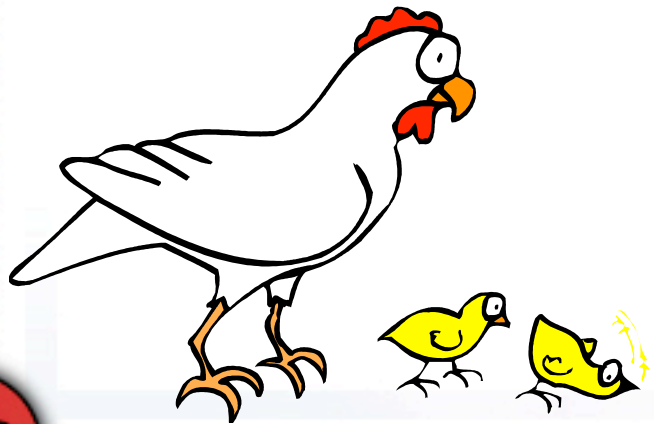


A Fox in the Hen House

UPnP IGD

Jonathan Squire, CISSP

Big Brain Labs



Black Hat Briefings

Black Hat Briefings, August 8, 2008
v1.1.0



Agenda

- Always popular disclaimer
- Intro to UPnP
- UPnP IGD profile
- Demos
- Why this works
- Future research





Important Disclaimer

(Pay Attention)

- This project is my own personal research and is not sponsored by anyone but me.
- If you break something you get to keep the pieces.
- No routers were harmed in the creation of this presentation.





Introduction to UPnP

- Goal of UPnP + SSDP
 - Allow devices to easily self organize and configure on a home network
 - DHCP or Reserved Space (169.254.0.0)
- Based on common standards
 - TCP, UDP, Multicast, XML, SOAP, HTTP





Finding Targets (SSDP)

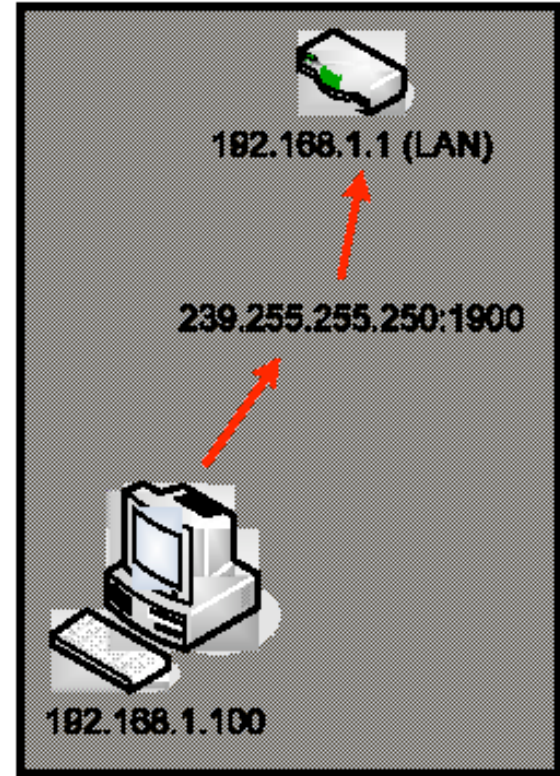
- 239.255.255.250:1900
- M-SEARCH
 - Control point initiated search
 - Responses come back via UDP Unicast
 - Responses contain Location URL
- NOTIFY
 - Periodically sent by UPnP devices





M-SEARCH

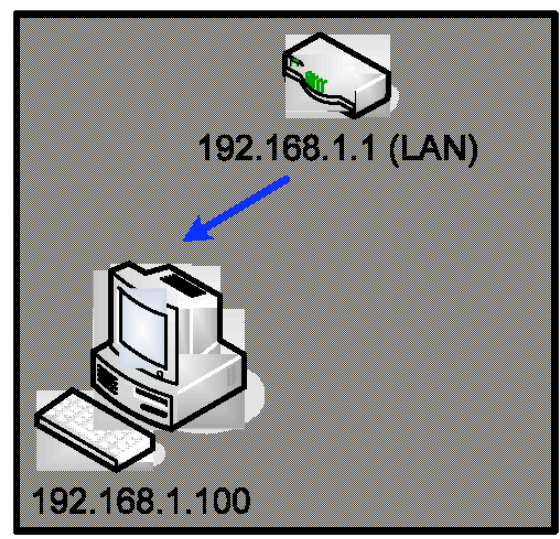
M-SEARCH * HTTP/1.1
ST: ssdp:all
MX: 5
MAN: ssdp:discover
HOST: 239.255.255.250:1900





