UPnP 보안 모델의 설계 및 구현

Design and Implementation of A UPnP Security Model

이동근, 임경식 • 경북대학교 컴퓨터과학과
박광로 • 한국전자통신연구원 네트워크연구소 홈네트워크팀
Dong-Gun Lee, Kyeng-Sik Lim • Dept. of Computer Science, Kyungpook National University
Kwang-Ro Park • Home Network Team, Electronics and Telecommunications Research Institute

요약

UPnP는 홈 네트워크 미들웨어 가운데 가장 먼저 상용화되었으나 보안에 관한 표준화된 기술이 없는 문제점이 있다. 본 논문에서는 이러한 UPnP를 위한 보안 모델을 설계하고 구현하였다. 설계된 모델은 XML Signature를 이용하여 사용자가 장치를 제어할 때 생성하는 UPnP 메시지에 보안 기능을 부가하도록 설계되었으며, 제공되는 기능은 장치 제어 메시지에 대한 인증 및 사용자 접근 제어이다. 본 보안 모델은 UPnP 모듈과는 독립적으로 구성되어 보안 서비스를 제공하는 특징을 가지고 있으며, 사용자 데이터의 부분 보안 기능을 제공하기위하여 사용자 부분으로 보안 모듈을 이동할 수 있도록 설계하였다. 마지막으로 구현한 UPnP 보안 모델이 사용자가 UPnP 오디오 장치를 제어할 때 적용되는 예를 보인다.

ABSTRACT

UPnP(Universal Plug and Play) is commercial product for the first time in home network middlewares, but it has problem that it has no security standards in UPnP specification. In this paper, we present UPnP security model. It is based on XML Signature of XML Security. It provides UPnP with secure services which are device control message authentication and user access level control. It is independent of UPnP modules and has mobility of secure service modules for non secure ability user part. We conclude this paper with an example of applying UPnP Security model to the UPnP audio device control and an test example.

Ⅰ. 서 론

2001년 10월 마이크로소프트사는 홈 네트워크 미들웨어인 UPnP가 기본적으로 운영체제 내에 포함된 Windows XP를 발표하였다. 이것은 홈 네트워크 미들웨어 가운데 가장 먼저 상용화되어 유포된다는 점에서 큰 의미를 가진다. UPnP는 TCP/IP, HTTP 및 XML과 같은 인터넷 표준과 기술을 기반으로 홈네트워킹 기기간의 제어모델을 설계하였기 때문에 기존 인터넷 기술을 이용하여 쉽게 제어모델을 구현할 수 있고 하드웨어와 소프트웨어

그리고 운영체제에 상관없이 동작이 가능하다. 하지만 보안에 관해서는 표준화된 기술이 없다. 그러한 이유는 홈 네트워크는 특별히 보안상 안전한 환경이라는 관점에서 디자인되었기 때문이다. 그러나 홈 네트워크와 인터넷의 연동은 필수적인 것이며 따라서 홈 네트워크에서도 기존 인터넷에서 발생할 수 있는 여러 가지 보안상의 문제가 충분히 발생할 가능성이 있다. 그러므로 표준화된 보안 기술이 없는 UPnP는 다양한 보안상의 위협에 노출되어질 것이다. 특히 SOAP 메시지를 통하여 장치를 제어하게 되는데 이러한 장치 제어 메시지에 대한 인증 및 사용자 접근 제어 메카니즘이 없기 때문에 보안상의 위험에 노출되어 있다[1,2,3,4].

본 논문에서는 UPnP 제어의 기본이 되는 XML 메시지 자체에 보안 기능을 제공할 수 있는 XML 보안의 XML Signature[5]를 이용하여 장치 제어 메시지를 인증하고 사용자 접근 제어가 가능한 보안 모델을 설계하고 구현하였다.

본 논문의 2장에서는 XML 보안을 기반으로 하는 보안 모델의 설계에 관한 내용으로 구조 및 동작 과정에 대하여 기술하고 3장에서는 보안 모델을 적용하여 구현한 내용에 관하여 설명한다. 4장에서는 구현한 보안 모델의 보안 기능 시험에 대한 설명을 하고 마지막으로 5장에서는 결론 및 향후 과제에 대하여 기술한다.

Ⅱ. XML 보안 기반의 UPnP 보안 모델

본 장에서는 UPnP 장치 제어 메시지 인증과 사용자 접근 제어 등의 보안 기능을 제공하기 위하여 XML 보안의 XML Signature를 이용하는 모델의 설계에 관한 것으로 구조 및 동작 과정에 대하여 설명한다.

