러므로 보안 정책을 기술하는 보안 프로토콜의 적어도 일부는 인간이 필수적인 컴포넌트이다. UPnP 보안에서 프로토콜뿐만 아니라, 완벽한 세리모니를 설계하고 분석하기 위한 노력이 있었다[23].

UPnP V.1의 기본 구조는 제어점(CP: control point)과 장치(device)로 구성되며, 컴포넌트들이 서로 상호 작용하기 위하여 세 가지의 프로토콜을 사용한다.

- SOAP(Simple Object Access Protocol): CP에서 장치로 원격 절차 호출(RPC: remote procedure call)을 위해서 필요하다.
- SSDP(Simple Service Discovery Protocol): 장치의 발견을 위한 방송 프로토콜이다.
- GENA(General Event Notification Architecture): 이벤트 보고서와 이벤트 출판물에 대한 구독을 위해서 필요하다.

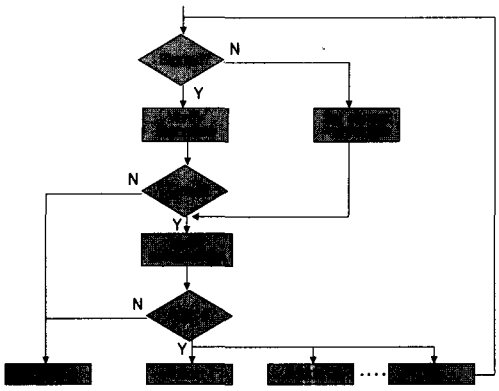
4.2 보안 모델

장치는 발견(discovery) 프로토콜을 통하여 자신을 광고하며 제어점이 호출하는 SOAP 행동의 집합체인 서비스를 제공한다. UPnP 보안은 SOAP 제어 메시지와 응답을 안전하게 한다. 이 메시지 보안은 다음과 같이 구성되어 있다:

- 신원(identification)
- 무결성(integrity)
- 인증(authentication)
- freshness
- 권한 검증(authorization)
- 비밀성(secrecy)

제어 메시지 보안이 그림 1의 흐름도에서 보여준다.

메시지의 송신자는 자신의 공개키 해시인 보안 ID에 의하여 식별된다. 메시지가 공개키 방법으로 서명된다면, 키 정보 필드에서 제공된 공개



DAE: Decrypt And Execute

그림 1. 메시지 보안 흐름도

키에 기초한 해시를 계산한다. 제어 메시지 보안 흐름은 다음과 같다.

1) 메시지가 도착되어 해석(parse)된다. 서명 여부를 판별한다.
2) 메시지가 서명되었다면 장치는 서명과 freshness를 검증한다. 서명의 검증은 메시의 무결성과 기원 인증 둘 다를 보증한다. 송신자는 자신의 공개키의 SHA-1 해시인 보안ID에 의하여 표시된다. freshness는 재생 공격을 방지하기 위한 것으로, 어떤 순서 번호나 시간 값으로 표시된다. 보안 ID는 모든 컴포넌트에서 유일하다.
3) 만약 서명과 freshness가 유효하다면, 소유주는 메시지 서명자의 보안ID에 설정된다. 그렇지 않은 경우, 메시지가 실패되고 에러 메시지가 생성된다.
4) 메시지가 권한 검증을 위하여 시험된다면, 권한 검증 정보가 수집된다. 이것은 소유자 목록, ACL(Access Control List), 캐시된 인증서, 메시지에서 제공되는 인증서로 구성된다.
5) 만약 송신자가 권한 검증되지 않으면, 메시지는 실패되고 에러 메시지가 생성된다.
6) 만약 요구되는 행동이 DAE라면, 암호문 인수(argument)가 복호되고 결과적인 평문이 처리를 위하여 처리과정의 처음으로 순환적으로 돌려 보내진다.

4.2.1 보안 정책 데이터

보안 정책 데이터는 다음을 포함 한다:

- 장치의 소유주 목록
- 장치의 ACL
- 캐시된 인증서
- 메시지의 일부로 송신자에 의하여 제공된 인증서

보안 정책 데이터는 장치 소유주(device owner)라고 언급된 인간의 마음에서 기원한다. 이 데이터는 그림 1의 보안 결정 시에 장치 내에 상주해야 한다. 그러므로 소유주로부터 장치에 통신되어야 한다. 통신을 이루기 위하여, UPnP 보안은 다음 두 가지를 정의한다.

