UPnP Revisited

The useful plug and pwn protocol

Arron “finux” Finnon

BSidesLondon 25/04/12

Disclaimer

Expect The Following:

- Bad Language
- Mild Ranting
- Some Technical Stuff
- Plenty of Lulz
- Some Pwnage
- Jail Time If You Hack Someone

Today's Outcomes

What you should leave with

UPnP Is Inherently Insecure

Shit be batshit insane bro!!!!

Arron “finux” Finnon

BSidesLondon 25/04/12

UPnP Is Hard To Mitigate

Disabling it will not fix it!

Arron “finux” Finnon

BSidesLondon 25/04/12

How You Can Audit UPnP

Yeah right, show me the hacks!

Arron “finux” Finnon

BSidesLondon 25/04/12

So What Is UPnP

You know, its the thing you all disable

One Definition for UPnP:

"A protocol that allows devices on a network to communicate with each other seamlessly"

bittorrent.com

Another Definition of UPnP:

"Its like a dynamic firewall protocol"

Lee Hughes - BSidesVienna 2011

Seamless Interconnectivity

Fancy way of saying "linking shit together"

Arron "finux" Finnon

BSidesLondon 25/04/12

The First Gotcha - Seamlessly

another way of saying no validation

Arron “finux” Finnon

BSidesLondon 25/04/12

THE TRUSTING PROTOCOL

Well in most cases your on the network. Which Obviously means your welcome to make UPnP requests

Lack of Authentication

It's a pretty big issue

Many UPnP Implementations

Its everywhere, no where is safe!

Arron “finux” Finnon

BSidesLondon 25/04/12

Examples

Personal Computers

Skype

Torrent Clients

Windows

PS3

Smart Phones

Printers

MSN

Internet Gateways

VoIP

Media Servers

iPhones

Wifi Access Points

How Does It Work

This will be the techie bit

UPnP Process

0 - Addressing

Addressing methods used by devices in addition to rules being established for devices that are unable to obtain an address through DHCP.

1 - Discovery

Announcements using SSDP. Devices send multicast search requests using HTTPU. Control points respond with HTTPU packets that specify a location for the XML description file.

2 - Description

After the discovery of the XML description file location, the device downloads the XML to discover the different services and actions that the device has available

3 - Control

Through the description process, vital information for interaction with the control point is delivered. SOAP requests are sent to the specified control points, different functions are executed. This is where the actual execution of the actions like port mapping happen.

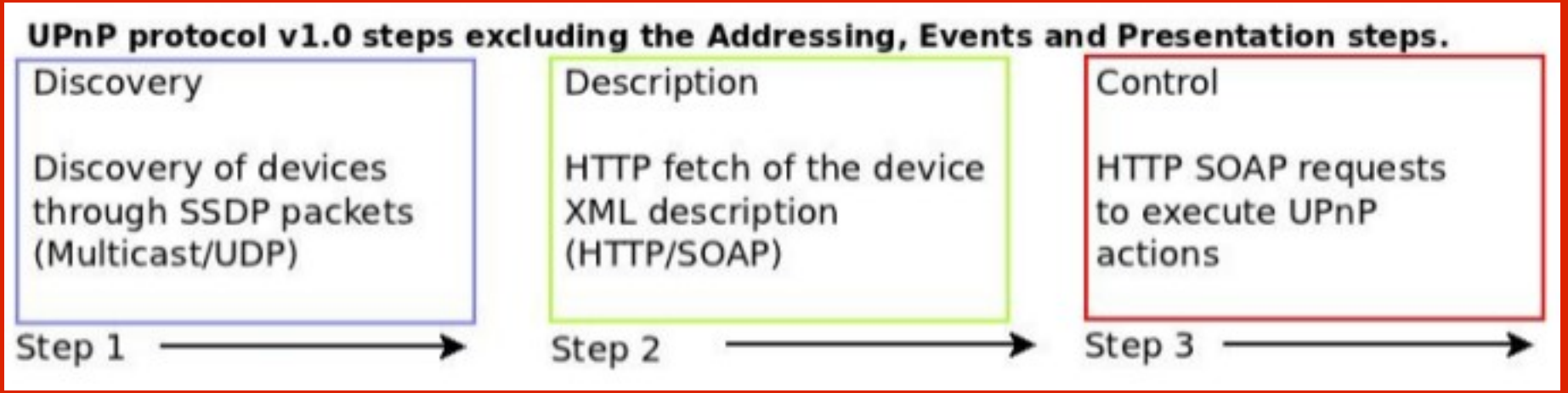
4 - Eventing

Control points listen to changes in devices.