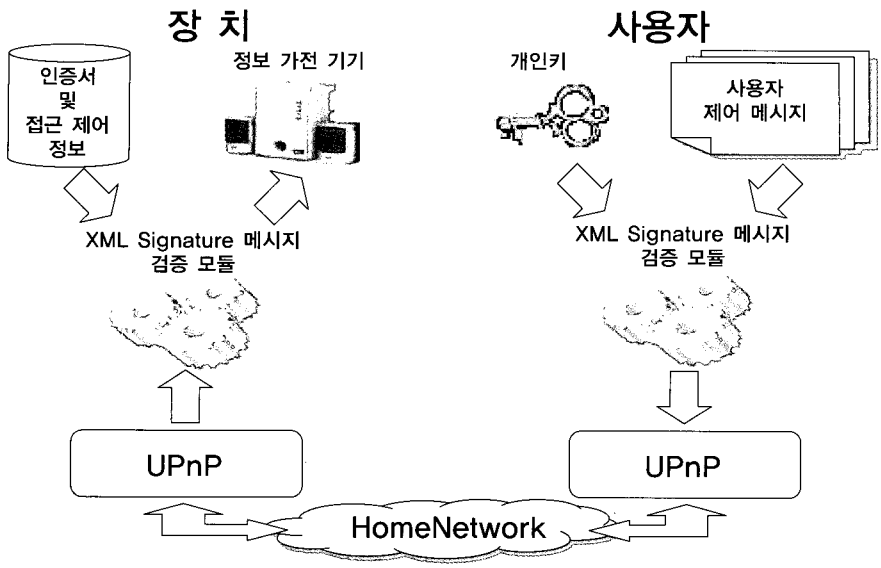
1. 보안 모델 구조

본 논문에서는 UPnP가 XML 메시지 기반의 동작 모델인 점에 착안하여 보안 모델을 설계하였다. 제안하는 보안 모델은 기본적으로 제어를 위하여 전달하는 XML 메시지에 인증 및 접근 제어 보안 서비스를 제공할 수 있는 정보를 같이 전달하여 동작하는 구조로 되어 있다. 사용자는 서비스 요청을 하는 제어 메시지를 생성하여 장치로 전달하고자 한다. 이때 기반 제어 인프라인 UPnP를 통하여 요청을 하게 된다. 결국 전달해야하는 인자를 사용자가 생성해야 한다는 것을 의미한다.

이러한 인자들의 내용에 인증 및 접근 제어 보안 서비스를 제공할 때 필요한 정보를 넣어서 장치로 전달하게 된다. 이러한 구조는 제어 메시지 형식을 만들고 전달하는 역할을 하는 미들웨어 즉 UPnP와 보안 서비스를 제공하는 모듈이 독립적으로 존재할 수 있고, 또한 보안 서비스 모델이 특정 미들웨어에 한정적으로 적용되지 않고 범용적으로 사용 가능한 장점이 있다.

[그림 1]은 보안 모델 구성 요소의 구조를 나타낸 것이다. 제시된 모델의 구조를 요약하면 다음과 같다. 사용자와 UPnP 사이에서 보안 서비스를 제공하며, XML Signature를 이용한 메시지 기반 보안 서비스 제공을 통하여 홈 네트워크 내에 정보 가전 기기들에게 사용자에 대한 인증 및 접근 제어 수단을 가질 수 있게 하는 보안 서비스 기반 구조이다[6].

사용자측에서 생성하는 인증 및 접근 제어 정보 메시지는 XML Signature를 기반으로 설정된다. 각각의 사용자들은 자신들의 신원 및 접근 제어 수준을 결정지을 수 있는 인증서를 가지게 된다. 인증서는 공개키 기반의 인증서로써 각각의 사용자들은 해당 공개키에 대한 개인키를 소유하게 된다. 이때 개인키 및 자신의 인증서는 여러 가지 방법으로 보



〔그림 1〕 보안 모델 구성 요소 구조

관 될 수 있다. 본 논문에서는 개인키와 인증서의 구체적인 관리 모델은 포함하지 않는다. 단지 개인키와 인증서를 안전하게 가지고 있다는 전제 하에서 본 논문을 기술한다. 사용자가 인증 및 접근 제어를 위하여 생성하는 XML 메시지 형태의 정보는 사용자에게 가독성을 높여준다. 예를 들어 기기들의 여러 기능들 가운데에서 보안 제어를 필요로 하는 것들이 어떠한 것이 있는지 쉽게 파악하고 홈 네트워크를 관리하는 사람들은 이러한 장치에서 사용할 수 있는 보안 요소들을 바탕으로 보안 정책을 결정할 수 있게 된다. 예를 들어 비디오 또는 열 가전 장치에 대하여 접근 제어를 할 수 있는 기능을 파악하고 제어할 수 있는 기능에 대한 접근 수준을 어떤 식으로 구분하는데 있어 XML 기반의 메시지는 도움을 준다. 이러한 XML 메시지는 각 사용자의 개인키로 서명되어 XML Signature 메시지 형태로 전달된다.

장치는 사용자로부터 전달받은 제어 메시지에 대한 구체적인 서비스를 처리하는 부분이다. 장치의 UPnP는 전달받은 제어 메시지에서 제어에 필요한 인자들을 장치 제어 모듈 부분으로 넘겨주게 된다. 이때 사용자에 대한 인증 및 접근 제어 정보 분석을 통하여 장치가 제공할 수 있는 서비스에 대한 처리를 결정하게 된다. 본 모델에서 장치는 가정내 각 구성원들이 할당받은 정당한 인증서를 확보하고 그것에 대한 정보를 관리한다. 정보 내에는 해당 사용자의 접근 수준 정보도 포함된다. 이러한 정보 역시 XML 형태로 저장 관리된다. 장치 부분의 구체적인 인증서 정보 관리 모델에 대해서는 기술하지 않는다. 단지 장치는 이러한 XML 정보를 안전하게 획득할 수 있다는 전제 하에서 기술을 한다. 사용자로부터 전달된 인증 및 접근 제어 정보를 획득한 장치는 이를 바탕으로 자신이 가지고 있는 인증서 관리 정보를 통해서 사용자의 공개키를 확보하게 되고 사용자가 서명하여 보낸 제어 메시지에 대하여 검증을 하게 된다. 검증이 완료되면 이에 대한 처리를 하게 된다.

첫째, 검증이 실패한 경우는 전달된 메시지에 문제가 있음을 의미한다. 인증되지 않는 사용자의 서명이 포함된 메시지이거나 혹은 누군가에 의하여 조작된 메시지임을 나타낸다. 그리고 전달된 제어 메

시지에 의하여 장치가 동작하지 않도록 보호한다.

둘째, 검증이 성공한 경우는 장치에서 사용자의 접근 수준을 검사하게 된다. 이는 장치가 확보하고 있는 해당 사용자에 대한 접근 수준 정보를 검색함으로써 알 수 있다. 이러한 정보는 XML 형태로 저장 관리되기 때문에 홈 네트워크를 관리하는 관리자가 쉽게 값을 설정, 판독할 수 있다. 정보의 설정은 관리자가 홈 네트워크 보안 정책을 수립하는 과정에서 결정이 된다. 장치에 대한 제어는 접근 수준에 따라 이루어진다.

