무선 LAN 환경에서 UPnP 홈네트워크 보안 취약점에 관한 연구

한설흠*, 권경희**
단국대학교 전자계산학과
e-mail :wise@dankook.ac.kr*, khkwon@dankook.ac.kr**

A Study for Vulnerability of Security of UPnP Home-Network in Wireless LAN Environment

Seol-Heum Han*, Kyung-Hee Kwon**
Dept. of Computer Science, DanKook University

요 약

UPnP(Universal Plug and Play) 홈네트워크에서 무선랜은 위치에 상관없이 쉽게 설치하여 사용할 수 있어 사용자에게 편의성을 제공 하지만, AP(Access Point)는 해킹을 통한 MAC 주소 및 SSID(Service Set Identifier), WEP(Wired Equivalent Privacy)의 암호를 쉽게 알 수 있어 보안에 취약하다. 또한 UPnP 는 TCP/IP 를 사용하는 인터넷 표준과 기술을 기반으로 하고 있고 HTTP, UDP, SSDP, GENA 등의 표준 프로토콜을 사용하기에 보안 대책에 취약점을 가지고 있다. 본 논문에서는 댁외에서 UPnP 홈네트워크에 사용되는 AP 를 해킹하고, 해킹한 AP 정보를 이용하여 UPnP 홈네트워크의 디바이스 정보를 취득하고, 댁내 컨트롤 포인트(Control Point)를 해킹하여 MAC 주소 및 IP 주소를 댁외 컨트롤 포인터로 변조하여 UPnP 홈네트워크 디바이스를 제어하는 실험으로 UPnP 홈네트워크 보안의 취약점에 대해 분석한다.

1. 서론

홈네트워크 분야에서는 다양한 정보가전기기를 하나의 통신망으로 묶어서 서비스하려는 연구가 최근 활발해 지고 있다. 홈네트워크 미들웨어로서는 Havi, JINI, UPnP 등의 대표적인 것들이 있는데, UPnP 는 마이크로소프트사가 홈네트워크 미들웨어로 상용화하여 많은 관심을 받고 있다. UPnP 는 윈도우 운영체제에서 plug & play 로 작동되며, 그 편의성으로 인해 최근 많은 관심을 받고 있다.

UPnP 는 독립적인 수행체제를 가지고 있지만 보안에 대한 표준이 없고 사용자가 쉽게 디바이스에 접근하고 서비스를 받도록 설계되어 보안에 취약하다.

현재 설계된 모델은 XML Signature[2]를 이용한 디바이스의 사용을 제안하는 UPnP 메시지에 대한 인증을 통한 사용자 접근제어 기능을 부가하여 사용하고 있으나 쉽게 정보를 유출할 수 있는 단점이 있다.

또한 HTTP 를 통한 HTML, XML 문서로 기능을 제어하는 인터페이스를 제공한다. 이는 프리젠테이션을 통하여 제어 디바이스의 기능과 정보를 제공하므로 컨트롤 포인트에서 홈네트워크 디바이스를 발견하고 제어할 수 있게 된다.[3] 특히 SOAP(Simple Object Access Protocol) 메시지를 통하여 장치를 제어하는데 이러한 제어 메시지에 대한 인증 및 사용자 메커니즘이 없기 때문에 보안상 노출되어 있다.[3,7]

UPnP 홈네트워크의 디바이스는 인가된 컨트롤 포인트와 비인가 컨트롤 포인트에 의해 제어되어 서비스에 문제가 발생될 수 있고, Sniffing 을 이용하여 비인가 컨트롤 포인트가 인가된 컨트롤 포인트의 IP 주소 및 MAC 주소를 변조하여 위장하면 UPnP 는 비인가된 컨트롤 포인트에게도 디바이스의 상태 값을 서비스하여 문제가 될 수 있다.

