Universal Pwn n Play

Martin Zeiser - Cisco Talos Researcher
Aleksandar Nikolić - Cisco Talos Researcher

www.talosintel.com
Agenda

● UPnP Overview
● UPnP Attacks
● Finding UPnP Devices On The Internet
● Client-side Vulnerabilities - New UPnP Threats
● Defense
● Conclusion
An Overview Of UPnP
What Is Universal Plug and Play (UPnP)?

- It’s a set of protocols which allows devices such as computers, printers, routers, or cameras on a network to discover each other’s presence and establish network services for data sharing, communications, and entertainment.

- The main intention behind UPnP is residential networks without enterprise-class devices.

- Designed by the UPnP Forum in 1999 (Microsoft)

- It works with a combination of SSDP, HTTP, SOAP, and XML.
How does it work?

• Addressing
• Discovery
• Description
• Control
• Eventing
• Presentation
Communication - Finding Devices

Frame 1: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits)
Ethernet II, Src: Vmware_97:2d:db (00:0c:29:97:2d:db), Dst: IPv4mcast_7f:ff:fa (01:00:5e:01:00:01)
Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 239.255.255.250
User Datagram Protocol, Src Port: jstel (1064), Dst Port: ssdp (1900)
HTTP Transfer Protocol
- M-SEARCH * HTTP/1.1
- Host:239.255.255.250:1900
- ST:upnp:rootdevice
- Man:"ssdp:discover"
- MX:3
HTTP/1.1 200 OK
LOCATION: http://192.168.1.1:49000/igddesc.xml
SERVER: FRITZ!Box WLAN 3170 UPnP/1.0 AVM FRITZ!Box WLAN 3170 49.04.58
CACHE-CONTROL: max-age=1800
EXT:
ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1
USN:
uuid:75802409-bccb-40e7-8e6c-001F3FE45B43::urn:schemas-upnp-org:device:InternetGatewayDevice:1
Communication
HTTP Stage
The HTTP Request

TCP/HTTP to specified server

Retrieve specified XML file

• Different device types (there is more than just IGD):
  • IGD (Internet Gateway Device)
  • AV (MediaServer and MediaRenderer aka DLNA)
  • HVAC (Heating / Ventilation / Air conditioning)
  • more
HTTP/1.0 200 OK
Content-Type: text/xml
Connection: close
Content-Length: 2669
Server: MMC_Tech AP miniupnpd/1.0 UPnP/1.0

<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
  <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>

  <device>
    <deviceType>urn:schemas-upnp-org:device:InternetGatewayDevice:1</deviceType>
    <friendlyName>Gateway Device</friendlyName>
    <manufacturer>MMC Technology</manufacturer>
    <manufacturerURL>http://www.mmctech.com/</manufacturerURL>
    <modelDescription>MMC Technology (MW-2060AP)</modelDescription>
    <modelNumber>2.2.7</modelNumber>
    <modelURL>http://www.mmctech.com/</modelURL>
    <UDN>uuid:12342409-1234-1234-5678-ee1234cc5678</UDN>
  </device>
</root>
Interesting Information

<deviceType> urn:schemas-upnp-org:device:InternetGatewayDevice:1

<friendlyName> Residential Gateway Device

<manufacturer> Linksys Inc.

<modelDescription> Internet Access Server

<modelName> WRT54GS

<modelNumber> v2.07.1
UPnP Attacks
Attack #1 - DDoS
Attack #2 - Change DNS Settings
Attack #3 - Request PPP Username And Password

AND THE PASSWORD IS....
Requesting the PPP Password - UPnP Style #1

```xml
POST /uuid:001c-1013-c2d50200a0a0/WANPPPConnection:1 HTTP/1.1
HOST: 192.168.0.93:5431
SOAPACTION: "urn:schemas-upnp-org:service=WANPPPConnection:1#GetPassword"
CONTENT-TYPE: text/xml; charset="utf-8"
Content-Length: 266

<?xml version='1.0' encoding='utf-8'?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>
    <GetPassword xmlns:u="urn:schemas-upnp-org:service=WANPPPConnection:1"/>
  </s:Body>
</s:Envelope>
```
HTTP/1.1 200 OK
DATE: Thu, 01 Jan 1970 00:35:18 GMT
Connection: Keep-Alive
Server: LINUX/2.4 UPnP/1.0 BRCM400/1.0
Content-Length: 327
Content-Type: text/xml; charset="utf-8"

<?xml version="1.0"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Body>
m:GetPasswordResponse xmlns:m="urn:schemas-upnp-org:service:WANPPPConnection:1">
<NewPassword>ThisIsMyPassword</NewPassword>
</m:GetPasswordResponse>
</s:Body>
</s:Envelope>
Attack #4 - Reset/Change Admin Password
Attack #5
Port Forwarding Requests From The Outside

Talos
Requesting Port Forwarding From A Device

POST /evt/IPConn HTTP/1.1
Host: 192.168.0.1:53033
User-Agent: KTorrent/0.0.0
Content-length: 633
Content-Type: text/xml
SOAPAction: "urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping"

Port Forwarding Security Issues:

Typically No Logging
Works For Both TCP And UDP
Custom Timeout Configurable
Finding UPnP Devices On The Internet
HD Moore’s Scans

HD Moore / Rapid7 / Second half of 2012

- Over 80 million unique IPs were identified that responded to UPnP discovery requests from the internet (2.2% of the Internet)
- Identified over 6,900 product versions that were vulnerable through UPnP
- List includes over 1,500 vendors and only took into account devices that exposed the UPnP SOAP service to the internet
Scanning for UPnP

- UDP banner scan on port 1900 finds UPnP devices, then tries to access advertised XML
- This is a unicast request. Microsoft Windows does NOT reply to them (Tested: WinXP and Win7)
- UDP Port 1900 closed/filtered does not mean it doesn't support UPnP
Software in use

- Unknown SDK 2: 9,226,225
- Unknown SDK 1*: 15,844,075
- MiniUPnP: 19,474,736
- Intel/Portable SDK: 23,660,530
- Other: 12,824,246

- Other
- Intel/Portable SDK
- MiniUPnP
- Unknown SDK 1*
- Unknown SDK 2**
- Net-OS 5.x
- Realtek
- Virata-EmWeb
- Torrent Clients
- Allegro Software
“Over 73% of all UPnP instances discovered through SSDP were derived from only four software development kits.