2. 보안 모델 동작 과정

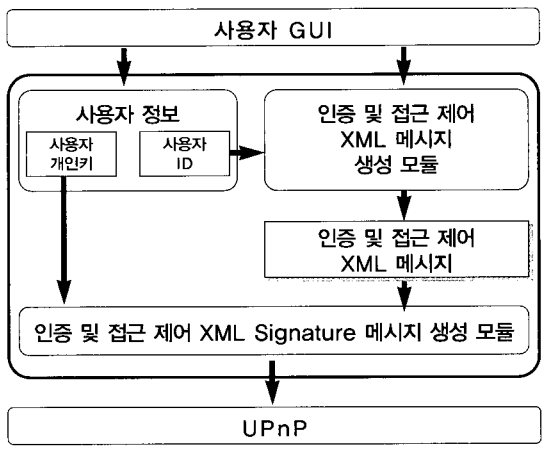
제안된 보안 모델의 구체적 동작 과정과 메시지 처리 과정은 사용자와 장치 부분으로 나누어서 기술한다. 먼저 사용자 부분에서의 동작 과정 및 메시지 생성 처리 과정을 살펴보면 다음과 같다.

사용자는 홈 네트워크 내의 기기들을 제어하고 정보를 얻기를 원한다. UPnP는 이러한 사용자에게 인터페이스를 제공하게 된다. 일반적으로 사용자들은 GUI를 통하여 이러한 정보를 인지하고 제어 이벤트를 발생시켜 전달하게 된다. 보안이 적용되지 않을 경우 이러한 이벤트에 의하여 발생된 메시지는 원본 그대로 장치로 전달되고 이를 받은 장치부분은 이러한 메시지에서 기기 제어 인자들을 분리해 내어서 실제 기기를 제어하는 모듈로 전달하여 기기를 제어하게 된다.

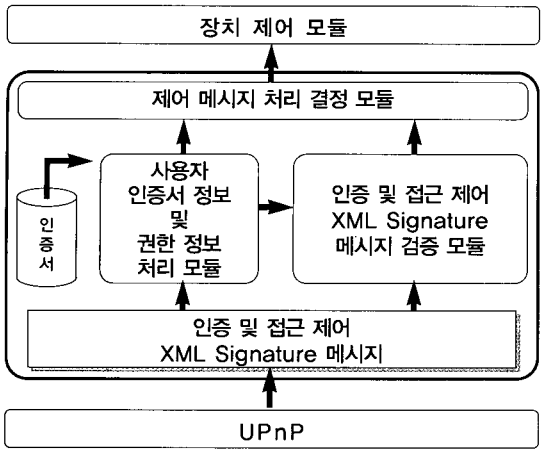
이러한 사용자 부분의 동작 과정에서 이벤트를 발생하여 메시지를 생성하고 UPnP로 전달하는 일련의 동작에서 보안 설정 관련 인자를 포함시켜 전달하는 것이 본 논문에서 제안하는 모델의 사용자 부분 기본 동작이 된다. 보안 설정이 포함된 동작 과정을 살펴보면 다음과 같다. 사용자는 홈 네트워크의 인증된 사용자임을 나타낼 수 있는 정보를 유지해야한다. 제시된 모델은 공개키 기반의 인증 방법을 사용한다. 사용자는 홈 네트워크 관리자로부터 발급 받은 인증서와 인증서의 공개키에 상응하는 개인키를 관리해야한다. 특히 개인키는 자신을 증명하는데 있어 중요한 역할을 하기 때문에 관리가 중요하다.

개인키는 XML Signature 메시지를 생성하는데 중요한 역할을 한다. 사용자의 개인키로 서명할 원본 메시지는 인증 및 접근 제어를 위한 정보인 사용자 ID, 메시지 생성 시간, 장치 제어 종류 등의 정보를 포함하고 있다. 생성된 메시지는 UPnP가 생성한 제어 메시지의 인자로써 장치에 전달되는데 이때 보안을 위한 인자를 포함하도록 제어 메시지를 생성하면 된다. 전달되는 내용은 두 가지 형태로 나누어 질 수 있다. 첫 번째는 XML Signature 메시지 전체가 인자의 내용이 되는 경우이고 두 번째는 장치와 사용자 사이의 공통된 규약을 통하여 서명처리된 메시지의 주요 인자만을 전달하는 방식으로 전송계층의 부담을 줄여 주는 방법이 있다.

〔그림 2〕는 사용자 부분의 동작과 메시지의 흐름을 나타낸 것이다. 사용자는 장치 제어 인터페이스를 통하여 제어 요청을 하게 된다. 이 때 제어 이벤트가 발생하면 사용자 정보 모듈에서는 사용자 ID 정보를 인증 및 접근 제어 XML 메시지 생성 모듈



〔그림 2〕 사용자 동작 과정



〔그림 3〕 장치 동작 과정

로 전달하여 서명할 원본 메시지를 생성하게 되고, 생성된 메시지를 인증 및 접근 제어 XML Signature 메시지 생성 모듈로 전달하게 된다. 그리고 사용자 정보 모듈에서 획득한 개인키를 이용해서 서명 처리된 메시지를 생성하게 된다.

〔그림 3〕은 장치 부분의 동작과 메시지의 흐름을 나타낸 것이다. 사용자로부터 제어 메시지를 수신한 미들웨어는 포함된 제어 인자들을 분리하게 되고 이를 상위 보안 처리 모듈로 전달하게 된다. 보안 처리 모듈의 사용자 인증서 정보 및 권한 정보 처리 모듈은 제어 메시지 정보를 바탕으로 해당 사용자에 대한 인증서 정보 및 권한 정보를 확보하게 되고 해당 정보를 인증 및 접근 제어 XML Signature 메시지 검증 모듈로 전달하게 된다. 이 때 미들웨어로부터 받은 서명 처리된 메시지를 검증하게 된다.