본 논문에서는 UPnP 를 이용한 서비스가 상용화되고 있는 시점에 실험을 통하여 UPnP 의 취약점을 분석하여, 차후에 이를 개선하기 위함이다. 이에 따른 실험은 비인가된 댁외에서 UPnP 홈네트워크에 사용되는 AP 를 Sniffing 툴로 해킹하고, 해킹한 AP 의 SSID, WEP 키값 그리고 MAC 주소를 이용하여 UPnP 홈네트워크의 디바이스 정보를 취득하고, 댁내 컨트롤 포인트를 해킹하여 MAC 주소 및 IP 주소를 댁외 컨트롤 포인터로 변조하여 UPnP 홈네트워크 디바이스를 제어하는 실험으로 무선랜 환경이 UPnP 홈네트워크의 보안 기능을 미치는 영향에 대하여 분석하며, UPnP 홈네트워크 보안의 취약점에 대해 분석하고 차후 개선방법을 연구하려 한다.

본 논문의 2 장에서 UPnP 의 보안 취약점에 대하여 설명하고, 3 장에서 무선랜 보안에 대하여 설명하고, 4 장에서 실험 및 결과에 대하여 설명하고, 마지막으로 본 연구에 대한 성과와 차후 연구에 대하여 설명하며

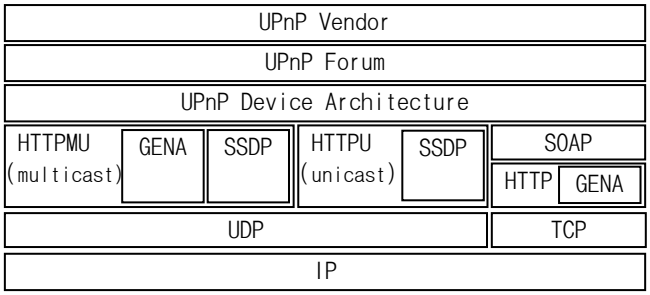
본 논문을 마무리 한다.

2. UPnP 의 보안 취약점

UPnP 는 홈네트워크 환경에서 플랫폼에 독립적인 서비스 환경을 제공하는 미들웨어로 단순하고 유연하며 단대단(Peer to Peer) 방식의 연결성을 제공하므로, 사용자는 단지 디바이스를 홈네트워크에 연결 시켜주면 홈네트워크 상에 연결된 기존의 디바이스를 발견하여 제어하거나 다른 디바이스가 가진 서비스를 찾을 수 있다. 이 장에서는 UPnP 구조 및 보안에 대하여 설명한다.

2.1 UPnP 구조

UPnP 는 TCP/IP 기술을 바탕으로 현재 인터넷에서 사용하고 있는 HTTP(Hyper Text Markup Language), SSDP(Simple Service Discovery Protocol), GENA(General Event Notification Architecture), 그리고 SOAP(Simple Object Access Protocol) 등의 프로토콜을 이용하여 디바이스의 정보를 수집하고 디바이스를 제어한다. SSDP 는 네트워크상에 서비스를 찾기 위한 프로토콜이며, GENA 는 한 디바이스의 상태가 변했을 때 이를 다른 디바이스에게 알리는 프로토콜이며, SOAP 는 한 디바이스가 다른 디바이스에게 제어명령을 보내기 위해 사용되는 프로토콜이다.[3] (그림 1)은 UPnP 프로토콜 구조를 나타낸 그림이다.



(그림 1) UPnP 프로토콜 스택

UPnP 프로토콜은 Addressing, Discovery, Description, Control, Eventing, Presentation 단계로 이루어진다.

UPnP 는 IP 기반으로 동작하므로 디바이스들은 우선적으로 자신의 IP 주소를 DHCP(Dynamic Host Configuration Protocol) 또는 Auto IP 를 이용하여 설정한다. 이후 디바이스들은 SSDP 를 이용하여 자신이 제공하는 서비스를 광고하며, [3] 컨트롤 포인트는 SSDP 와 GENA 를 이용하여 자신이 제어하고자 하는 디바이스를 찾게 된다. 컨트롤 포인트는 디바이스들을 발견한 후 제어를 위한 문서를 디바이스로부터 전송 받아 이들을 제어할 준비를 마치게 된다.

