

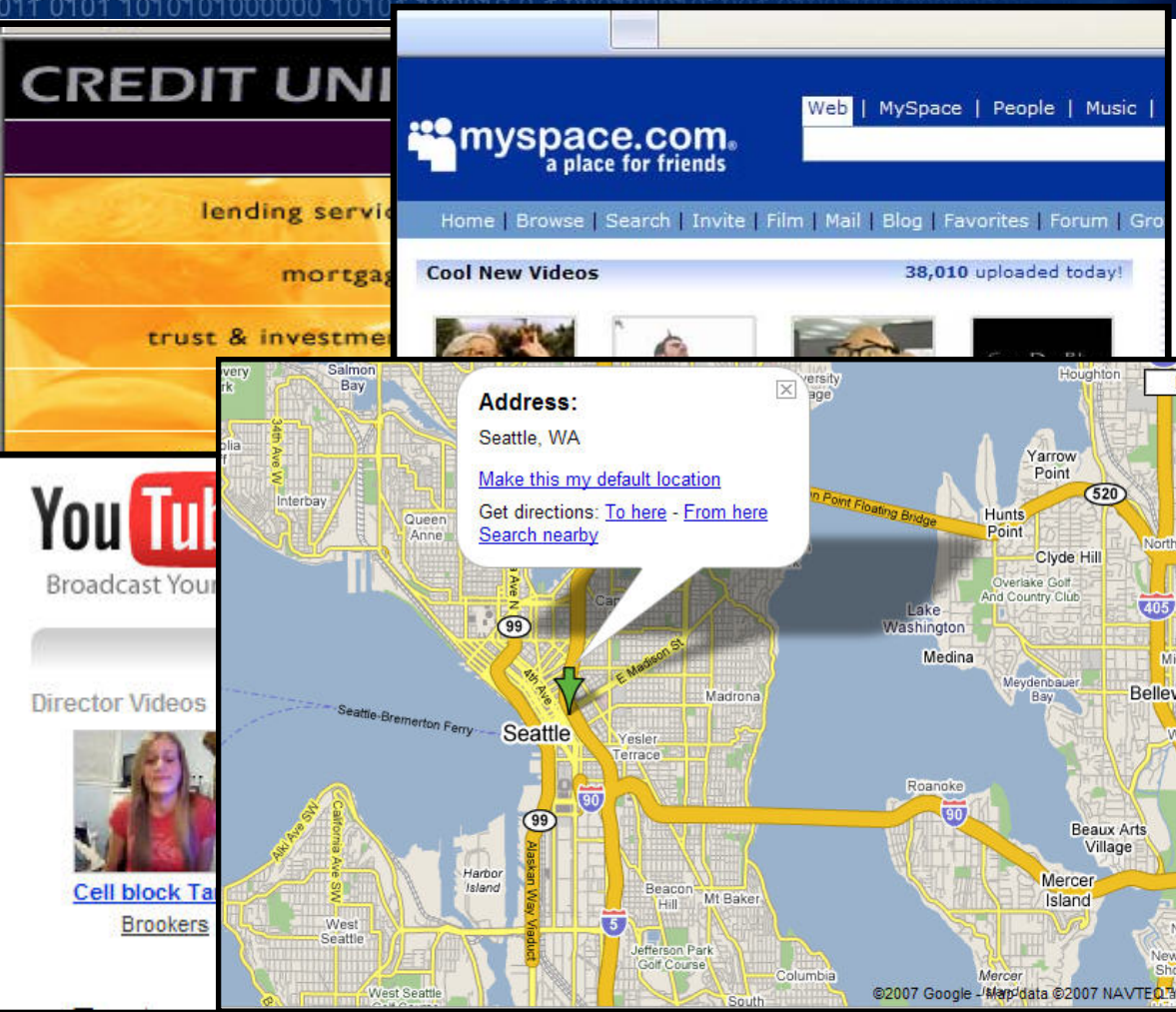


Kicking Down the Cross Domain Door

Techniques for Cross Domain Exploitation

Billy K Rios (BK) and Raghav Dube

Implication of Cross Domain Attacks



Rich Content

Cookies

Mash-ups

Tabbed Browsing

Ajax

JSON

Implication of Cross Domain Attacks

Problem loading page - Mozilla Firefox

File Edit View History Bookmarks Tools Help del.icio.us

http://www.theshadyinternet.com/

CU Online Banking - Account Balance Summary

Below is a summary of your current account balances. This information is as of 5:00 PM EST on 2/26/2007.