공개키 기반으로 인증 및 접근 제어를 관리하기 때문에 장치 부분은 사용자의 개인키로 서명하여 보내온 메시지를 검증할 수 있는 해당 공개키를 확보하고 있어야 한다. 이를 위하여 장치는 제어를 요청한 사용자들의 인증서의 정보를 획득할 수 있어야 한다. 본 논문에서는 인증서를 관리하는 방법에 대해서는 기술하지 않는다. 그 대신 사용자의 인증 정보를 맵핑하는 방법에 대하여 기술하고자 한다. 본 논문에서 제안하는 모델은 각 사용자별로 각각 다른 인증서를 홈 네트워크 관리자가 발급하게 된다. 각각의 사용자들은 고유 계정을 가지게 되고 이에 맵핑되는 인증서 또한 고유하게 된다. 따라서 특정 사용자가 서명한 내용을 검증하기 위한 인증서는 유일하게 존재하게 되는 것이다.

인증서와 함께 관리되어야 하는 정보는 각각의 사용자들의 장치에 대한 접근 수준이다. 이는 홈 네트워크 보안의 요구사항에도 포함되는 내용이다. 사용자로부터 수신된 보안 정보를 기반으로 생성된 XML Signature 메시지는 제어 메시지 요청자의 인증서와 접근 제어 수준 정보를 맵핑시켜 검증을 하게 된다. 이러한 과정을 통하여 장치 부분은 제어를 요청한 사용자가 정당하게 해당 홈 네트워크에서 인증된 사용자임을 판단하게 되고 사용자가 접근할 수 있는 기기에 대한 접근 수준을 결정한다〔7,8〕.

본 논문에서 설계된 보안 모델은 다음과 같은 보안 기능을 제공한다. UPnP 보안 모델을 통하여 기기를 제어할 경우 제어 요청을 하는 사용자에 대한 인증 서비스를 제공하며, 요청한 사용자의 기기에 대한 접근 수준을 판단한다. 또한, 요청한 메시지가 정확히 요청 사용자에 의하여 생성된 것인지 판단하며 메시지의 무결성에 관한 검사를 한다. 이러한 보안 기능은 XML Signature를 이용함으로써 제공된다. 사용자의 개인키로 서명된 메시지는 메시지의 무결성을 보장하고 공개키 인증서 기반의 사용자 관리는 사용자에 대한 인증 및 접근 수준을 관리하는 기능을 제공한다.

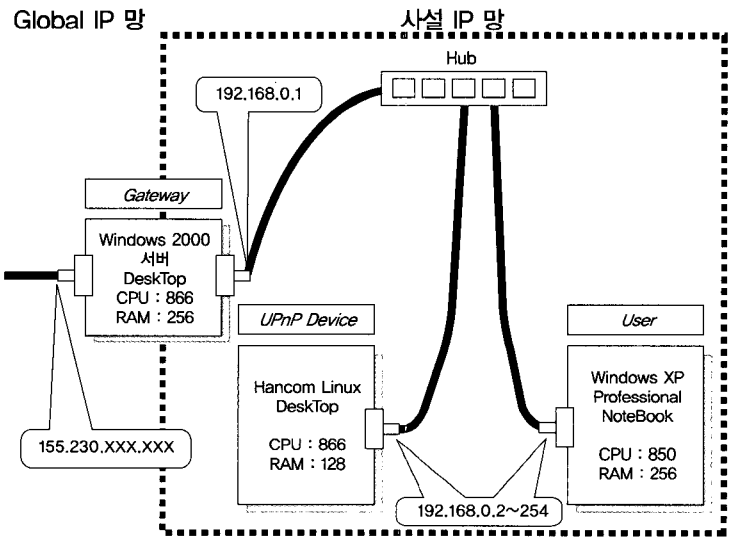
Ⅲ. UPnP 보안 모델 구현

본 장에서는 제시된 보안 모델의 설계를 바탕으

로 UPnP에 적용하여 구현한 결과에 대하여 기술한다.

1. 구현 환경

[그림 4]는 구현 환경을 나타낸 것이다. 홈 네트워크와의 유사성을 고려하여 홈 게이트웨이를 중심으로 분리된 독립 네트워크 망을 구성하였다. 이를 위하여 홈 게이트웨이에 해당하는 부분은 Windows 2000 서버를 사용하였으며 Internet Connection Service(ICS)를 사용하여 네트워크를 구분하였다. ICS는 Windows 운영체제에서 지원되는 IP 공유 서비스 프로그램이다. 사용자 부분은 운영체제 기본으로 UPnP모듈이 탑재되어 있는 Windows XP를 사용하였으며, 장치 부분의 운영체제는 Linux 이며, Intel에서 제공하는 UPnP SDK[9]를 설치하였다. 그리고 XML Signature 생성 및 처리는 Aleksey에서 구현한 공개 XML Security 라이브러리인 XMLSec[10]을 사용한다. XMLSec은 XML Security 표준을 지원하기 위해서 개발된 C 라이브러리로써 LibXML2와 OpenSSL[11]을 기반으로 구현되어 있다. 현재 XML Signature와 XML Encryption[12]을 지원하고 있으며 Canonical XML과 Exclusive Canonical XML은 LibXML2에서 지원 받고 있다. MIT 라이센스로써 GNU 자유 사용 라이브러리이다. Linux 와 Windows에 모두 사용이 가능하기 때문에 본 논문의 구현 모델에서 사용하였다. <표 1>