2.2 UPnP 보안

UPnP에서는 홈네트워크 내에 여러 보안 도메인이 존재하고, 물리적 공간을 뛰어 넘는 가상 홈네트워크 보안 도메인구성이 가능하며 디바이스 단위로 인증과 암호화를 수행하며, 보안 명령을 발행하는 컨트롤 포인트와 보안 명령을 수신하여 해당 명령을 수행하는 디바이스 간에 보안 서비스를 제공하기 위해 필요한 표준을 정의하고 있다.[4,5,6]

UPnP 홈네트워크 보안 표준은 디바이스를 사용하는 사용자 단위의 보안 서비스를 제공하는 것이 아니라, 홈네트워크 내에 존재하는 다양한 디바이스에 대한 인증 기능을 제공하고, 또한 디바이스 단위의 ACL(Access Control List) 또는 인가 인증서(Authorization Certificate)에 기반하는 접근 제어 기능을 제공하고 있으며, SOAP 메시지 단위의 선택적인 기밀성 서비스와 무결성 서비스를 제공하고 있다. 디바이스에 대한 접근제어는 ACL, 그룹 맴버십 인증서, 인가 인증서를 이용하여 수행하고, 디바이스의 ACL은 주체, 인가정보, 대리여부, 유효기간으로 구성되며, 각 디바이스에서 관리한다. 디바이스 보안 서비스는 해당 디바이스에 대한 제어 권한을 가지고 있는 제어 디바이스를 규정하고 있는 디바이스 소유권 관련 동작, 세션키 공유 동작, 각 디바이스의 ACL 편집 관련 동작, 인가 인증서 관련 동작 등으로 구성된다.[5,6, 10]

UPnP 보안은 디바이스들 상호간에 커뮤니케이션을 위한 기술과 표준을 사용한다. 홈네트워크에는 여러 종류의 가전기기들이 서로 연결되어 사용자에게 다양한 서비스를 제공한다. 사용자는 댁내에서 네트워크에 연결된 디바이스들을 수시로 모니터링하고 제어할 수 있으며, 중요한 이벤트가 발생하였을 경우 디바이스는 이를 사용자에게 능동적으로 알려줄 수 있다.[9] 그러므로 UPnP 홈네트워크의 디바이스 정보를 사용자가 알 수 있고 제어할 수 있다.

UPnP 홈네트워크는 디바이스에 대한 보안 규정은 있지만 사용자에 대한 보안 규정이 없어 디바이스를 제어하는 컨트롤 포인트에 대한 보안이 없어 비인가 사용자가 쉽게 접근할 수 있어 취약하고, 또한 무선랜을 이용한 UPnP 홈네트워크의 접근에 대한 보안은 허가되지 않은 사용자의 접근에 매우 취약하다.

3. 무선랜 보안

무선랜은 UPnP 홈네트워크 서비스를 위한 디바이스 연결이나 컨트롤 포인트의 연결에 이용한다. UPnP 홈네트워크에서 발생할 보안의 취약점과 기능을 분석한다. 무선랜의 보안기능은 사용자 인증과 기존의 무선랜 시스템에서 제공되는 보안기능에 대해 분석한다.

IEEE802.11x 표준은 무선랜의 인증과정과 비밀성을 제공하기 위하여 SSID(Service Set Identifier)와 WEP (Wired Equivalent Privacy)을 정의하여 사용자 접근제어의 기본 수준을 제공한다. SSID 를 기반으로 하는 방안은 효율이 떨어지므로 추가적으로 데이터에 대한 보안성을 제공하기 위하여 WEP 방식의 암호화를 병행하면서 좀더 높은 강도의 보안을 제공한다.[12]

IEEE802.11x 에서 사용자 인증은 암호기술을 이용하는 경우와 그렇지 않은 경우가 있다. 우선 암호기술에 기반하지 않은 인증 방법에 대해서 살펴보면 SSID 를 이용하는 방법과 MAC 주소를 이용하는 방법이 있다.

SSID 를 이용하는 방법에 대해서 살펴보면, 무선랜 카드에서 AP 로 전송되는 SSID 는 단순한 평문 형태로

되어 있어 도청이 가능하며[11], 공격자는 도청한 SSID 를 이용해 자신을 위장하여 AP 에 접속할 수 있다.

또한 UPnP 는 디바이스에 대한 보안은 있지만 사용자에 대한 보안이 없어 IP 주소 및 MAC 주소를 변조하여 위장하면 인가된 사용자인지 알 수 없어 보안에 취약하다.