- 장치보안 서비스: 데이터의 설정을 허락하기 위한 행동을 기술한다.
- 보안 콘솔(SC: Security Console): UPnP 장치이며 동시에 제어점인 컴포넌트로, 어떤 장치의 인간 소유주를 위한 사용자 인터페이스를 제공한다.

소유주는 SC 공개키의 해시에 의하여 표시된다. 소유주 목록은 이러한 해시 값들의 목록이다. 장치 ACL은 다음을 기술하는 항목들의 목록이다.

- 주체(subject): 보안 ID 혹은 보안ID 그룹의 이름- 이 ACL 항목에 의하여 권리가 부여되는 CP 혹은 SC를 나타낸다.
- 권한 검증: 이 항목에 의하여 주체에게 무엇이 부여되는가를 기술하는 허락 요소의 목록

- 위임 불가능(May-not-delegate): 주체가 이 항목에서 부여된 어떤 권한도 다른 CP, SC 혹은 그룹에게 위임할 수 없다는 것을 나타내는 선택적 플래그
- 유효성(validity): 항목의 유효성 기간을 제한하는 시작일자/시간과 종료일자/시간을 포함할 수 있는 선택적 요소의 집합

UPnP 보안에서는 두 가지 종류의 정의된 인증서가 있다: 지명된 그룹(named group) 멤버십 인증서와 권한검증(authorization) 인증서.

지명된 그룹 멤버십 인증서는 다음 항목을 포함한다.

- 발행자(issuer): 발행 SC의 보안ID
- 이름: 그룹의 원문 이름
- 주체: 보안ID 혹은 이 그룹에서 멤버십이 주어지는 개인키 혹은 그룹키의 이름
- 유효성: 시작일자/시간과 종료일자/시간, 갱신 요소를 포함할 수 있는 선택적 요소의 목록

권한검증 인증서는 ACL 항목과 같은 요소뿐만 아니라, 발행자 필드와 지명된 그룹 인증서처럼 모든 동일한 유효성 옵션을 가지고 있다.

4.3 신뢰 컴포넌트 발견

CP나 SC에게 어떤 장치 상의 권한을 부여하기 위하여, 그런 컴포넌트들이 먼저 장치 소유주의 SC에 의하여 발견되어야 한다. UPnP 발견은 대칭적이지 않다. 즉, 제어점이 장치를 발견하나, 반대의 경우는 없다. 그러나 UPnP 보안은 장치와 제어점 둘 다를 발견할 필요가 있다.

4.3.1 신뢰 장치 발견

신뢰 장치는 정상적인 UPnP 방법으로 발견될 수 있다. 신뢰 장치는 장치보안 서비스를 포함하기 때문에 비신뢰 장치와 구분된다. 그러나 SSDP를 통한 정규적인 발견 과정은 안전하지 못하다. 발견 과정을 안전하게 하기 위하여, 그림 2에서 보여주는 것과 같은 세리모니가 있다.

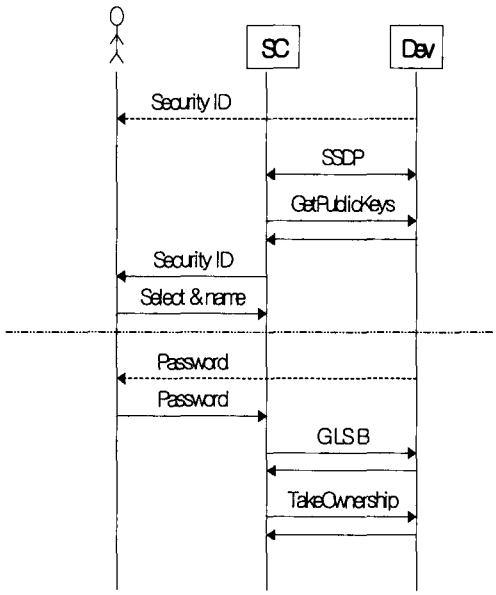


그림 2. 장치 발견 세리모니와 소유권취득

보안-가능 장치의 발견은 UPnP의 SSDP에 의하여 수행되는 기본적인 발견 이상의 절차가 필요하다. 이 발견 과정의 목적은 사용자의 SC가 정확한 장치와 연계하고 사용자 네트워크의 각 장치가 정확한 SC와 연계하도록 하는 것을 보장하기 위한 것이다. 그림 2에서의 안전한 발견 과정은 다음과 같다.