[그림 4] 구현 환경

<표 1> 구현 환경 구성원별 설명

구분	운영체제	미들웨어	프로그래밍도구	XML Security 라이브러리
홈 게이트웨이	Windows 2000 Server	없음	없음	
사용자	Windows XP professional	Windows UPnP	Visual C++ ATL COM	XMLSec
장치	Hancom Linux (Kernel 2.4.13)	Intel UPnP SDK	gcc	XMLSec

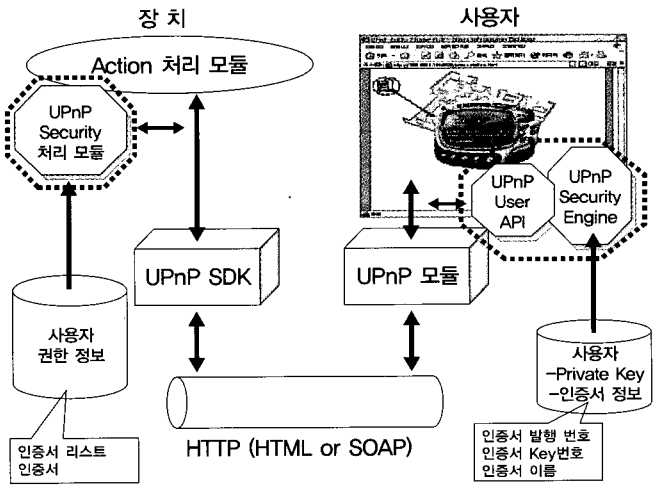
은 구현 환경 구성원별 운영체제, 사용된 미들웨어 및 프로그래밍 도구를 나타낸 것이다.

2. 구현 내용

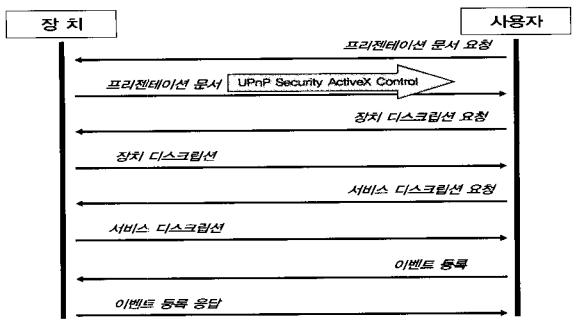
[그림 5]는 구현 결과물의 전체 구조를 나타낸 것이다. 장치와 사용자 부분으로 나누었을 때 장치 부분의 *UPnP Security* 처리 모듈이 구현된 부분이고 사용자 부분에서는 *UPnP User API*와 *UPnP Security Engine* 모듈이 구현된 부분이다. 나머지 부분들은 일반적인 UPnP 구성 요소들이다. 구현된 보안 처리 모듈이 UPnP와는 독립적임을 알 수 있다.

보안이 적용된 UPnP 모델은 오디오 장치를 제어하는 것으로써 사용자가 웹브라우저를 통하여 오디오 장치의 상태를 파악하고 오디오의 음악 데이터를 플레이, 정지시키거나 다음 곡을 선택할 수 있도록 동작한다. 사용자는 웹브라우저를 통하여 장치의 프리젠테이션 문서를 받게 되고 장치의 상태 정보를 알게된다. 장치에 대한 제어는 사용자가 GUI를 통하여 이벤트를 발생시킴으로써 이루어진다. 프리젠테이션 문서에 포함된 매크로미디어 플래쉬의 인터페이스를 통하여 플레이 버튼, 정지 버튼, 스캔버튼을 누름으로써 해당 제어 이벤트를 발생시켜 장치로 전달하게 된다. 이때 사용자측은 Windows XP에서 지원되는 UPnP 모듈을 통하여 제어 메시지를 장치로 보내게된다. 장치는 Linux에 설치된 Intel UPnP SDK가 지원하는 인터페이스를 통하여 사용자로부터 수신한 제어 메시지의 인자를 상위 계층으로 전달하게 된다. 이러한 과정은 보안 모델이 설정되지 않은 일반적인 동작이며, 보안이 적용될 경우는 다음과 같다.

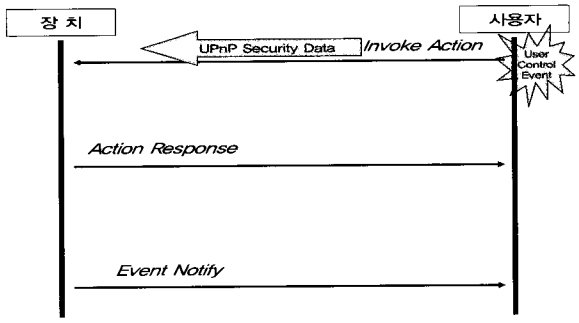
[그림 6]은 보안이 적용된 UPnP의 초기 설정 과정을 나타낸다. 클라이언트가 장치에게 프리젠테이션 문서를 요청하면 장치는 자신의 상태정보를 나타낼 수 있는 HTML 기반의 사용자 인터페이스 정보 문서를 사용자에게 전달한다. 이를 바탕으로 사용자는 장치의 상세 설명서에 해당하는 장치 디스크립션을 요청하고 이를 수신한 다음 정확한 서비스 정보를 포함한 서비스 디스크립션을 요청하고 수신한 다음 이벤트를 등록하게 된다. 이러한 과정을 통하여 사용자는 장치에 관한 정보를 획득하게된다. 보안 처리를 수행하는 ActiveX 컨트롤은 사용자가 프리젠테이션 문서를 받을 때 함께 전달된다.