M-Search Response

HTTP/1.1 200 OK
ST: upnp:rootdevice
USN: uuid:13529010-1ad7-10c2-9abc-001cc33fa2ca::upnp:rootdevice
EXT:
SERVER: VxWorks/5.4.2 UPnP/1.0 iGateway/1.1
LOCATION: http://192.168.1.1:2869/IGatewayDeviceDescDoc
CACHE-CONTROL: max-age = 126
Content-Length: 0





NOTIFY

NOTIFY * HTTP/1.1

HOST: 239.255.255.250:1900

LOCATION: http://192.168.1.1:2869/IGatewayDeviceDescDoc

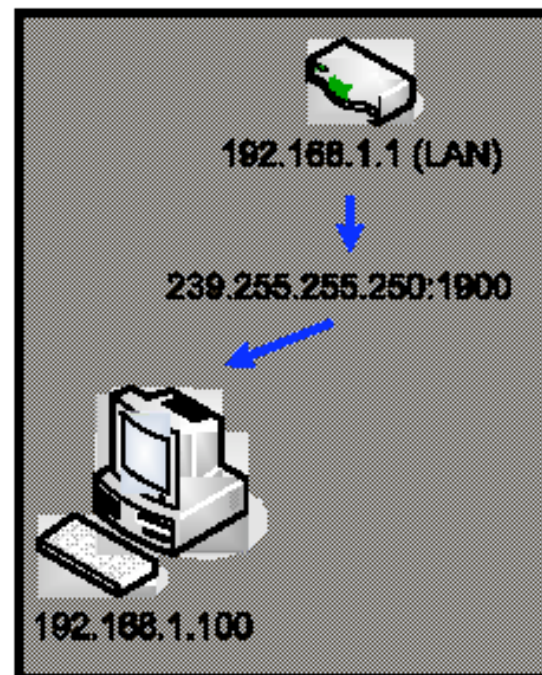
USN: uuid:13529010-1ad7-10c2-9abc-001cc33fa2ca::upnp:rootdevice

SERVER: VxWorks/5.4.2 UPnP/1.0 iGateway/1.1

NT: upnp:rootdevice

NTS: ssdp:alive

CACHE-CONTROL: max-age = 126





What now?

- Pull description XML file from Location
- Description file contains “Services”
 - `<serviceType></serviceType>`
 - `<serviceId></serviceId>`
 - `<controlURL></controlURL>`
 - `<eventSubURL></eventSubURL>`
 - `<SCPDURL></SCPDURL>`





What now?

- For each service
 - Pull SCPDURL via HTTP
 - Parse description for actions
 - Send SOAP messages to Control URL
 - Have Fun.





What is UPnP IGD

- Internet Gateway Device profile
- Attempts to simplify network connectivity and configuration for client systems.
- Allows client systems to request firewall rule modifications so services such as chat and gaming work





Can I log into your router?

- NO!
- *Ok, I'm assuming you changed the default username and password.





That's OK, I'll do it myself

- WANIPConnection:1
- WANPPPConnection:1
 - AddPortMapping(NewRemoteHost, NewExternalPort, NewProtocol, NewInternalPort, NewInternalClient, NewEnabled, NewPortMappingDescription, NewLeaseDuration)





Demonstration Network



Demonstration 1

Adding a forward rule to the router





So... what happened?

- Found an IGD via SSDP M-Search
 - `n.discover("urn:schemas-upnp-org:device:InternetGatewayDevice:1")`
- Found service description for:
 - `WANIPConnection:1`
- Sent a SOAP message to add a forward
 - `s.AddPortMapping("",1234,"TCP",1234,"192.168.1.123",1,"UPnPwn",0)`
- Success





And this is bad?