4. 실험 및 결과

본 장에서는 사용자 인증에 관한 UPnP 홈네트워크 보안을 실험으로 알아보고, AP 보안이 UPnP 보안에 미치는 영향에 대하여 실험으로 살펴본다. 실험의 순서는 댁외에서 AP 정보를 취득하고, AP 와 접속이 이루어지면 댁내 컨트롤 포인트의 정보를 취득하고, 컨트롤 포인터로 변조하여 위장하고, 디바이스를 제어하는 순서로 진행한다.

먼저 Sniffing 툴을 이용하여 AP 의 SSID 및 WEP 키값을 쉽게 알 수 있었고, AP 의 MAC filtering 은 접속이 허용된 MAC 주소의 목록을 저장하고 있는데 Sniffing 툴을 이용하여 AP 와 통신하는 무선랜 카드에 대한 정보를 알 수 있었다. MAC 주소를 이용한 인증의 경우도 SSID 를 통한 인증과 마찬가지로 MAC 주소가 평문 형태로 전송되기 때문에 쉽게 알 수 있었다.

댁내 컨트롤 포인트와 댁외 컨트롤 포인트가 보안이 설정된 AP 를 이용하여 UPnP 홈네트워크의 디바이스의 제어하는 방법에 대하여 실험을 한다. 인가된 댁내 컨트롤 포인트는 PC 의 무선랜을 이용하고, 비인가된 댁외 컨트롤 포인트는 노트북의 내장 무선랜을 이용하여 AP 에 연결하고, MAC 주소 및 IP 주소를 변조하여 UPnP 서비스를 받는 실험을 한다.

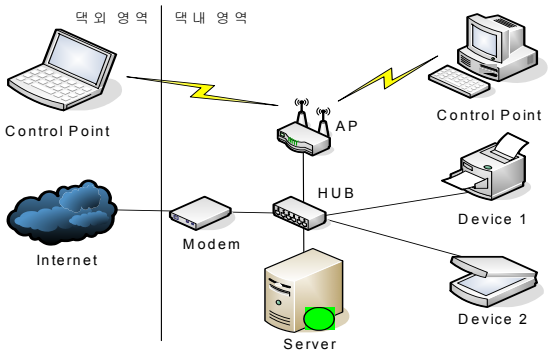
Device	Desc
Server	Linux Kernel 2.4.x Linux SDK for UPnP Device 1.04
AP	Linksys WAP54G
Control Point1	Linksys WUSB54G
Control Point2	Intel Pro/Wireless 3945ABG

<표 1> 실험에 사용된 디바이스

실험을 위해 <표 1>과 같이 Linux 서버에 SDK UPnP 미들웨어를 설치하고[1] 서버와 AP 그리고 컨트롤 포인트를 연결하였다. 컨트롤 포인트는 PC 에 무선랜을 설치하였으며, 노트북의 내장 무선랜을 이용하여 해킹한다.

UPnP 프로토콜은 Addressing, Discovery, Description, Control, Eventing, Presentation 단계로 이루어진다. UPnP 는 Presentation 단계에서 게이트웨이 내의 모든 컴퓨터에게 디바이스 정보를 광고한다. 이때 UPnP 는 HTTP, XML 로 디바이스의 위치 및 제어 정보를 전달하기 때문에 디바이스 정보를 받은 모든 컴퓨터는 UPnP 홈네트워크의 디바이스를 제어할 수 있다.

아래 (그림 3)은 실험에 사용된 UPnP 홈네트워크의 구성도이다. 댁내영역의 컨트롤 포인트는 인가된 디바이스이며 댁외 컨트롤 포인트는 비인가된 디바이스로 AP 를 이용하여 댁내 컨트롤 포인트로 변조하여 위장하는 방법을 설명한다.



(그림 3) UPnP 홈네트워크 구성도

댁외 컨트롤 포인트가 댁내 컨트롤 포인트의 MAC 주소 및 IP주소로 변조하여 위장하는 방법은 IP주소만 변조하는 방법과 MAC주소만 변조하는 방법 그리고 MAC주소와 IP주소 모두를 변조하여 방법이 있는데, 마치 댁외에서 댁내 컨트롤 포인트처럼 디바이스를 제어하는 방법을 실험한다.