5 - Presentation

The referral to an HTML-based user interface for controlling and/or viewing the device status.

Simple Process



Discovery, Description, Control

Abilities Detailed By XML

Ask and you shall receive

Arron “finux” Finnon

BSidesLondon 25/04/12

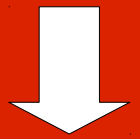
Example XML

I'll fire up the description files!!!

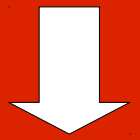
How It Is Used In Practice

You know, its intended use

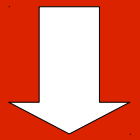
Skype: Ding, Ding, Service Please



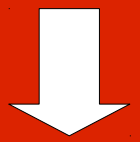
IGD: What Can I Do For You Today



Skype: I would Like A Port Please, and its traffic please.



IGD: Sure, what table are you at?



Skype: I'm sitting at 192.168.1.100

*IGD = Internet Gateway Device - aka router

The Second – Gottcha

In most cases the data supplied is trusted

UPnP Hack Number 1

I talked about this last year

Dynamic Port Mapping

That's what an app opening a port on a IGD is called

A Port Map Looks Like This:

TCP 30331->192.168.1.100:30331 'Skype'

So the IGD has opened port 30331 externally
and is filtering traffic to port 30331 internally
to 192.168.1.100

The Issue In Play

We supply the IP address

Think About This:

TCP 1337->192.168.1.1:80 'pwn3d'

So the IGD has opened port 1337 externally and is filtering traffic to port 80 internally to 192.168.1.1

That Is Just The Beginning

I've banged on enough about what it is

Its Has Long A Long History

As far back as '99

The UPnP Forum

Guess what? It was set up by Microsoft

Its Insecurity Time Line

2001 - Multiple DoS attacks in Windows UPnP Stack

2001 - Multiple BoF in Windows UPnP Stack

2003 - Stickler Discusses UPnP information Disclosure

2006 - Hemel Starts www.upnp-hacks.org

2008 - GNUCitizen Totally Pwn's BT HH

2011 - Finux Goes To BSidesVienna to Chat About UPnP

2011 - Garcia - Some IGD will accept remote Commands

2011 - Kaminsky - He also did some UPnP shit!

2012 - You guys voted to hear about UPnP hacking

So Lets Get Some Meat On It

Example time!!!!!

I'm Gonna Show Some Videos

These tools are in Ubuntu Repositories

*Unless Otherwise Stated

Arron "finux" Finnon

BSidesLondon 25/04/12

So What Did Garcia Discover

That UPnP devs batshit inane!

Arron “finux” Finnon

BSidesLondon 25/04/12

Remote IGD UPnP Command

Yeah, you read that right!