- Ummm... Yeah.
- No authentication
- No user notification
- Any internal host can request a forward “on behalf of” any other inside host





Some more fun with AddPortMapping

- Forward to any internal host (LAN side)
- Forward to any host (on WAN side)
 - Some firmware is so broken they define “NewInternalHost” as ANY.
- Forward to the admin interface from the outside
- DoS (fill forwards table)



Demonstration 2

What does the router owner see?





Is this bad?

- Forwarding rules that aren't listed in any obvious place? You tell me.
- Most users don't check their rules anyway, but if they do, they get a false sense of security.
- Does your mom know how to run nmap?





Is this bad? Or worse?

- Some devices save these rules to flash
- Some devices show you the rules, but you can't change them unless you use UPnP



Can we do anything?

- Turn off UPnP
 - Don't forward "on behalf of" anybody else
 - Modify UPnP Servers to only trust specific hosts
 - This breaks part of the spec, but in practice isn't really a problem
 - Implement UPnP Device Security and Security Console Profiles (maybe)
 - Simplified key system for updates (token)
 - Would require modified UPnP client and server
 - Should run over SSL
- Stop buying insecure devices





Some other stuff to scare you

- LANHostConfigManagement:1
 - SetDHCPRelay(NewDHCPRelay)
 - SetIPRouter(NewIPRouters)
 - SetDNSServer(NewDNSServers)
- WANPPPPConnection:1
 - GetUserName()
 - GetPassword()





Be more afraid

linux-igd hack (Credit to: Armijn Hemel <http://www.upnp-hacks.org/>)

- Many devices are based on and old version of Linux IGD project code that has this vulnerability:

```
int pmlist_AddPortMapping (  
char *protocol, char *externalPort, char *internalClient, char *internalPort) {  
char command[500];  
sprintf(command, "%s -t nat -A %s -i %s -p %s -m mport  
--dport %s -j DNAT --to %s:%s", g_iptables,  
g_preroutingChainName, g_extInterfaceName,  
protocol, externalPort, internalClient, internalPort);  
  
system (command);  
...  
}
```

- So, what do you think happens if NewInternalClient="/sbin/reboot"





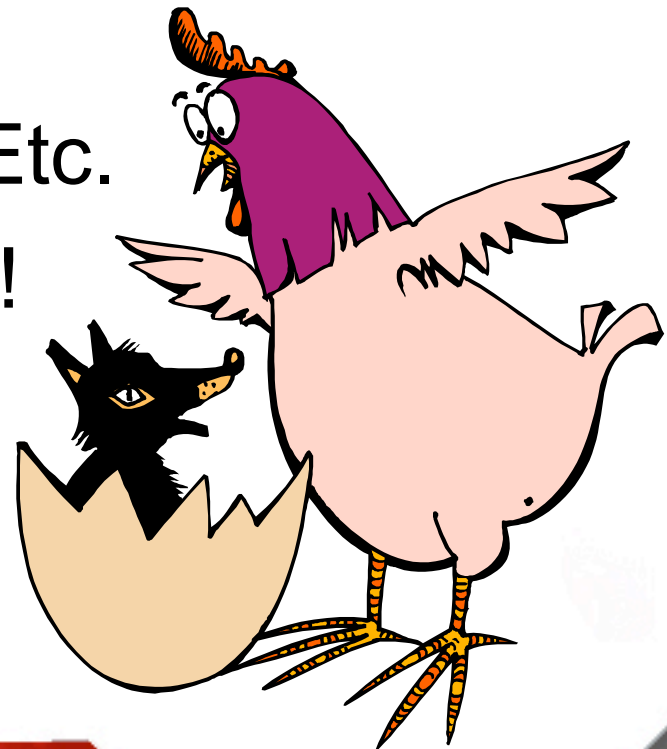
And remember...