Previous Balance	\$ 99994.69
Current Withdrawals	(6999.62)
Current Deposits	4999.73
Current Balance	\$ 97994.80



Attack Foundations

Cross Site Scripting (XSS)

- **Injected Client Code**
- **Cookie Stealing**
- **Browser Hijacking**
- **Web Page Defacement**
- **Hawtness**



Attack Foundations

XSS Example / Demo

Attack Foundations

Cross Site Request Forgery (XSRF)

- Applications Trust
- Parameters, Cookie, IP Space...
- Authenticated Examples
- New Hawthness



Attack Foundations

XSRF Example / Demo



Attack Foundations

XSS meets XSRF

- Using XSS and XSRF together!
- XSSXSSRFSSX?
- Both Have Strengths
- Both Have Weaknesses
- One Armed Boxers

XSS Proxies and Frameworks

XSS Proxy Fundamentals

- Anton Rager – XSS Proxy
- BeEf, XSS Shell, Backframe
- `<script>alert('xss')</script>`
- `<script src = ../proxy.js>`
- Dynamic JavaScript Payloads
- Frames and Control Channels

XSS Proxies and Frameworks

XS-Sniper

- Typical XSS Proxy
- Rendering of HTML
- Organization of Data
- JavaScript Payloads Provided
- Source Code Snippets

Sniper Sniper Scope KeyLogger Nikto Results Scanner Recon Javascript External Attacks Settings Nikto S < >

External Active Payload

```
sniperscope();
```

Dynamic JavaScript
Payload for external.js

External Spotter Payload

```
document.write('<body onload=spotter()>');  
var randomnumber=Math.floor(Math.random()  
*1000001);  
  
function spotter(){  
var  
bigframe=document.documentElement.innerHTM  
L;  
  
iframeHTML='<IFRAME NAME="myFrame" iframe  
id="myFrame" width="50%" height="50%"  
scrolling="auto" frameborder="0"></IFRAME>';  
  
iframeHTML+='<IFRAME NAME="myFrame2"  
iframe id="myFrame2" width="0%" height="0%"  
scrolling="auto" frameborder="0"></IFRAME>';  
  
iframeHTML+='<IFRAME NAME="myFrame3"  
iframe id="myFrame3" width="50%" height="50%"  
scrolling="auto" frameborder="0"></IFRAME>';
```

External Spotter Payload Location

```
C:\Documents and Settings\BK\My Documents\Visua
```

XSS Proxies and Frameworks

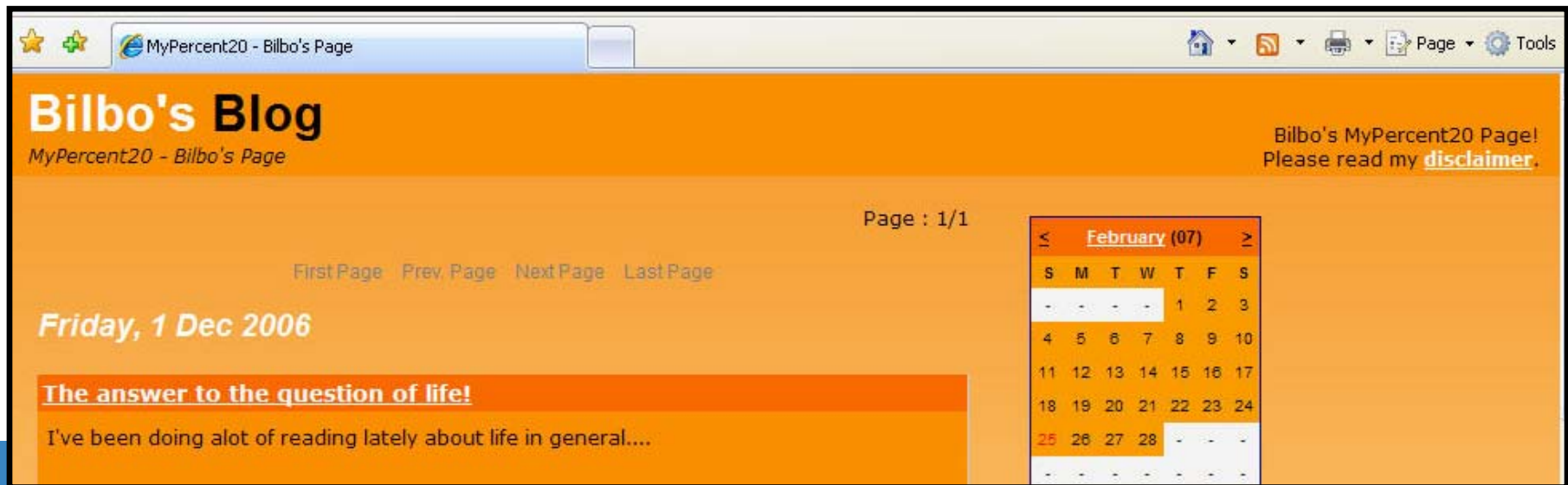
The screenshot shows a Windows Internet Explorer browser window displaying a blog page titled "Bilbo's Blog" on "MyPercent20 - Bilbo's Page". The URL is `http://www.mypercent20.com/MyBlog/Comments.asp?Entry=5`. The page content includes a comment titled "The answer to the question of life!(Comments RSS)" with the text "I've been doing alot of reading lately about life in general....". Below the comment, three frames are highlighted with dashed black borders:

<code>myFrame2</code> (invisible) Control Channel	<code>myFrame3</code> (invisible) Cross Domain Contents	<code>crossDomainPostFrame</code> (invisible) POSTs off Domain
---	--	--

The Attack – The Initial XSS

MyPercent20.com

- Popular Social Networking/Blogging Site
- User Base of Tens of Thousands of Users
- Allows Uploading of HTML and Other Content



MyPercent20 - Bilbo's Page

Bilbo's Blog

MyPercent20 - Bilbo's Page

Bilbo's MyPercent20 Page!
Please read my [disclaimer](#).

Page : 1/1

First Page Prev Page Next Page Last Page

Friday, 1 Dec 2006

The answer to the question of life!

I've been doing alot of reading lately about life in general....

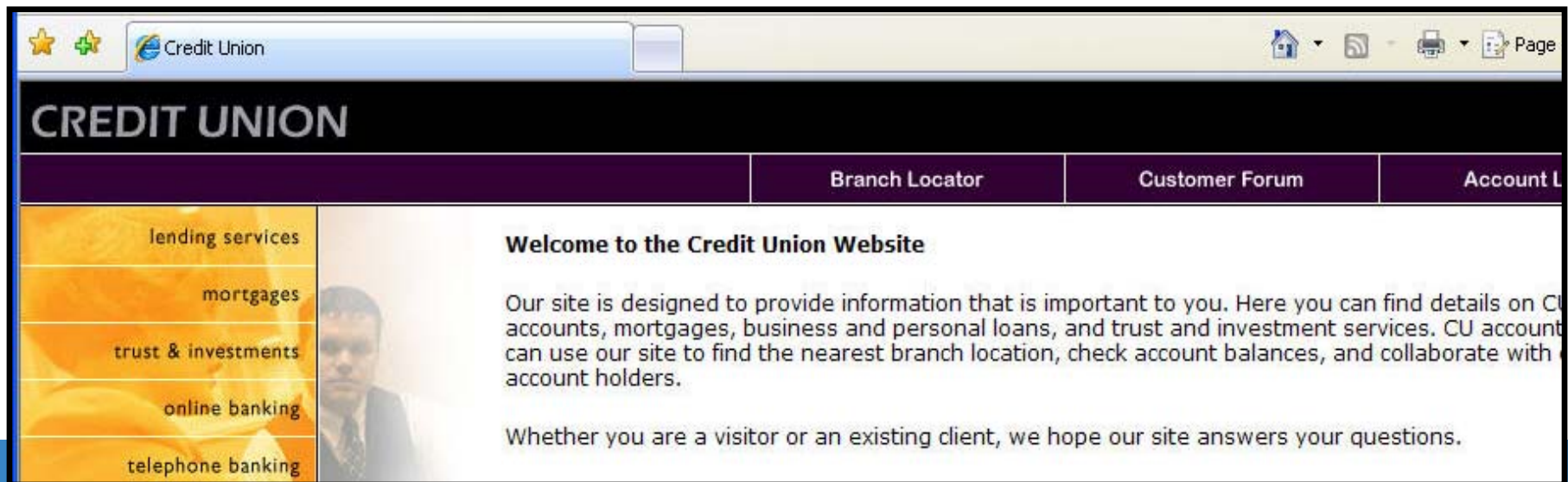
February (07)						
S	M	T	W	T	F	S
-	-	-	-	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	-	-	-
-	-	-	-	-	-	-