1) 사용자가 장치로부터 목표 장치(target device) 보안ID를 읽는다.
2) SC는 SSDP를 통하여 목표 장치를 발견한다.
3) 장치보안을 제공하는 각 장치를 위하여, SC는 GetPublicKeys에 대한 호(call)로 장치 공개키를 얻는다.
4) SC는 공개키로부터 각 장치의 보안ID를 계산하여 사용자에게 전시한다. 이것은 단계

1에서 얻은 보안ID와 비교하기 위하여 사용된다.

5) 사용자는 이용가능한 장치 목록으로부터 목표 장치를 선택하여 명명한다.

보안-인식(security-aware) 장치를 발견하고 명명하는 이외에, 사용자가 만약 그 장치의 보안 소유권을 갖기를 원한다면, 추가적인 절차가 필요하다.

6) 사용자는 장치로부터 목표 장치의 초기 패스워드를 읽는다.

7) 사용자는 그 패스워드를 SC에게 제공하며, SC는 이것을 소유권취득(TakeOwnership) 호를 위하여 필요한 값을 계산하기 위하여 사용한다.

8) SC는 소유권취득 호를 위한 인수를 계산하는데 사용할 현재 LifetimeSequenceBase(LSB) 값을 얻기 위하여 GLSB(GetLSB) 호를 실행한다.

9) SC는 소유권취득 호를 실행한다.

4.3.2 신뢰 CP 혹은 SC의 발견

그림 3은 CP와 SC 노드의 발견 과정을 보여준다.

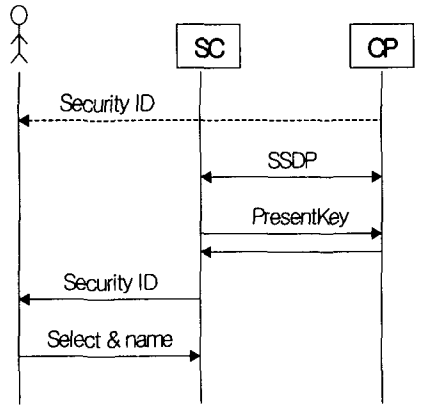


그림 3. CP와 SC 노드의 발견

그림 3의 과정은 다음과 같다.

1) 사용자는 목표 CP나 SC로부터 보안ID를 읽는다.

2) CP는 SSDP를 통하여 사용자의 SC를 발견한다.

3) CP는 PresentKey 행동을 통하여 자신이 찾은 자신의 공개키를 모든 SC에게 제공한다.

4) SC는 CP의 공개키로부터 보안ID를 계산하여 사용자를 위하여 전시한다.

5) 사용자는 단계 1에서 얻은 것과 SC에 의하여 계산된 보안ID를 비교하여 적절한 CP를 선택하여 명명한다.

4.4 소유권

만약 SC의 공개키가 장치의 소유주 목록에 열거된다면 SC가 장치를 소유(own)한다고 말한다. 한 장치를 소유하는 SC는 소유주 목록과 장치의 ACL을 조작하는 것을 포함하여 그 장치 상에 모든 것을 할 수 있도록 허용된다. 장치보안은 장치의 소유주 목록의 조작을 허용하는 다음과 같은 다섯 가지 행동을 정의 한다:

- 소유권취득(TakeOwnership)
- 소유자열거(ListOwners)
- 소유권부여(GrantOwnership)
- 소유권취소(RevokeOwnership)
- FactorySecurityReset

4.4.1 소유권 취득

소유권취득은 장치가 소유되어 있지 않은 경우에만 가능하다. 디폴트 소유권취득 과정은 그림 2에서 기술된 바와 같다. 그림 4는 UPnP의 일부로 표준화되지 않은 더욱 편리한 소유권 취득 방법을 보여준다. 이 방법은 제조사가 여분의 하드웨어 제공을 원할 경우이다. 예를 들어, 장치와 SC 모두가 USB 커넥터를 가질 경우, 그림 4

에서 보여주는 바와 같이, 이 기능을 위한 전용 점대점 케이블 상으로 소유권취득이 일어날 수 있다. 이 방법의 보안은 케이블이 두 개체-장치와 SC-를 연결하는 것에 의존한다.