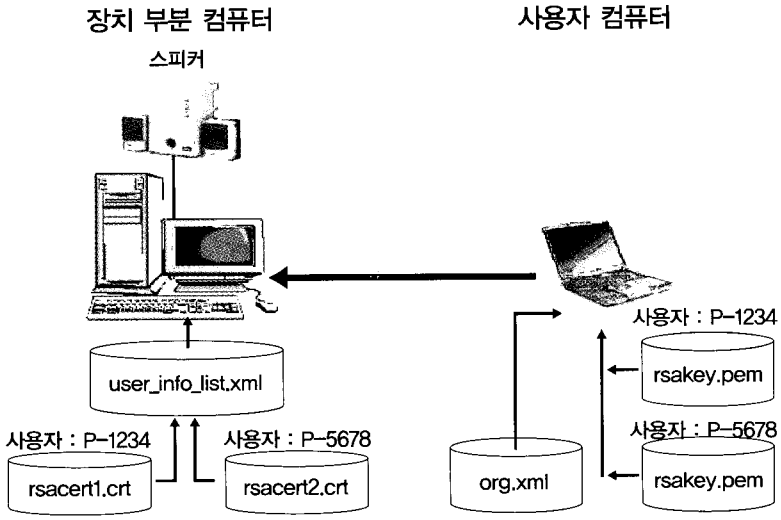
[그림 5] 구현 결과물 전체 구조



〔그림 6〕 UPnP 보안 적용 모델 초기 설정 동작 과정



〔그림 7〕 UPnP 보안 적용 모델 제어 동작 과정



〔그림 8〕 시험 환경

〔그림 7〕은 보안이 적용된 UPnP 제어 동작 과정을 나타낸다. 장치로부터 특정 서비스를 받기 위하여 사용자는 장치로 이벤트를 보내게된다. 이벤트가 발생하면 보안 ActiveX 컨트롤이 사용자 인증 및 접근 제어를 위한 정보를 생성하고 XML Signature 처리하여 UPnP로 전달하게 된다.

장치 제어 메시지는 Invoke Action을 통하여 SOAP 메시지 형태로 전달되게 된다. 장치는 수신된 제어 메시지에 대하여 사용자 인증 및 접근 제어를 결정한다. 그리고 제어 수준에 따른 장치 제어를 한 다음 결과를 Event Notify 형식으로 사용자에게 전달하게 된다.

Ⅳ. 시험

본 논문에서 구현된 UPnP 보안 모델을 시험하기 위하여 다음과 같은 설정을 하였다. 〔그림 8〕은 시험을 위한 환경을 나타낸 것이다. 장치와 사용자 부분으로 나누어져 있으며 사용자 노트북의 웹브라우저를 통하여 데스크탑 장치 부분 컴퓨터의 오디오 장치를 제어하여 음악이 나오도록 한 것이다. 그리고 사용자별 정보를 각 파일별로 읽어오는 것을 나타내고 있는데 장치 부분에서는 개인별 인증서 정보를 읽어 오는 것과 사용자 부분에서는 개인별 개인키를 읽어 오는 것이 나타나 있다. 부분별 정보 저장 파일

들에 대한 설명은 〈표 2〉를 통해서 기술된다.

홈 네트워크의 허가된 사용자를 2명으로 정하고 사용자 구분을 위하여 *P-1234*와 *P-5678*의 ID를 부여한다. 또한, 사용자별로 개인키와 공개키 인증서를 생성 발급한다. 공개키 인증서, 홈 네트워크 사용자별 정보 및 접근 수준을 저장한 파일들을 장치가 있는 컴퓨터의 특정 디렉토리에 저장하고 사용자별 개인키는 사용자 컴퓨터의 특정 디렉토리에 저장한다. 〈표 2〉는 저장된 정보 파일별 설명을 나타낸 것이다. *user_info_list.xml*은 홈 네트워크 사용자별 정보 및 접근 수준 정보가 저장된 XML 파일로써 〈표 3〉에 나타난 것처럼 사용자 ID를 알려주는 〈*UserID*〉, 인증서 이름을 알려주는 〈*Cert*〉, 장치 제어의 종류를 알려주는 〈*Action*〉, 제어 수준을 알려주는 〈*Level*〉로 구성되어 있다. 이러한 정보를 바탕으로 해당 사용자에 대한 인증서 파일의 이름과 특정 제어에 대한 사용자 제어 수준을 알 수 있다. *org.xml*은 사용자가 생성한 제어 메시지를 XML Signature 처리하여 생성된 메시지 정보가 저장된 파일이다. *rsacert1.crt*와 *rsacert2.crt*는 사용자들에게 발급된 공개키 인증서들이며, *rsakey.pem*은 RSA 공개키에 대한 사용자의 개인

〈표 2〉 장치와 사용자 부분 정보 파일

장치 부분 저장 파일		사용자 부분 저장 파일	
홈네트워크 사용자별 정보 및 접근 수준 정보 저장	user_info_list.xml	서명된 제어 메시지 정보	org.xml
사용자 P-1234 인증서	rsacert1.crt	사용자 P-1234 개인키	rsakey.pem
사용자 P-5678 인증서	rsacert2.crt	사용자 P-5678 개인키	rsakey.pem

〈표 3〉 user_info_list.xml

```
〈?xml version="1.0" encoding="UTF-8" ?〉
  〈User_Info〉
    〈List1 xmlns="http://leedg/P-1234#"〉
      〈UserID〉P-1234〈/UserID〉
      〈Cert〉rsacert1.crt〈/Cert〉
      〈Action xmlns="http://leedg/Play_P-1234#"〉
        〈Level〉5〈/Level〉
      〈/Action〉
    〈/List1〉
  〈List2 xmlns="http://leedg/P-5678#"〉
      〈UserID〉P-5678〈/UserID〉
      〈Cert〉rsacert2.crt〈/Cert〉
      〈Action xmlns="http://leedg/Play_P-5678#"〉
        〈Level〉3〈/Level〉
    〈/Action〉
  〈/List2〉
  〈/User_Info〉
```

키를 저장한 파일이다.

