

The logo for SecTheory Internet Security. The word "SecTheory" is written in a large, bold, italicized sans-serif font. Below it, the words "Internet Security" are written in a smaller, regular sans-serif font. A large, light gray, stylized graphic element, resembling a thick, irregular loop or a stylized letter 'S', is positioned behind the text, partially overlapping it.

SecTheory
Internet Security

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



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

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?

[-] AddTrust AB		
AddTrust External CA Root		Builtin Object Token
AddTrust Class 1 CA Root		Builtin Object Token
AddTrust Public CA Root		Builtin Object Token
AddTrust Qualified CA Root		Builtin Object Token
UTN-USERFirst-Hardware		Software Security Device
[-] America Online Inc.		
America Online Root Certification Authority 1		Builtin Object Token
America Online Root Certification Authority 2		Builtin Object Token
[-] AOL Time Warner Inc.		
AOL Time Warner Root Certification Authority 1		Builtin Object Token
AOL Time Warner Root Certification Authority 2		Builtin Object Token
[-] Autoridad de Certificacion Firmaprofesional CIF A62634068		
Autoridad de Certificacion Firmaprofesional CIF A62634068		Builtin Object Token
[-] Baltimore		
Baltimore CyberTrust Root		Builtin Object Token
[-] beTRUSTed		
beTRUSTed Root CA		Builtin Object Token
beTRUSTed Root CA-Baltimore Implementation		Builtin Object Token
beTRUSTed Root CA - Entrust Implementation		Builtin Object Token
beTRUSTed Root CA - RSA Implementation		Builtin Object Token
[-] Bypass AS-983163327		
Bypass Class 3 CA 1		Builtin Object Token
Bypass Class 2 CA 1		Builtin Object Token
[-] Certplus		
Class 2 Primary CA		Builtin Object Token
[-] certSIGN		
certSIGN ROOT CA		Builtin Object Token
[-] Chunghwa Telecom Co., Ltd.		
ePKI Root Certification Authority		Builtin Object Token
[-] CNNIC		
CNNIC ROOT		Builtin Object Token
[-] COMODO CA Limited		
COMODO ECC Certification Authority		Builtin Object Token

Certificates

Intended purpose: <All>

Intermediate Certification Authorities Trusted Root Certification Authorities Trusted Publ <>

Issued To	Issued By	Expiratio...	Friendly Name
GTE CyberTrust Root	GTE CyberTrust Root	4/3/2004	GTE CyberTrust ...
GTE CyberTrust Root	GTE CyberTrust Root	2/23/2006	GTE CyberTrust ...
Halcom CA FO	Halcom CA FO	6/5/2020	Halcom CA FO
Halcom CA PO 2	Halcom CA PO 2	2/7/2019	Halcom CA PO 2
Hongkong Post Roo...	Hongkong Post Root CA	1/16/2010	Hongkong Post ...
Hongkong Post Roo...	Hongkong Post Root ...	5/14/2023	Hongkong Post ...
http://www.valicer...	http://www.valicert.c...	6/25/2019	SECOM Trust Sy...
http://www.valicer...	http://www.valicert.c...	6/25/2019	ValiCert Class 3 ...
http://www.valicer...	http://www.valicert.c...	6/25/2019	Starfield Technol...

Import... Export... Remove Advanced...

Certificate intended purposes

Server Authentication, Client Authentication, Secure Email

View

Close

Attacking Resellers



[StartCom Home](#)

[Start](#)

StartSSL™ Certificates & Public Key Infrastructure (PKI)

[Tool Box](#)

[Certificates Wizard](#)

[Validations Wizard](#)

Add Domains

- Select the top target domain name for your certificate.
- Note: Only domain names which were validated within the last 30 days are eligible for selection.