댁내 컨트롤 포인트의 IP 주소나 MAC 주소를 댁외 컨트롤 포인트의 주소로 변조하여 위장하고 접속을 시도하여 디바이스 상태값을 변경할 수 있었다. 이를 통하여 사용자에 대한 인증이 없는 것을 확인 했다.

실험한 결과를 정리하면 비인가 댁외 컨트롤 포인트가 인가된 댁내 컨트롤 포인트의 IP 주소나 MAC 주소를 변조하여 위장하면 UPnP 홈네트워크에 치명적인 영향을 줄 수 있다는 것을 확인 하였다.

UPnP 홈네트워크의 보안을 위해 메시지나 키값을 이용한 전통적인 인증방법을 이용할 수도 있는데 서비스 속도 저하 및 추가적인 시스템이 필요할 수도 있어 단점이 될 수 있다. 이를 개선하기 위해서는 기존 UPnP 프로토콜을 이용한 보안 강화로 디바이스 및 사용자 인증을 하여 안정된 서비스를 할 수 있어야 한다.

5. 결론

본 논문에서 AP 를 해킹을 통하여 AP 의 보안 취약점에 대하여 살펴보았고 UPnP 홈네트워크를 MAC 주소 및 IP 주소를 변조하여 위장한 디바이스를 제어하는 실험으로 UPnP 홈네트워크의 보안에 대하여 점검해 보았다. UPnP 홈네트워크는 디바이스에 대한 보안 규정을 두고 운영하지만 사용자에 대한 보안 규정이 없어 보안에 취약하였다. UPnP 홈네트워크에서 디바이스에 대한 보안의 강화와 사용자에 대한 보안 규정을 만들어 안전한 UPnP 서비스가 되어야 한다. 또한 무선랜은 홈네트워크 환경에서 반드시 필요한데 보안이 취약하여 UPnP 보안을 더욱 취약하게 할 수 있다. UPnP 보안을 강화하기 위해 UPnP 사용자 인증이나 UPnP 프로토콜에 대한 연구가 필요하다.

UPnP 홈네트워크의 기술향상을 위해 무선랜 보안,

UPnP 미들웨어 보안 그리고 UPnP 관련 프로토콜에 대해서는 향후 지속적인 연구가 필요하다.

참고문헌

[1] Linux SDK for UPnP Device 1.04, Open Source UPnP Development Kit, http://upnp.sourceforge.net
[2] XML Signature Syntax and Processing (Second Edition), http://www.w3.org/TR/xmldsig-core/
[3] Single Download File for UPnP™ Documents , 2008, http://www.UPnP.org
[4] UPnP, UPnP Security Ceremonies Design Document, 2003. 10, http://www.UPnP.org
[5] UPnP, DeviceSecurity:1 Service Template, 2003. 11 , http://www.UPnP.org.
[6] UPnP, SecurityConsole:1 Service Template, 2003. 11, http://www.UPnP.org
[7] 이동근, 임경식, 박광로, UPnP 보안 모델의 설계 및 구현, 정보통신설비학회 논문지 1 권 2 호, 2002.
[8] 오임걸, 이종일, UPnP 홈네트워크 보안 취약점에 관한 연구,한국산업정보학회 논문지 제 12 권 제 2 호, 2007.
[9] 김동희, 임경식, 이화용, 안준철, 조충래, 박광로, 댁내 디바이스의 원격제어를 위한 UPnP 프록시 시스템, 정보과학회논문지:컴퓨팅의 실제 10 권 제 4 호, 2004.
[10] 염흥열, 홈네트워크 보안, 표준기술동향, TTA journal No.109, 2007.
[11] 이종후, 이명선, 류재철, AP 인증 및 동적 키 분배를 이용한 안전한 무선랜 시스템 구현, 정보처리학회논문지 C 제 11-C 권 제 4 호, 2004.
[12] 송일규, 홍충선, 이대영, 무선LAN 환경에서 단말 이동시 전송되는 AP간 WEP키 전송 개선 방안, 정보처리학회논문지 C 제11-C권 제2호, 2004