- It's a small computer
- It's got a web server
- How many people patch their router?
- Classic flaws exist
 - Format String
 - Buffer Overflow
 - General Input Validation
- They have file systems



Oh, and it's not always local

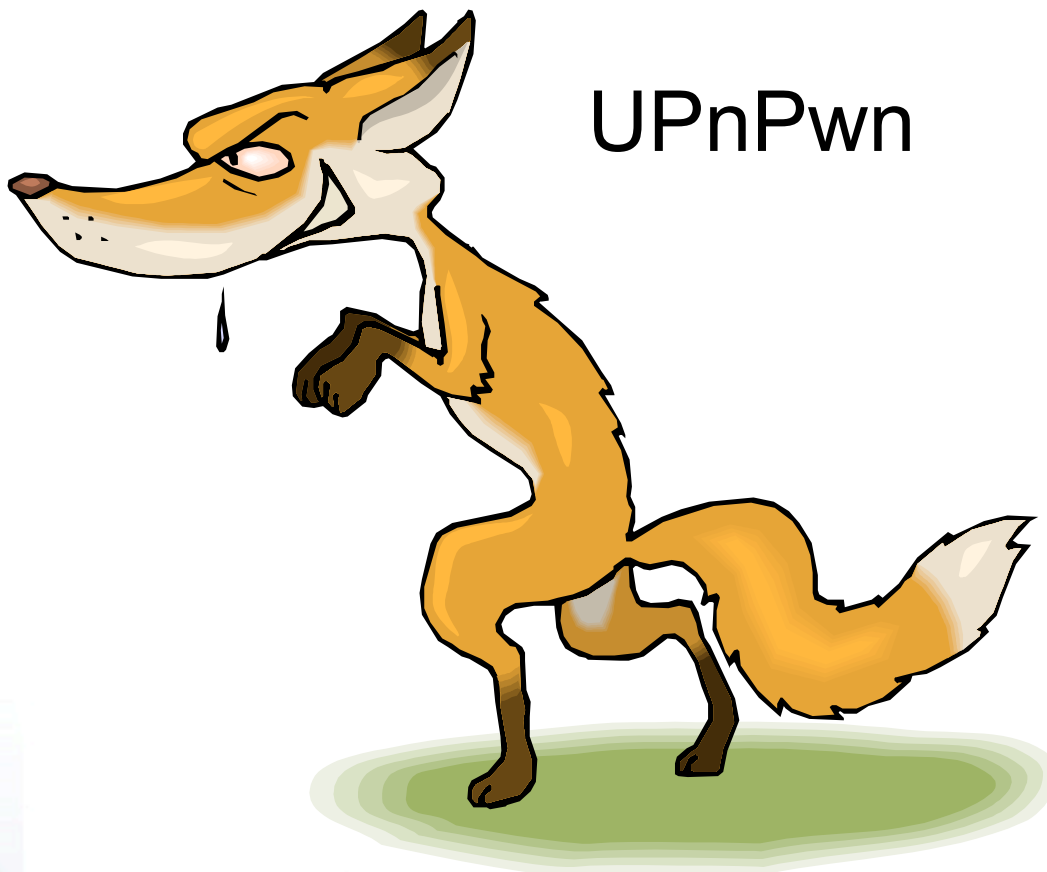
- GNU Citizen Flash UPnP Attack
- XSS
- Worms, Virus, Trojans, Etc.
- UPnP on WAN interface!





Demonstration 3

UPnPwn





Demonstration 4

Do you really know what your gadgets do to help you?





Future Research

- UPnP Stack Fingerprinting
- UPnP Fuzzer
- Code Execution / Buffer Overflows / Re-Flash
- UPnP Watchdog
- Windows Connect Now (WFADevice:1)
- UPnP A/V Profiles
- UPnP HVAC (anybody have one?)
- Other Dynamic configuration protocols





Questions?

Jonathan Squire, CISSP

UPnPwn<at>bigbrainlabs<dot>com





References

- UPnPwn updates and other research
 - <http://www.bigbrainlabs.com/>
- UPnP-hacks (Linux IGD attack)
 - <http://www.upnp-hacks.org/igd.html>
- GNUCitizen Flash UPnP Attack
 - <http://www.gnucitizen.org/blog/hacking-the-interwebs/>
- Crazy Toaster
 - <http://www.drورشalev.com/dev/upnp/toaster/DC-15-Shalev-004.ppt>
- RFCs
 - <http://tools.ietf.org/html/draft-cai-ssdp-v1-03>
 - <http://tools.ietf.org/html/draft-cohen-gena-client-00>
 - <http://tools.ietf.org/html/draft-goland-http-udp-01>
- UPnP Forum
 - <http://www.upnp.org/standardizeddcps/igd.asp>

