UPnP mapping

Daniel Garcia
(FormateZ)
Toor.do
Introduction

• Who am I?

• What is UPnP (Universal Plug and Play)?

• What is an IGD (Internet Gateway Device)?

• How many IGD devices are on line?
UPnP hacking timeline

2001 – Ken from FTU – Three windows UPNP DoS attacks

2001 – Eeye – Multiple remote BoF XP/ME/98

2003 – Björn Stickler - Netgear FM114P UPNP information Disclosure

2006 – Armijn Hemel (www.upnp-hacks.org)

2008 – GNUCitizen(Adrian Pastor, Petko Petkov)
Main problems

- It uses the words “Plug and Play”
- No authentication
- Most stacks don't validate data
- Allowing indiscriminate WAN requests
- Some devices don't log UPnP requests
## Devices affected (So far)

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linksys</td>
<td>WRT54GX</td>
<td>&lt; 4.30.5</td>
</tr>
<tr>
<td>Edimax</td>
<td>BR-6104K</td>
<td>&lt; 3.21</td>
</tr>
<tr>
<td>Sitecom</td>
<td>WL-153</td>
<td>&lt; 1.39</td>
</tr>
<tr>
<td>Speedtouch/Alcatel/Thomson</td>
<td>5x6</td>
<td>&lt; 6.2.29</td>
</tr>
<tr>
<td>Thomson</td>
<td>TG585 v7</td>
<td>&lt; 7.4.3.2</td>
</tr>
</tbody>
</table>
Umap / What is it?

- SocksV4 proxy server that automatically forward's Requests through UPnP devices
- TCP/UDP scanner for hosts behind an IGD NAT
- Manual port mapper for UPnP devices
Umap / How does it work?

UPnP protocol v1.0 steps excluding the Addressing, Events and Presentation steps.

**Discovery**
- Discovery of devices through SSDP packets (Multicast/UDP)
  - **Step 1**

**Description**
- HTTP fetch of the device XML description (HTTP/SOAP)
  - **Step 2**

**Control**
- HTTP SOAP requests to execute UPnP actions
  - **Step 3**

**Steps used by Umap**
- Skipped
  - **Step 1**

- Discovery/description
  - **Step 2**

- Control
  - **Step 3**
Umap / How does it work?

Start

- Scan for UPnP/IGD WAN control points

Handle SOCKS request

If Positive UPnP

- Attempt to add port mapping on UPnP device

Queue request

Open connection and forward traffic to host

Attempt to delete port mapping
Umap / How does it work?

Start → Scan for UPnP/IGD WAN control point → Guess Internal LAN IP block → Add port mapping from WAN port to LAN port → TCP scan mapped port → Report open port → Delete port mapping
UPnP mapping cons

- UPnP stacks are buggy/unstable
- Limited bandwidth
- Protocols with heavy amounts of connections don't work well
- Some devices actually report having the port mapping functionality, but don't do anything
Umap Demo

SOCKS Proxy mode
Umap Demo
Internal LAN scanning
Umap Demo
Manual port mapping
Mitigation

- Disabling UPnP actions from being executed on the WAN
- Operators using base configurations with UPnP disabled
- On some cases, disabling UPnP (things might break)