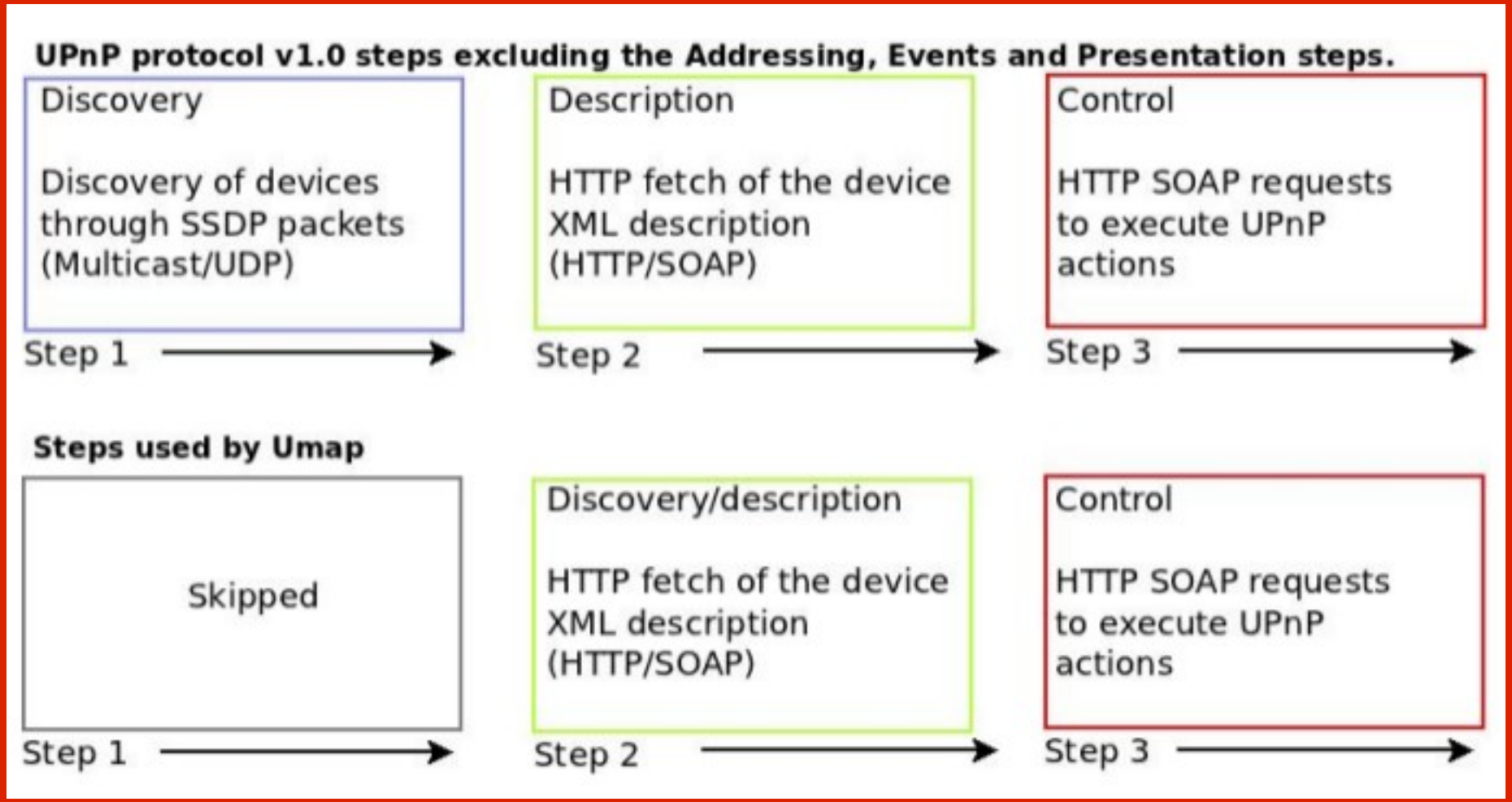
Arron “finux” Finnon

BSidesLondon 25/04/12

The Guilty Parties

Manufacturer	Model	Version
Linksys	WRT54GX	< 4.30.5
Edimax	BR-6104K	< 3.21
Sitecom	WL-153	< 1.39
Speedtouch/Alcatel/Thomson	5x6	< 6.2.29
Thomson	TG585 v7	< 7.4.3.2

UMap Flow Process



Conclusion Time

Hang on tight!!!!

Why You So Insecure!

It Will Never Be Secure

My Final Thoughts

Thanks BSidesLondon

Ask question, buy me beer!

Contact Details

Email : finux@finux.co.uk

Twitter : www.twitter.com/f1nux

Podcast : www.finux.co.uk

Linked in :
http://uk.linkedin.com/in/finnon