The Attack – BigCreditUnion.com

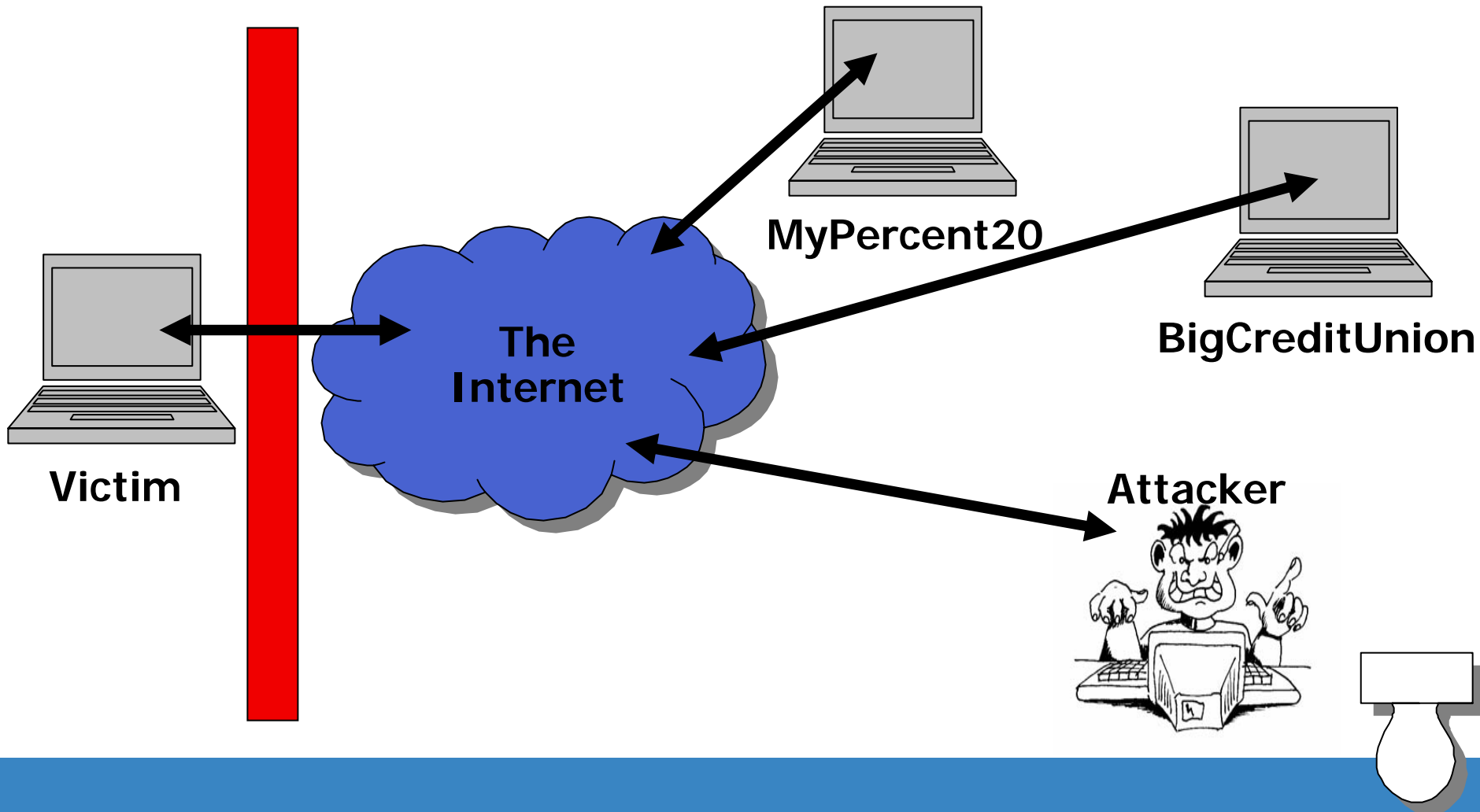
BigCreditUnion.com

- Typical Online Banking Website
- Fictional Credit Union
- Built-in Vulnerabilities for Demo



The screenshot shows a web browser window with the address bar displaying "Credit Union". The website header features the text "CREDIT UNION" in a dark banner. Below the header is a navigation menu with four items: "Branch Locator", "Customer Forum", and "Account L". The main content area is divided into a left sidebar and a main body. The sidebar contains a vertical list of services: "lending services", "mortgages", "trust & investments", "online banking", and "telephone banking". The main body contains a "Welcome to the Credit Union Website" section with a brief description of the site's purpose and a closing statement: "Whether you are a visitor or an existing client, we hope our site answers your questions." The background of the website features a faint image of a man in a suit.