These include the Portable SDK for UPnP Devices, MiniUPnP, a commercial stack that is likely developed by Broadcom, and another commercial kit that could not be tracked to a specific developer.”

HD Moore
Rapid7
Client-side vulnerabilities
New UPnP Threats
The Notify Packet

NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
SERVER: FRITZ!Box WLAN 3170 UPnP/1.0 AVM FRITZ!Box WLAN 3170 49.04.58
CACHE-CONTROL: max-age=1800
NT: upnp:rootdevice
NTS: ssdp:alive
USN: uuid:75802409-bccb-40e7-8e6c-001F3FE45B43::upnp:rootdevice
Notify Threats - Making Clients Perform Tricks

- Send HTTP Exploit Requests To Local Or Remote Hosts
- DoS Requests
- Advertisement 'Click Fraud'
- Parsing Potentially Malicious XML
User Agents Seen From The Internet

USER-AGENT: Linux/2.6.23.17_stm23_0119-mb680, UPnP/1.0, Portable SDK for UPnP devices/1.6.6

USER-AGENT: Linux/2.6.30, UPnP/1.0, Portable SDK for UPnP devices/1.6.18

User-Agent: UPnP/1.0 DLNADOC/1.50 Platinum/1.0.4.9 (NAS)

User-Agent: SMCD3G-CCR, UPnP/1.0, MiniUPnPd/20130201 (Business Gateway)
Attacking Client Applications
What about the client applications?

- Clients actually using UPnP servers
- Port forwarding – mostly
- Basically, anything peer2peer and more:
  - Torrent clients
  - Cryptocurrency clients/server
  - ...

Client applications using UPnP servers and port forwarding are widespread, especially for peer-to-peer applications such as torrent clients and cryptocurrency clients.
How? SSDP M-SEARCH *

- Discovery by client - on startup usually
- On broadcast IP
- Local servers reply with description location
- Client fetches the description
Let’s see it 1/3

Client app is sending M-SEARCH request to broadcast address
Let’s see it 2/3

Server(s) reply with location of the description.
Let’s see it 3/3

Client does a GET request for the description.
• Same as previously mentioned with NOTIFY
• Client fetches description XML
• Exposes XML parser to attack
• Fun fact: most (all) upnp libs embed their own XML parsers
  − Neat! Less dependencies for embedded systems.
  − Neat! Less audited code for attackers.
• Let’s take a look!
MiniUPnP Client – An UPnP IGD Control Point
- http://miniupnp.free.fr/
- A small, lightweight, self contained library
  - "The compilation is known to work under Linux, FreeBSD, OpenBSD, MacOS X, AmigaOS and cygwin."

• As seen, 2\textsuperscript{nd} most popular server side library
• How about clients?
Highlights

Transmission

Bitcoin

*Until recently*
In case of Tor

After July

Good decision, even though it wasn’t used by default.
MiniUPnPc Vulnerability

- Buffer overflow in the XML parser
- Triggered while parsing the description XML fetched from the server
- Patched as of 1st of October
- TALOS-CAN-0035 - CVE 2015-6031
MiniUPnPc Vulnerability

Set the data buffer and callbacks and then call the parser

```c
parser.xmlstart = buffer;
parser.xmlsize = bufsize;
parser.data = data;
parser.starteltfunc = IGDstartelt;
parser.endeltfunc = IGDendelt;
parser.datafunc = IGData;
parser.attfunc = 0;
parsexml(&parser);
```
MiniUPnP PC Vulnerability

struct IGDdatas {
    char cureltname[MINIUPNPC_URL_MAXSIZE];
    char urlbase[MINIUPNPC_URL_MAXSIZE];
    char presentationurl[MINIUPNPC_URL_MAX_SIZE];
    .....  
};

IGDdatas is a struct with static size buffers.
MINIUPNPC_URL_MAXSIZE is 256.
void IGDstartelt(void * d, const char * name, int l) {
    struct IGDdatas * datas = (struct IGDdatas *)d;
    memcpy( datas->cureltname, name, l);
    datas->cureltname[l] = '\0';
    datas->level++;
    if( (l==7) && !memcmp(name, "service", l) ) {
        datas->tmp.controlurl[0] = '\0';
        datas->tmp.eventsuburl[0] = '\0';
        datas->tmp.scpdurl[0] = '\0';
        datas->tmp.servicetype[0] = '\0';
    }
}
Exploitation

- Run a (fake) server on a LAN
- Victim starts up an application
- Application does M-SEARCH for discovery
- Server replies with an URL
- Application fetches the XML and starts parsing it…
- Pwn3d!
DEMO

bitcoind seemed like a nice target…
Defense
Snort Rules

1917: M-Search to UDP 1900

10475: Microsoft Windows UPnP notification type overflow attempt

1388: Microsoft Windows UPnP Location overflow attempt

25780: MiniUPnPd ExecuteSoapAction buffer overflow attempt
Defense

• General sanity – Do not listen for UPnP traffic on WAN interface

• Port forwarding request should only be allowed to self, not a third party

• Patches. But who really patches home routers and embedded devices?
Conclusion
Thank you!

“Thats all Folks!”

www.talosintel.com