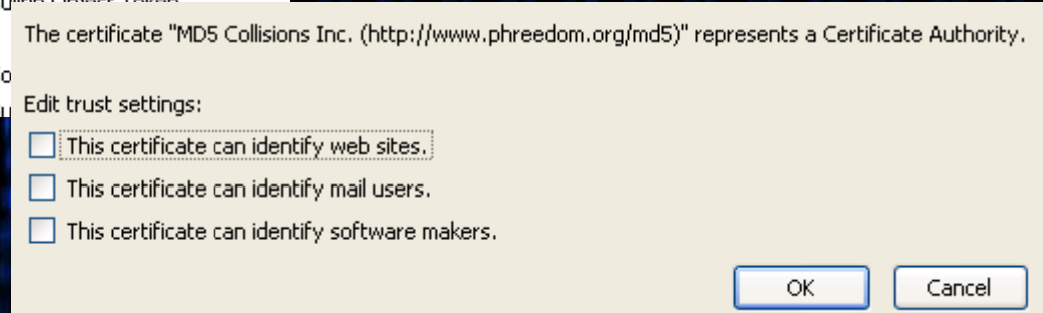
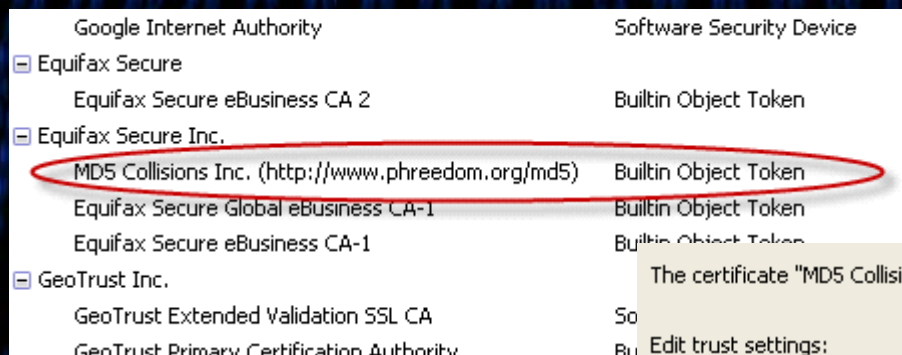
Domain:

dishuplink.com
phishme.com
intrepidusgroup.com
paypal.com
verisign.com



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 Own the web



Packet Forensics

“Packet
and rem
noticeal
intercep
while it
wire. Us
essentia
cryptog
product
to impo
(potenti
keys de
in its au



PACKET FORENSICS

May 18th 2010, 2:46pm UTC

[solutions](#) · [products](#) · [helpdesk](#) · [about us](#) · [contact us](#) · [extranet portal](#)

o Product Overview
o LI-3

o LI-5B
o LI-5

o 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
Buy. Comply. Relax.



Packet Forensics LI-5B

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.

Specs at a Glance

Feature Highlights

Ethernet Probe / IAP
Dialed Digit Extraction
Integrated Mediation Server

Network Interfaces

4x 10/100 Copper
[Need something faster?](#)