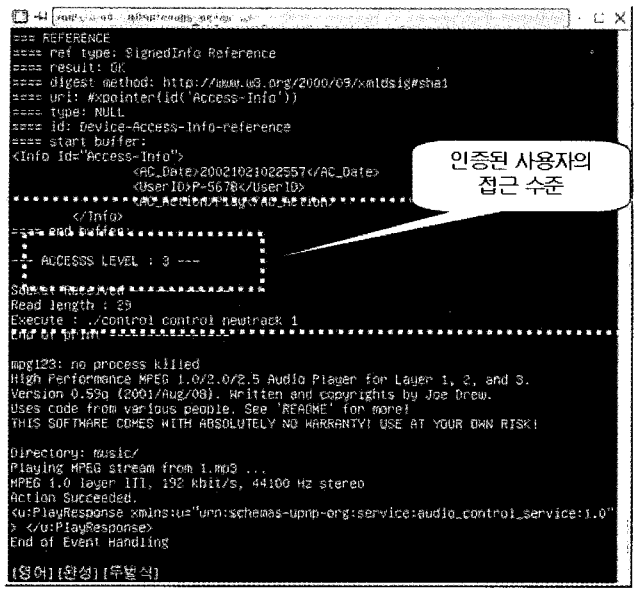
시험은 3가지 시나리오로 이루어진다. 첫 번째는 사용자 *P-1234*가 오디오 장치를 제어하는 것이고, 두 번째는 *P-5678*이 오디오 장치를 제어하는 것이고, 세 번째는 프리젠테이션 파일을 수정하여 허가되지 않은 사용자가 인증 메시지를 조작한 경우이다. 시험 과정에서 확인하는 내용은 다음과 같다. 사용자가 제어하는 과정에 나타나는 장치 부분의 로그 메시지 정보를 바탕으로 사용자 인증 및 제어 메시지에 대한 인증 여부를 확인하고 접근 제어 수준 값이 해당 사용자의 제어 수준 값인지를 확인한다. 사용자 변경은 *rsakey.pem* 파일을 교환하는 방식으로 이루어지며 프리젠테이션 파일에 대한 조작은 서버의 *presentation.html* 파일의 정보를 변경시키는 방법으로 한다.

1. 시험 결과

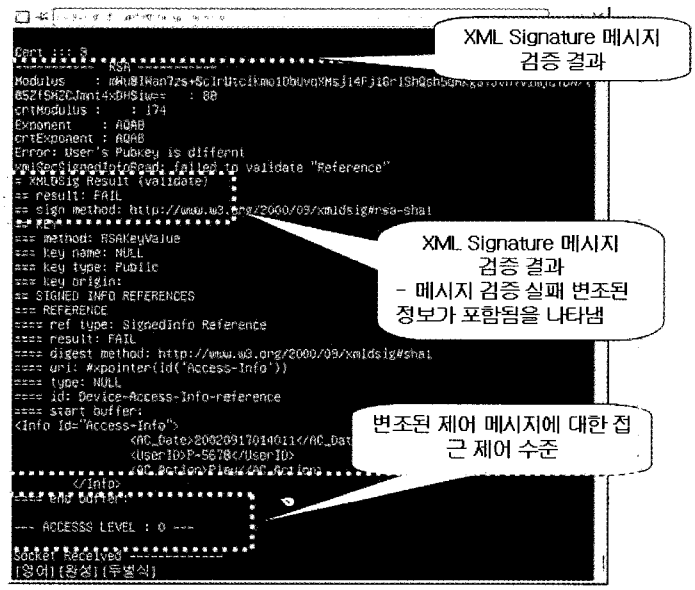
3가지 시나리오에 있어 공통적으로 동작하는 결과에 대하여 설명하면 다음과 같다. 사용자가 웹 브라우저를 통하여 장치를 제어하기 위하여 장치의 프리젠테이션 문서를 요청하면 웹브라우저에 장치를 제어하고 장치의 정보를 보여주는 인터페이스가 나오게 된다. 이때 프리젠테이션 문서와 함께 보안 적용이 가능한 ActiveX 컨트롤도 함께 전송이 되어 오고 서명된 컨트롤 CAB 파일을 승인하면 컨트롤이 사용자의 시스템에 설치가 되고 보안 기능을 사용할 수 있게 된다.

첫 번째 시나리오인 사용자 *P-1234*가 오디오를 플레이시키기 위하여 제어 메시지를 보낸 경우에 사용자로부터 오디오 데이터를 플레이하라는 제어 메시지를 전달받은 모습을 로그 메시지로 확인할 수 있었고 또한 사용자 인증 및 접근 제어 인자 데이터도 같이 전달되어 온 것을 알 수 있었다. 또한, XML Signature 메시지를 검증한 결과가 정상적임을 확인할 수 있었고 마지막으로 홈 네트워크 관리자가 사용자에게 부여한 장치에 대한 접근 제어 수준 값인 *5*가 나타남을 알 수 있었다. 두 번째 시나리오인 사용자 *P-5678*이 오디오를 플레이시키기 위하여 제어 메시지를 보낸 경우에도 첫 번째 시나리

[그림 9] 검증 결과에 따른 사용자 P-1234의 접근 제어 수준 결정



〔그림 10〕 검증 결과에 따른 사용자 P-5678의 접근 제어 수준 결정



〔그림 11〕 변조된 메시지에 대한 검증 및 접근 제어 수준 결과

오와 같은 결과를 얻을 수 있었으며 마지막으로 홈 네트워크 관리자가 부연한 장치에 대한 접근 제어 수준을 값인 3이 나타남을 알 수 있었다. 세 번째 시나리오인 변조된 메시지를 사용하는 경우에는 XML Signature 메시지를 검증한 결과에서 검증 실패를 출력하였고 변조된 메시지임을 나타냈었다. 또한, 메시지에 대한 인증을 할 수 없기 때문에 사용자의 장치에 대한 접근 제어 수준을 값이 0으로 나타남을 확인할 수 있었다. 〔그림 9〕는 첫 번째 시나리오에서 인증과정을 거친 후 접근 제어 수준 값

이 표시된 로그 메시지를 나타낸 것이다. [그림 10]은 두 번째 시나리오에서 나타난 결과를 보여주는 로그 메시지이며 [그림 11]은 세 번째 시나리오의 결과인 검증 실패 및 장치에 접근할 수 없음을 나타내는 로그 메시지이다.