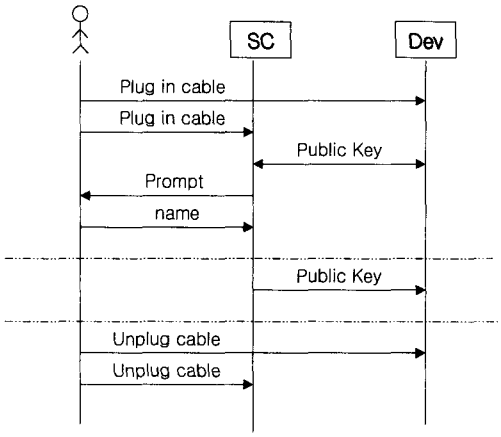


그림 4. 사설 케이블을 통한 소유권 취득

4.4.2 소유자열거

소유자열거 행동은 사용자의 클라이언트와 에이전트로써 SC에 의하여 호출된다. 그림 5에서 그 플로우를 보여주며 열거되는 장치의 소유주는 그림 2에서 보여준 것과 같이, 발견되고 명명되어, 사용자에게 이미 알려져 있다고 가정한다.

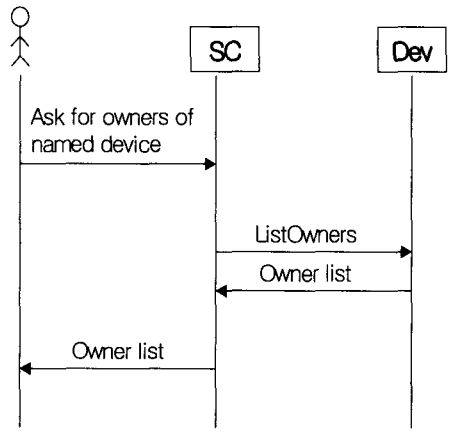


그림 5. 소유자열거

4.4.3 소유권부여

사용자의 SC가 소유주인 SC와 목표 장치를 명명하고 나서, 사용자는 소유권부여를 위하여 그 SC와 장치를 선택하고 사용자의 SC는 소유권부여 행동을 수행한다. 그림 6에서 소유권부여 절차를 보여준다.

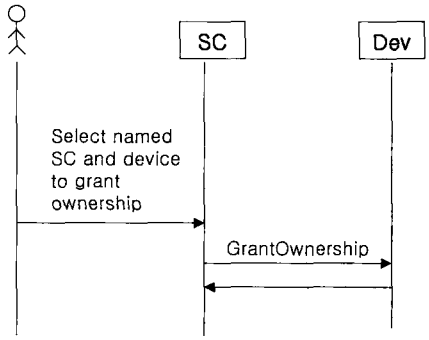


그림 6. 소유권부여

4.4.4 소유권 취소

사용자의 SC가 소유권을 가지고 있는 장치의 소유주 목록의 전시로부터, 사용자는 소유권이 취소될 SC를 선택한다. 이 SC는 이름이나 보안 ID에 의하여 열거될 수 있다. 소유권취소 행동은 사용자의 SC가 자신의 소유권을 취소하도록 허용하지는 않는다(그림 7 참조).

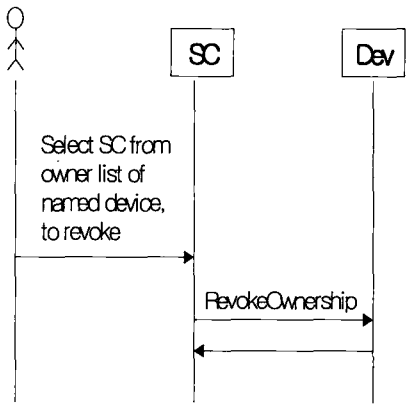


그림 7. 소유권취소

FactorySecurityReset은 장치의 소유주에 의하여만 수행될 수 있다. 모든 보안 정책을 지우고 장치를 비소유 상태로 돌려준다.