The Attack – BigCreditUnion.com



The Attack – BigCreditUnion.com

Assumptions

- The victim has access to the Internet
- BigCreditUnion.com has an XSS exposure
- The victim is using IE or Firefox



The screenshot shows a web browser displaying the Wiktionary page for the word "assumption". The page layout includes a sidebar on the left with navigation links and a main content area on the right. The main content area features a title "assumption" with tabs for "article", "discussion", "edit", and "history". Below the title, the word is defined in English as a Noun, with a list of four numbered definitions. The definitions are: 1. The act of assuming, or taking to or upon one's self; the act of taking up or adopting. 2. The act of taking for granted, or supposing a thing without proof, supposition; unwarrantable claim. 3. The thing supposed; a postulate, or proposition assumed; a supposition. 4. The minor or second proposition in a categorical syllogism.

Wiktionary
[ˈwɪkʃənri] n.,
a wiki-based Open
Content dictionary

Navigation:
Main Page
Community portal
Requested entries
Recent changes
Random page

article discussion edit history

assumption

English

Noun

assumption (plural **assumptions**)

1. The act of assuming, or taking to or upon one's self; the act of taking up or adopting.
2. The act of taking for granted, or supposing a thing without proof, supposition; unwarrantable claim.
3. The thing supposed; a postulate, or proposition assumed; a supposition.
4. The minor or second proposition in a categorical syllogism.

The Attack – BigCreditUnion.com

Steps to Exploitation

- Target Reconnaissance
- Initial XSS
- Jumping to BigCreditUnion
- Authenticated Attacks
- Unauthenticated Attacks





The Attack – BigCreditUnion.com

DEMO

The Attack – WhatsUP Gold 2006

WhatsUP Gold 2006

- Made by Ipswitch
- Has Known XSS Vulnerabilities
- Found on Corporate Intranets
- Not Limited to WhatsUP Gold
- “Protected by Firewalls!”

The Attack – WhatsUP Gold 2006

Home | Devices | Reports | Add Content | General | Help

Map View Menu

Remote Office

Duplex Printer
Accounting1
Accounting2
TLA Router
Switcheroo
Tauron
WS_FTP Server 6
Caprica
IMail Premium
Acctg. DB

Ping Response Time - Last 4 Hours (Single Device) Menu

HP ProCurve Switch - Network interface: 192.168.3.158

Response Time (ms)