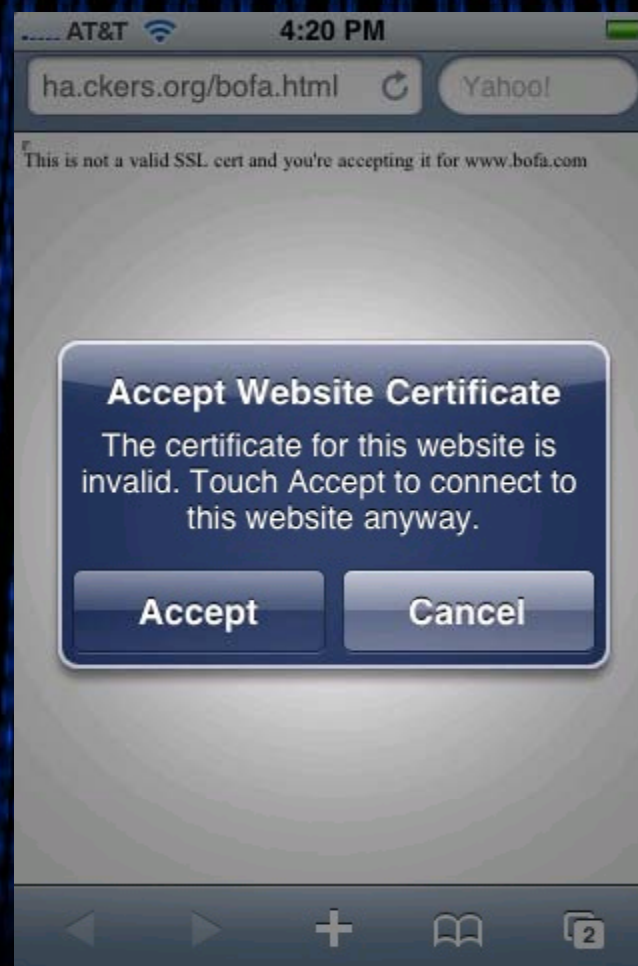
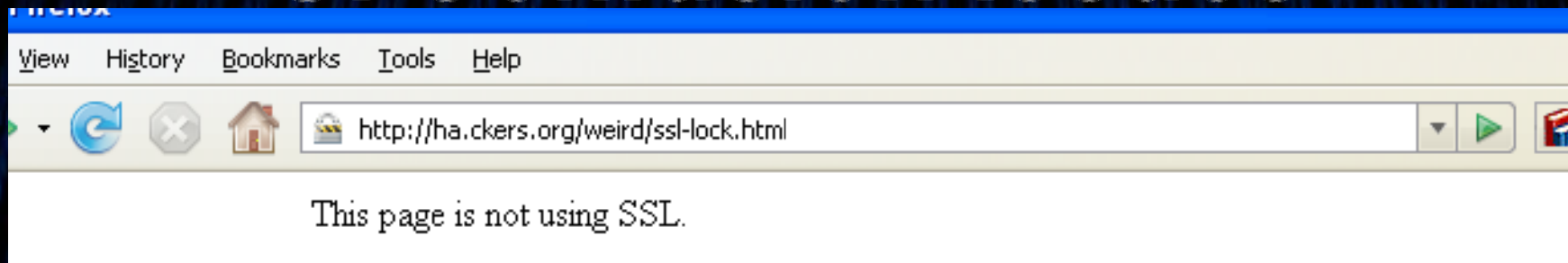
Storage Capacity