4.5 세션 키

소유권취득과 세션키 설정을 제외하고, 장치 상에서 모든 안전한 행동을 위하여, SC나 CP는 세션키가 필요하다. 세션키는 그림 8에서 보여주는 프로토콜로 얻어진다.

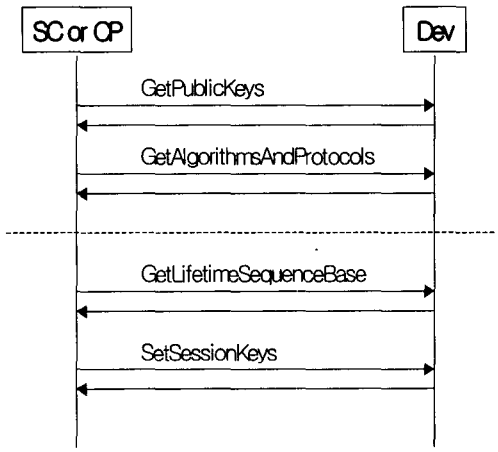


그림 8. 세션키 설정

세션키 설정을 위한 프로토콜은 4 단계로 이루어진다. 처음 두 단계는 비교적 일정한 데이터를 수집하며 캐시 될 수 있다.

1) CP는 장치의 공개키를 얻는다.
2) CP는 장치의 지원되는 알고리즘과 프로토콜의 목록을 얻는다.
3) CP는 장치의 LSB를 얻는다. 이 값은 장치의 수명동안 변경되며 어떤 공개-키-인증 행동(소유권취득과 세션키 설정)을 위한 freshness를 제공하기 위하여 사용된다.
4) CP는 사용하고자 하는 세션키를 생성하여 세션키설정(SetSessionKeys) 행동 호에서, 해당 장치의 공개키를 사용하여 암호화하여 그 장치로 보낸다.

4.6 ACL 편집

보안 소유권의 주 목적은 누가 장치의 ACL을 편집(edit)하는 것이 허용되는지를 확립하기 위한 것이다. ACL은 장치 보안 정책의 근본이며 인간 사용자에 의하여 확립되어야 한다. 소유주 목록은 특별한 경우의 ACL로 볼 수 있다. 보통의 ACL은 선택된 CP, SC나 지명된 그들의 그룹에게 대표적으로 전체 허락이 아닌, 장치 상에 어떤 집합의 허락을 부여한다. ACL 편집은 사용자-주도 동작이기 때문에 완전한 세리모니를 기술할 수가 없다. 그림 9는 한 포함된 세션이 발생할 수 있는 표본을 보여준다. 이 세리모니는 SC가 장치와 이미 세션키를 확립하였다고 가정한다. 또한 사용자가 이 장치 상에 액세스를 허용하고자 하는 모든 CP나 SC를 명명하였고 어떤 명명된 CP나 SC 그룹이 이미 생성되었다고 가정한다. 그림 9는 ACL 편집 과정을 보여준다.

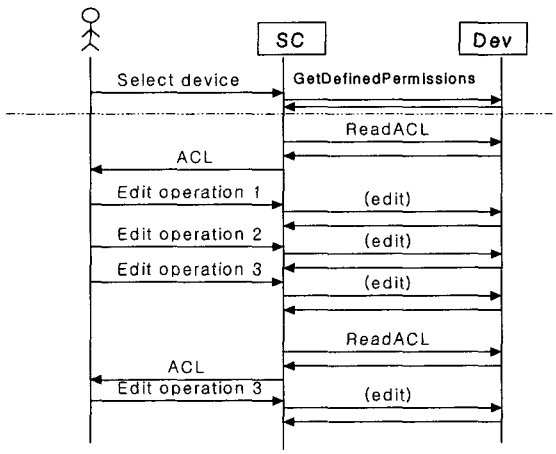


그림 9. ACL 편집

그림 9의 단계를 간략히 기술하면 아래와 같다.

1) 이 세션은 사용자가 이름에 의하여 장치를

선택하면서 시작한다. 선택된 장치는 이 SC가 이미 소유하고 있는 것이어야 한다.