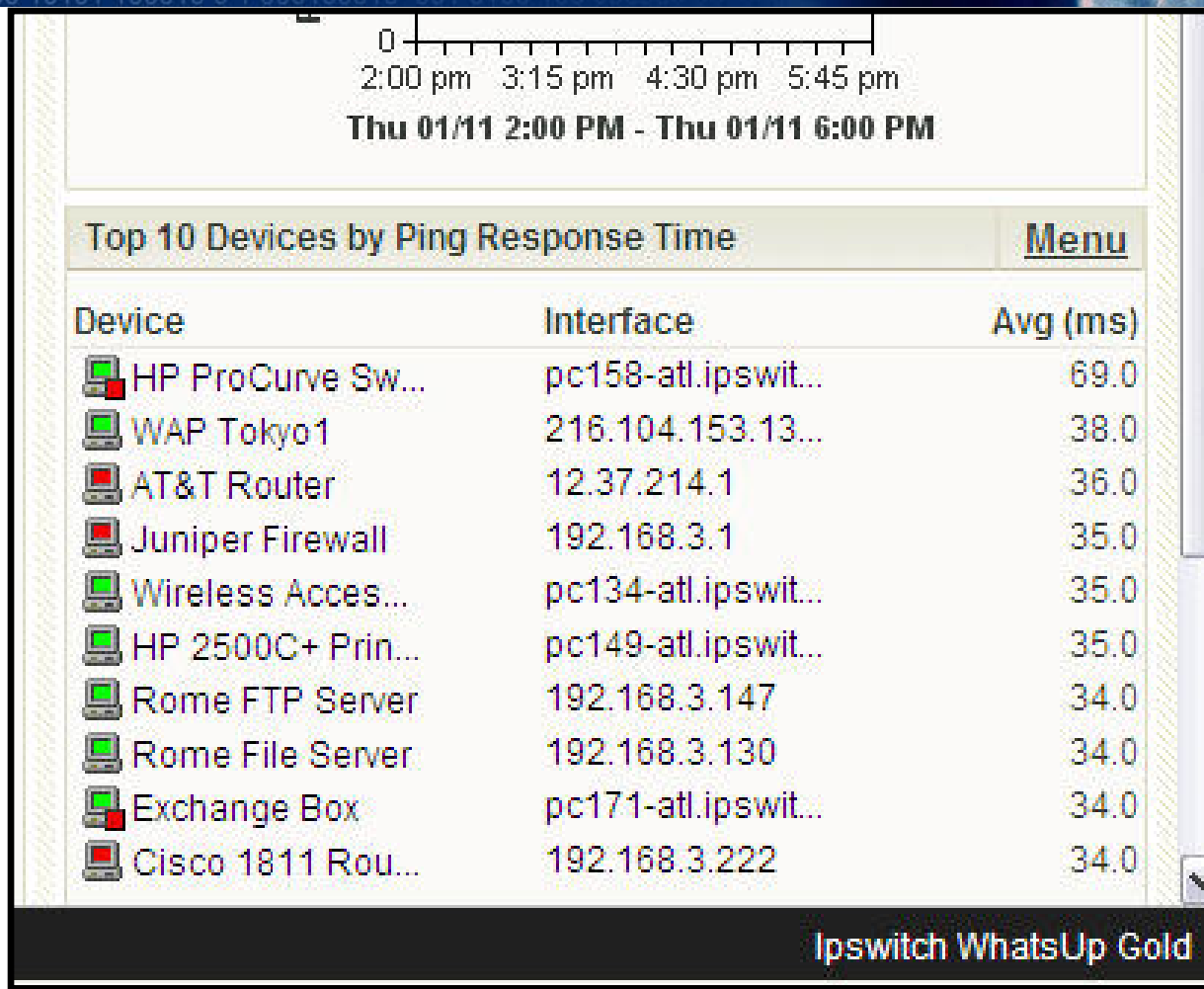
2:00 pm 3:15 pm 4:30 pm 5:45 pm

Thu 01/11 2:00 PM - Thu 01/11 6:00 PM

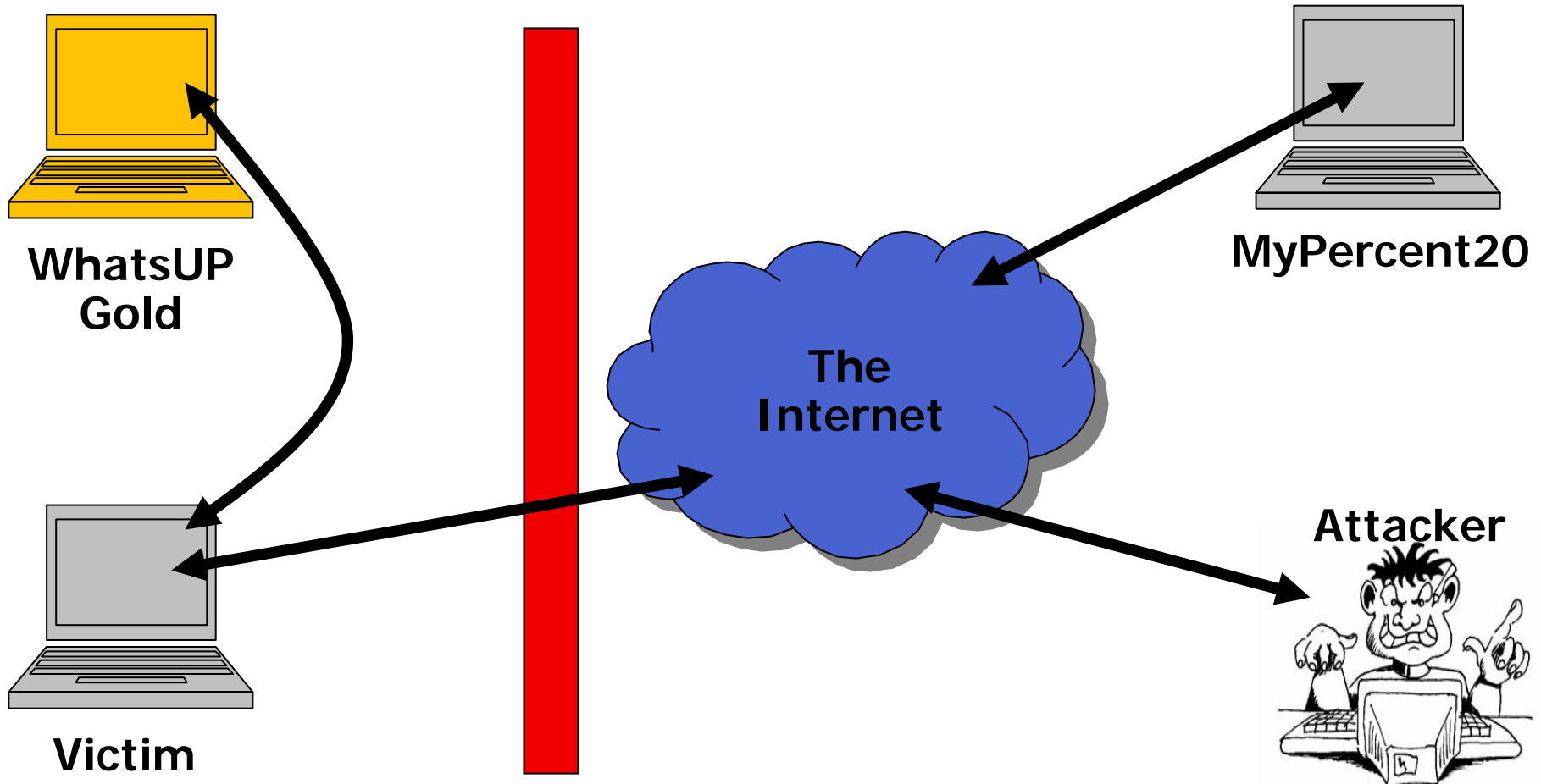
Top 10 Devices by Ping Response Time Menu

Device	Interface	Avg (ms)
HP ProCurve Sw...	pc158-atl.ipswit...	69.0
WAP Tokyo1	216.104.153.13...	38.0
AT&T Router	12.37.214.1	36.0
Juniper Firewall	192.168.3.1	35.0
Wireless Acces...	pc134-atl.ipswit...	35.0
HP 2500C+ Prin...	pc149-atl.ipswit...	35.0
Rome FTP Server	192.168.3.147	34.0
Rome File Server	192.168.3.130	34.0
Exchange Box	pc171-atl.ipswit...	34.0
Cisco 1811 Rou...	192.168.3.222	34.0

The Attack – WhatsUP Gold 2006



The Attack – WhatsUP Gold 2006



The Attack – WhatsUP Gold 2006

Assumptions

- The management console is only available via the Intranet
- The victim will NOT be logged into the management console
- The victim does NOT have a WhatsUP account
- The victim is using Firefox (Possible with IE)
- No unauthenticated XSS vulnerabilities

The Attack – WhatsUP Gold 2006

Steps to Exploitation

- Vulnerability Research
- Target Reconnaissance
- Initial XSS
- Port scanning and Fingerprinting
- Brute Forcing Credentials
- XSS follow-up
- Driving Interaction

The Attack – WhatsUP Gold 2006

Creds List

```
var usernameList = new Array("administrator", "whatsup", "admin");  
var passwordList = new Array("password", "admin", "administrator");
```



The Attack – WhatsUP Gold 2006

NOT LIMITED TO WhatsUP Gold!





The Attack – WhatsUP Gold 2006

DEMO



WTF?



One More Time... This time in Slow motion

Questions and Thanks...

PEOPLE I've MET

Danya

Nitesh Dhanjani

Rajat Swarup

Sriram

Mike Crabtree

Old PAC-CERT Crew

Ed Souza

PEOPLE I haven't MET

Jeremiah Grossman

RSnake

Anton Rager

SPI Dynamics

Black Hat

Houston & New York Advanced Security Centers!