3가지 시나리오의 시험 결과 본 논문에서 설계된 UPnP 보안 모델은 정당한 사용자에게는 홈 네트워크 관리자가 인정한 장치 제어 수준에 따라 장치를 제어할 수 있었으며 장치를 부당하게 사용하려는 사용자 혹은 메시지에 대해서는 장치를 사용할 수 없도록 차단하는 기능을 제공함을 알 수 있었다.

Ⅴ. 결론 및 향후 과제

본 논문에서는 XML 보안의 XML Signature를 이용하여 UPnP에 인증 및 접근 제어 보안 기능을 제공하는 모델을 설계하였고 실제로 모델을 적용하여 구현하였다. 구현된 모델을 통하여 오디오 장치를 작동시키는 제어 명령에 대하여 사용자의 인증 확인과 접근 제어 수준을 처리를 통하여 장치 제어에 보안 기능을 확보할 수 있도록 하였다. 제안된 모델은 UPnP에 보안 기능을 제공하도록 설계되었지만 구조상 특정 미들웨어에 종속되지 않는 특징을 가지고 있으며, 또한 보안 서비스가 제공되지 않는 사용자 환경에 보안 모듈을 이식할 수 있는 특징을 가지고 있다.

이러한 특징은 구현 부분에서 보안 기능 ActiveX 컨트롤을 구현함으로써 보여줄 수 있었다. 홈 네트워크 또한 하나의 인터넷으로써 정보 가전 기기들이 홈 네트워크상에서 하나의 호스트로서 동작하고 있다. 따라서 인터넷에서 발생할 수 있는 보안상의 문제점은 홈 네트워크 내에서도 충분히 발생할 수 있다. 그리고 홈 네트워크 사용자는 이러한 보안상의 문제점으로부터 보호받기를 원한다. 이러한 점에서 보안에 관한 표준화된 기술이 없는 UPnP에 새로운 보안 모델을 제시하고 구현하여 보안 기능을 제공함으로써 UPnP가 홈 네트워크 사용자들로부터 안전성을 인정받는 것이 가능하도록 하였다.

본 논문에서 제안된 모델은 인증 및 접근 제어용 보안 모델이므로, 향후 XML Encryption을 이용하여 기밀성을 포함한 다양한 보안 서비스를 제공할 수 있는 범용 모델로의 확장에 관한 연구가 요구된다.

저자 소개

이 동 근

2001년 경북대학교 컴퓨터과학과(이학사)
2001년~현재 경북대학교 컴퓨터과학과(석사과정)
관심분야 : 무선 인터넷, 네트워크 보안, 컴퓨터통신

박 광 로

1982년 경북대학교 전자공학과(학사)
1985년 경북대학교 대학원(석사)
2002년 충북대학교 대학원(박사)
1984년~현재 ETRI 네트워크연구소 홈네트워크팀장(책임연구원)
관심 분야 : 홈 네트워크 기술, 무선LAN 기술, VoIP 기술, L-Biz

임 경 식

1982년 경북대학교 전자공학과 (공학사)
1985년 한국과학기술원 전산학과 (공학석사)
1994년 University of Florida 전산학과(공학박사)
1985년~1998년 한국전자통신연구원 책임연구원, 실장
1998년~현재 경북대학교 컴퓨터과학과 조교수
관심분야 : 이동 컴퓨팅, 무선 인터넷, 홈 네트워킹, 컴퓨터 통신

■ 참고문헌

[1] Steven G. Ungar,Home Network Security, Proceedings of 2002 IEEE 4th International Workshop on Networked appliances, pp.41 -48, January 15-16, 2002.

[2] Saif, U., Gordon, D., Greaves, D., Internet access to a home area network, IEEE Internet Computing, Volume: 5 Issue: 1, January-February 2001.

[3] Senthil Sengodan, Robert Ziegler Linda Edlund, On Securing Home Networks, INET 2001 Conference proceedings, T79- HomeSec, June 2001.

[4] 전호인, 신용섭, 홈 네트워킹 기술 및 표준화 동향, 대한전자공학회 전자공학회지, 제29권, 제6호, pp.18-39, 2002년 6월.

[5] W3C, XML-Signature Syntax and Processing, February 2002, http://www.w3.org/tr/2002/rec-xmldsig-core-20020212/.

[6] Jan Christian Kerlefsen, XML-based household profiling for home networks, IEEE International Conference on Consumer Electronics, pp.198-199, June 17-21, 2001.

[7] Prashant Krishnamurthy, Joseph Kabara, Security Architecture for Wireless Residential Network, IEEE Transactions on Consumer Electronics, Volume: 48, Issue: 1, February 2002.

[8] Roli G. Wendorft, Rob T. Udink, Maarten P. Bodlaender, Remote Execution of HAVi Applications on Internet-enabled Devices, IEEE Transactions on Consumer Electronics, Volume: 47, Issue: 3, August 2001.

[9] Linux SDK for UPnP Devices 1.0, An Open Source UPnP Development Kit, http://upnp.sourceforge.net/.

[10] Aleksey, XMLSec Library, http://www.aleksey.com/xmlsec/.

[11] OpenSSL, http://www.openssl.org/.

[12] W3C, XML-Encryption Syntax and Processing, October 2002, http://www.w3.org/tr/2002/pr-xmlenc-core-20021003/.