2) SC는 장치에게 정의된 허락(permission)의 집합에 대하여 질문한다. 이 정보는 캐시가 가능하여, 매번 SC가 질문할 필요가 없다.
3) SC는 장치의 ACL을 읽어야 한다.
4) SC는 사용자에게 ACL을 제시한다.
5) 사용자는 편집 동작 (1)을 수행한다.
6) SC는 다음의 편집 행동의 하나를 통하여 편집 동작을 수행한다: WriteACL, DeleteACLEntry, ReplaceACLEntry, AddACLEntry.
7) 사용자는 두 번째 편집 동작 (2)를 수행한다.
8) SC가 그것을 수행한다.
9) 사용자는 세 번째 편집 동작 (3)을 수행한다.
10) SC가 그것을 수행하고자 시도하나, ACL 버전이 오래되었다는 에러 메시지를 얻는다.
11) SC는 ACL을 다시 읽는다.
12) SC는 사용자에게 갱신된 ACL을 제시한다.
13) 사용자는 다시 세 번째 편집 동작을 수행한다.
14) SC가 세 번째 편집 동작을 수행한다.

4.7 인증서 캐싱

UPnP 보안에서 인증서는 두 가지 목적이 있다: 첫째는 제어점의 지명된 그룹을 정의하는 것이고, 두 번째는 ACL을 편집하는 것이 가능하지 않을 때 어떤 CP, SC 혹은 명명된 그룹에게 권한검증을 부여하는 것이다. 편집이 가능하지 않은 이유로는, 신규 항목을 위하여 ACL에 공간이 거의 없거나, SC가 ACL을 편집하기 위한 허락이 없는 경우이다. 인증서는 장치에 캐시될 수 있다. 만일 인증서가 메시지 안이나 캐싱에 의하여 CP로부터 전달된다면, CP는 그것을 생성한 SC로부터 얻어야 한다. CP가 인증서 캐시 행동을 제공할 수 없기 때문에, CP가 SC로부터 인증서를 가져온다.

〈표 1〉 무선 LAN 보안 요소별 표준화 단체

번호	보안 요소	표준화 단체
1	사용자 인증 (authentication)	- IEEE 802.1X, IEEE 802.1aa 태스크 그룹 - IETF EAP(Extensible Authentication Protocol), IETF AAA(Authentication, Authorization and Accounting) 워킹 그룹
2	접근제어 (access control)	
3	권한 검증 (authorization)	
4	데이터 기밀성 (privacy)	- IEEE 802.11i 태스크 그룹
5	데이터 무결성 (integrity)	
6	부인방지 (non-repudiation)	
7	안전한 hand-off	- IEEE 802.11i, IEEE 802.11f 태스크 그룹 - IETF Seamoby, IETF MobileIP 워킹 그룹

5. 기타 보안 기술 동향

5.1 무선 LAN 보안기술 동향

2.2절에서 홈네트워크를 구성하는 무선기술로 무선 LAN 기술, 무선 PAN 기술, UWB 기술, 무선 1394 기술 등이 있다고 기술하였다. 본 절에서는 이 중에서 무선 LAN 보안 보안기술 동향에 대하여 기술한다[1]. 무선 LAN의 보안요소별 표준화 단체는 표 1과 같다.

무선 LAN 보안기술의 진화동향을 요약하여 기술하면 표 2와 같다.

5.2 홈게이트웨이 보안기술 동향

홈게이트웨이 표준에서 소프트웨어 프로토콜은 브리징 기능, 라우팅 프로토콜, 망관리 프로토콜, 방화벽 기능 등에 대한 기준을 제시한다. 다음에서 표준화 단체들이 추진하고 있는 보안 관련 활동들을 살펴본다[4].

(1) OSGi

OSGi는 해외에서 Sun, IBM, Oracle, Ericsson, Toshiba 등과 국내의 삼성전자와 ETRI 등이 참여하여 활동하고 있는 단체이다. 워킹 그룹(WG)을 포함하고 있는 전문가 그룹에서 공개키 암호화의 기능과 특징에 대하여 연구를 진행하고 있다[22].

