Attacking UPnP

The useful plug and pwn protocol

- Arron "finux" Finnon
- www.finux.co.uk
- finux@finux.co.uk
- www.twitter.com/f1nux
- www.facebook.com/finux

BsidesVienna June 18th 2011

Outline

What is UPnP?

Setting the scene

The Hacks

Tunneling

Potential Attacks

Software and Device that use UPnP

The Future

Conclusions

News

Q&A

Intended Audience!

You guys

Thanks for voting

So who am i

Good question, up until recently i was a student at the university of Abertay Dundee, studying Ethical Hacking and Countermeasures. During my studies i took a year out and did some consulting. I have also been involved with podcasting for a few years, and have given a number of talks over the years with regards to Linux, Hacking and Security. I've just recently joined the NodeZero_Linux development team. You can catch my podcast at www.finux.co.uk

Feel free to follow me on twitter, or drop me an email. I'm mostly harmless but some may disagree.

What is UPnP????

Its that thing you turn off! Or that's what you all say to me.

UPnP, is really a bunch of networking protocols designed to allow a seamless integration between other UPnP devices. It allows Skype to talk to a home router and open up ports. Yeah you heard me, its allow's ports to be opened up in the context of a Internet Gateway Device (IGD), aka home router. That is UPnP enabled of course.

But it is capable of a lot more

Setting the scene

So as i have said i do a few talks, and recently did one at the Universities hacking society on passively capturing packets on a wireless network. There is a number of open wireless networks around me.

I noticed a large number of SSDP packets (Simple Service Discovery Protocol). It turns out my neighbours own a couple of iPhones. At first i thought that it might be an interesting way of ennumerating some devices on a network. I quickly learned i could do much more.

So what did I learn?

UPnP Enabled, because fearless /b/tard needed a new name!

Where my research took me

That an attacker can gain a lot of information about UPnP devices on the network.

That UPnP is friendly, it doesn't ask questions. It just does as told.

UPnP solved problems with authentication, by not using it.

Where's the hacks, bro???

Dynamic port mapping

So in essence it is the process of taking an internal network resource and allowing it traffic out. This is really a firewall/access rule.

Internet 5060:SkypeClient:5060 LAN

So things to remember here, Skype speaks to the router and asks for it to open port 5060 on the router, and map that traffic to port 5060 on the client.

Notice there isn't a request for a password.

For you to do this, you would “logon” to the router and write the rule.

Where's the hacks, bro???

Dynamic port mapping

Now here's an interesting point, you can within the protocol ask for a map for a different IP address. Yeah you heard right.

So this is a completely legit

Internet 1337:192.168.0.1:80 LAN

So I can legitimately map traffic from the internet on port 1337, to the internal LAN side of port 80 on 192.168.0.1

Where's the hacks, bro???

Dynamic port mapping

Hmmm what about;

53:192.168.0.1:53

Okay, this is pretty cool.

Pinpoint Dynamic port mapping

This is when you setup mapping to a specific external address .i.e

EvilServer.ru <<< 53:192.168.0.1:53

Where's the hacks, bro???

Other attacks worth mentioning

Malware > MIME types > Icon

Each device has an XML scheme detailing what the UPnP device is capable of doing. The device may have an icon. However nothing stops those resources from being requested outside the network

Window's will display the icon from the XML.

DoS > Lots of Port Maps > occupy RAM/NVRAM of IGD

Routers really only have a finite amount of memory

Lets just occupy as much memory as we can.

GNUCitizen.org

I have no idea why British Telecom thought this was a good idea.

But BT Home Hub's allowed for DNS server setting to be updated via UPnP

Yeah, you got it. They allowed a protocol that doesn't support authentication to change DNS settings.

GNUCitizen conducted a Flash Based XSS that did something very similar 2 years ago

Conficker

Its reported that conficker had UPnP

Why not. I would much prefer to ask the router than do some crazy tunnelling

What uses It????

- UPnP Enabled Devices
  - A lot of home routers have it enabled by default
  - Games consoles use it
  - MSN Messenger(tm) uses it
  - Skype(tm) Uses it
  - Printers
  - Smart Phones
  - Storage Devices
  - Home entrainment systems
  - Torrents clients for randomising ports
  - And of course home computers

Some management tools for it

- upnp-router-control
  - A Linux tool for configuring a home router
- upnp-inspector
  - A tool for examining UPnP device
- Miranda
  - UPnP administration tool written in Python
- UPnP-Popper
  - ??????????

Conclusions

- Now easy to consider your networks, but what about these external networks that I may have been on before you!
- Yeah turn it off, but understand that ”it just works” feeling users like, that's gone. You are going to knock some network functionality out of the gate for some, and of course some people will never notice it.
- I am not too considered with the enemy within, my believe they would get out anyway, its the scripted attacks that scare me. Conficker used UPnP as some of its attack payloads.
- It is not going anywhere, and can be very handy for its users.
- Scary moment but any UPnP enabled device on your network could be a potential attacker.
- Lots of LuLz to be had here.

The UPnP-Popper Project

- So we want to develop an application that is modular in design
- Our aim is to have an alpha release of our tool available September/October
- The project has two supporters

www.calibre-secure.net

www.file-away.co.uk

Questions????

- http://www.artima.com/spontaneous/upnp_digihome.html
- http://www.gnucitizen.org/blog/flash-upnp-attack-faq/
- http://www.gnucitizen.org/blog/bt-home-flub-pwnin-the-bt-home-hub-5/
- http://www.gnucitizen.org/blog/hacking-with-upnp-universal-plug-and-play/
- https://www.kb.cert.org/vuls/id/347812
- http://www.techrepublic.com/blog/tech-news/severe-upnpflash-vulnerability-disco
- http://support.microsoft.com/kb/944993
- http://en.wikipedia.org/wiki/Zero_configuration_networking
- http://www.gnucitizen.org/blog/hacking-the-interwebs/

- The END