(2) CableHome

CableHome은 북미와 남미의 케이블 회사들로 구성된 CableLabs가 추진 중인 표준이며, 케이블 기반의 서비스를 홈네트워크 환경으로 확장하는

〈표 2〉 무선 LAN 보안기술 진화동향

단계	단 계 명	특 징
1	비 보안	보안 기능 없음
2	WEP(Wired Equivalent Privacy) 보안	- 무선 단말과 액세스 포인트가 WEP 키를 공유하여 공유키 인증방식과 WEP 암호화 기능을 수행 - <표 1>의 보안 요소 1,2,4 기능 지원 - 공중망 서비스에서 개별 사용자 보호 미비 - 데이터 오버헤드로 인한 전송속도의 저하
3	IEEE 802.1X 보안	- 인증 서버가 사용자 인증 수행 - <표 1>의 보안 요소 중 1,2,3 만족 - 무선 LAN 공중망 서비스를 위한 기초적인 보안
4	동적 WEP 보안	- <표 1>의 보안 요소 중 1-4 지원 - 악의적인 공격자가 합법적인 사용자로 위장 불가 - 향후 가정망, 기업망, 공중 액세스망 등에서 이용 가능
5	WPA(Wi-Fi Protected Access) 보안	- <표 1>의 보안 요소 중 1-5 지원 - 무선 데이터 보호 및 무결성 지원 - 향후 홈네트워킹에서 사용 가능
6	RSN(Robust Security Network) 보안	- <표 1>의 보안 요수 중 1-5 지원 - 5단계보다 강한 암호알고리즘 사용 - 암호 알고리즘 처리 모듈의 하드웨어 구현
7	이동 보안	- <표 1>의 보안 요소 중 1-5, 7 지원
8	무선 네트워크 보안	- 무선 LAN 보안기술의 최종 목표 - 글로벌 로밍 서비스 포함

것이 목적이다. 2002년 4월에 발표된 CableHome1.0 사양은 크게 관리 및 공급(provisioning) 기능, 주소기법(addressing)과 패킷 처리 기능, 서비스 품질(QoS: Quality of Service) 기능, 보안 기능으로 나눌 수 있다.

이 중에서 보안 기능은 아래와 같은 기능들을 포함한다[18].

- 홈게이트웨이 장치 인증 기능
- 암호화된 홈게이트웨이 관리 메시지 기능
- 설계 정보와 소프트웨어 파일을 위한 암호화된 다운로드 기능
- HFC 링크상의 암호화된 QoS 기능
- 원격 홈게이트웨이 방화벽 관리 기능

(3) TIA TR-41.5

다른 종류의 WAN과 홈 LAN 기술들 간의 인터페이스를 위한 물리계층의 사양을 만들기 위하여, 멀티미디어 서비스 분배를 위한 표준을 만들기 위한 것이 북미에서 설립된 TIA(Telecommunication Industry Association) TR-41.5의 목표이다. 산하 RG(Residential Gateway) 그룹에서는 표준 홈 게이트웨이 구조의 기초가 될 설계 원칙을 정하고 권고안을 만든 바 있다.

(4) ISO/IEC JTC1 SC25 WG1

ISO 산하에서 운영되고 있는 표준 단체로 홈게이트웨이의 명세 및 요구사항을 정의하는 작업을 하고 있다. 여기서 다루는 홈게이트웨이를 홈게이트(Home Gate)라고 하며, 홈게이트가 가져야 할 기능 중에서, 프로토콜 변환, 방화벽 등을 포함하고 있다. WG1에 의하여 정의된 홈게이트웨이의 구성 요소는 WGI(WAN Gateway Interface), HGIP(HomeGate Internal Protocol) 혹은 RGIP(Residential Gateway Internal Protocol) 및 LGI(LAN Gateway Interface)가 있는데, HGIP에서 보안 정책들에 대한 기능을 가진다.

6. 맺음말

홈네트워크의 한 가지 중요한 목표는 사용자가 쉽게 사용할 수 있어야 한다는 것인데, 이런 측면에서 하부의 다양한 네트워킹 토폴로지에 따른 네트워크 설정이나 관리를 할 필요가 없고, 쉽게 기기를 홈네트워크에 연결하고 서비스 받을 수 있도록 하는 UPnP 기술의 개발이 가속화 될 것으로 판단된다. 국내의 보안업체에서도 홈네트워크 환경에서 홈네트워크를 제어하는 미들웨어의 표준 프로토콜인 UPnP와 연동해 인터넷 가전제품을 쉽게 연결할 수 있는 제품을 개발한 바 있고, 앞으로 UPnP를 지원하는 제품 개발이 더욱 활발해질 전망이다[15].

현재로선 IEEE1394 프로토콜을 이용한 유선 기술이 주도적으로 개발되고 있으나, 향후 이동 단말기기의 확산에 따라 무선 홈네트워크 솔루션의 적용이 확대될 것이 예상되므로 무선 홈네트워크 보안기술의 개발이 중요하다고 여겨진다[10].

그러므로 기존 유선 네트워크에서 사용되고 있는 다양한 보안 기능인 방화벽, 침입탐지, 서비스 거부(DOS: Denial of Service) 공격 방어 등과 같은 기능들을 통합하여, 향후 무선 기반 기술의 보급에 따라서 무선 사용자에게 제공할 수 있도록 하는 방안 연구가 필요하다.

참 고 문 헌

[1] 강유성, 오경희, 정병호, "무선랜 보안기술의 진화동향 및 전망", 전자통신동향분석 제 18권 제 4호, pp36-46, 2003년 8월.

[2] 박봉혁, 이재호, "무선 홈네트워크 기술", 주간기술동향 통권 1089호, 2003년 4월 1일.

[3] 박석지, 유종현, "u-센서 네트워크 산업의 개념과 발전동향", 주간기술동향 통권 1135호, 2004년 3월 3일.

[4] 박천교, "홈게이트웨이 기술 및 시장동향", 주간기술동향 통권 1114호, 2003년 9월 23일.

[5] 송석일, "홈 네트워크 표준화 기술 동향", 전자통신동향분석 제 15권 제 6호, pp.56-64, 2000년 12월.

[6] 윤봉환, 홈네트워크를 위한 보안설정, http://www.linuxlab.co.kr/docs/11-5.htm

[7] 이석준, 원유재, "무선인터넷 보안기술의 동향과 향후 전망", 주간기술동향 통권 963호, 2000년 9월 14일.

[8] 이윤철, "최근의 홈 네트워크 기술동향 및 시장 전망", 주간기술동향 통권 1098호, 2003년 6월 3일.

[9] 이준석, 김서균, 오경석, "PC 기반 홈네트워킹 정보단말 기술동향", 주간기술동향 통권 1091호, 2003년 4월 15일.

[10] 조병선, 하영욱, "홈네트워킹 주요 사업자 분석 및 향후 전망", 전자통신동향분석 제 19권 제 1호, pp94-108, 2004년 2월.

[11] 조충래, 박광로, "UPnP 기술 표준화 현황", 주간기술동향 통권 1075호, 2002년 12월 3일.

[12] CERT Coordination Center, Home Network Security, http://www.cert.org/tech_tips/home_networks.html

[13] Carl M. Ellison, "Home Network Security", Intel Technology Journal, Vol. 6, Issue 4, pp.37-48, Nov. 2002.

[14] http://www.hackersnews.org/data/2003/10_1/1028_34.html

[15] http://www.itdata.co.kr/column/200110/dailynews/daily_security.htm

[16] Lakshman Krishnamurthy et al., "Meeting the Demands of the Digital Home with High-Speed Multi-Hop Wireless Networks", Intel Technology Journal, Vol. 6, Issue 4, pp.57-68, Nov. 2002.

[17] Aaron Lowe, Computer Security at Home, April 22, 2003, http://www.aarondlowe.com/Computer_Security_at_Home.htm

[18] http://www.cablelabs.com

[19] http://www.homepna.org

[20] http://www.homerf.org

[21] http://www.ieee1394.org

[22] http://www.osgi.org

[23] UPnP Security Ceremonies Version 1.0, October, 2003, http://www.upnp.org

전 용 희

1971. 3~1978.2 고려대학교 전기공학과
1985. 8~1987.8 미국 플로리다공대 대학원 컴퓨터공학과
1987.8~1992.12 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사
1978. 1~1978.11 삼성중공업(주)
1978.11~1985.7 한국전력기술(주)
1989.1~1989.6 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989.7~1992.9 미국 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA
1992.10~1994.2 한국전자통신연구원 광대역통신망연구부 선임연구원
1994.3~현재 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2000.1~현재 한국통신학회 학회지 편집위원
2001.3~2003.2 대구가톨릭대학교 공과대학장 역임
2004.2~현재 한국전자통신연구원 정보보호연구단 초빙연구원

관심분야 : 네트워크 보안, 통신망 성능분석, QoS 보장 기술