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

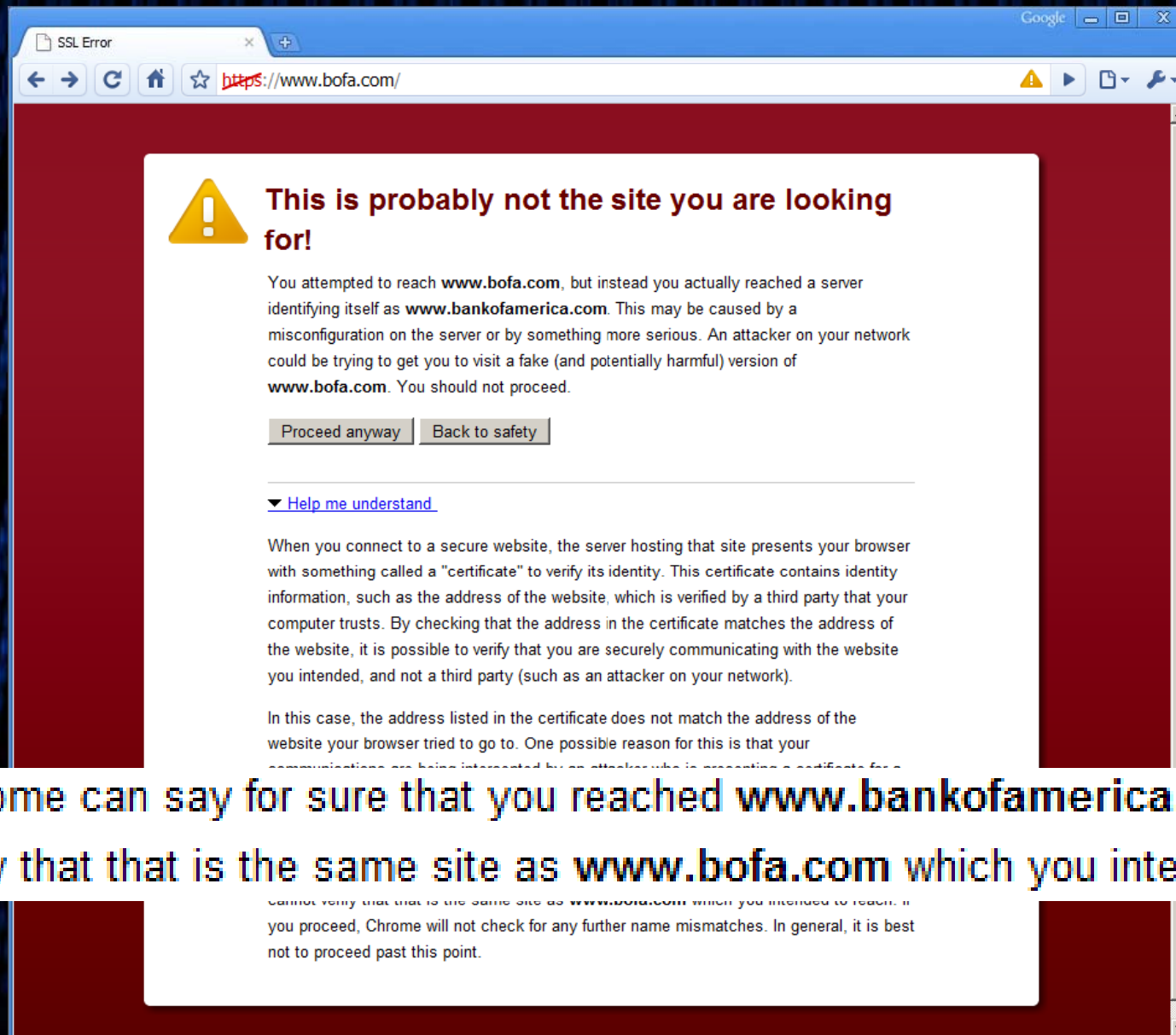
-into
y
tionally
ren
on the
3L is
man
r
ability
-alike'
dence

<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

The screenshot shows a Firefox browser window with a security warning. The address bar contains `https://www.youtube.com/`. A yellow warning icon is present. The main content area displays a message: "This Connection is Not Secure" with a yellow shield icon. Below this, it says "You have asked Firefox to continue to this site, but the connection is not secure." and "Normally, when you try to connect to a site you are going to the right place, but here you are being redirected to a different site." The "What Should I Do" section offers a "Get me out of here!" button and two options: "Technical Details" and "I Understand the Risks". The "I Understand the Risks" option is selected, and a checkbox "Permanently store this exception" is checked. The "Technical Details" section shows a "Wrong Site" warning: "Certificate belongs to a different site, which is not www.youtube.com". The "Certificate Status" section shows "Server" as "www.youtube.com" and "Location" as "https://www.youtube.com/". The "Certificate Information" section shows the certificate is issued to "*.google.com" by "Google Internet Authority".

Legitimate banks, stores, and other sites

Server: www.youtube.com
Location: https://www.youtube.com/

Certificate Status
This site attempts to identify itself with invalid information.

Wrong Site
Certificate belongs to a different site, which is not www.youtube.com.

Certificate Information
This certificate has been verified for the following uses:
SSL Server Certificate
Email Signer Certificate
Email Recipient Certificate

Issued To
Common Name (CN): *.google.com
Organization (O): Google Inc
Organizational Unit (OU): <Not Part Of Certificate>
Serial Number: 19:F9:00:E8:00:03:00:00:11:20

Issued By
Common Name (CN): Google Internet Authority
Organization (O): Google Inc
Organizational Unit (OU): <Not Part Of Certificate>

Validity
Issued On: 3/4/2010
Expires On: 3/4/2011

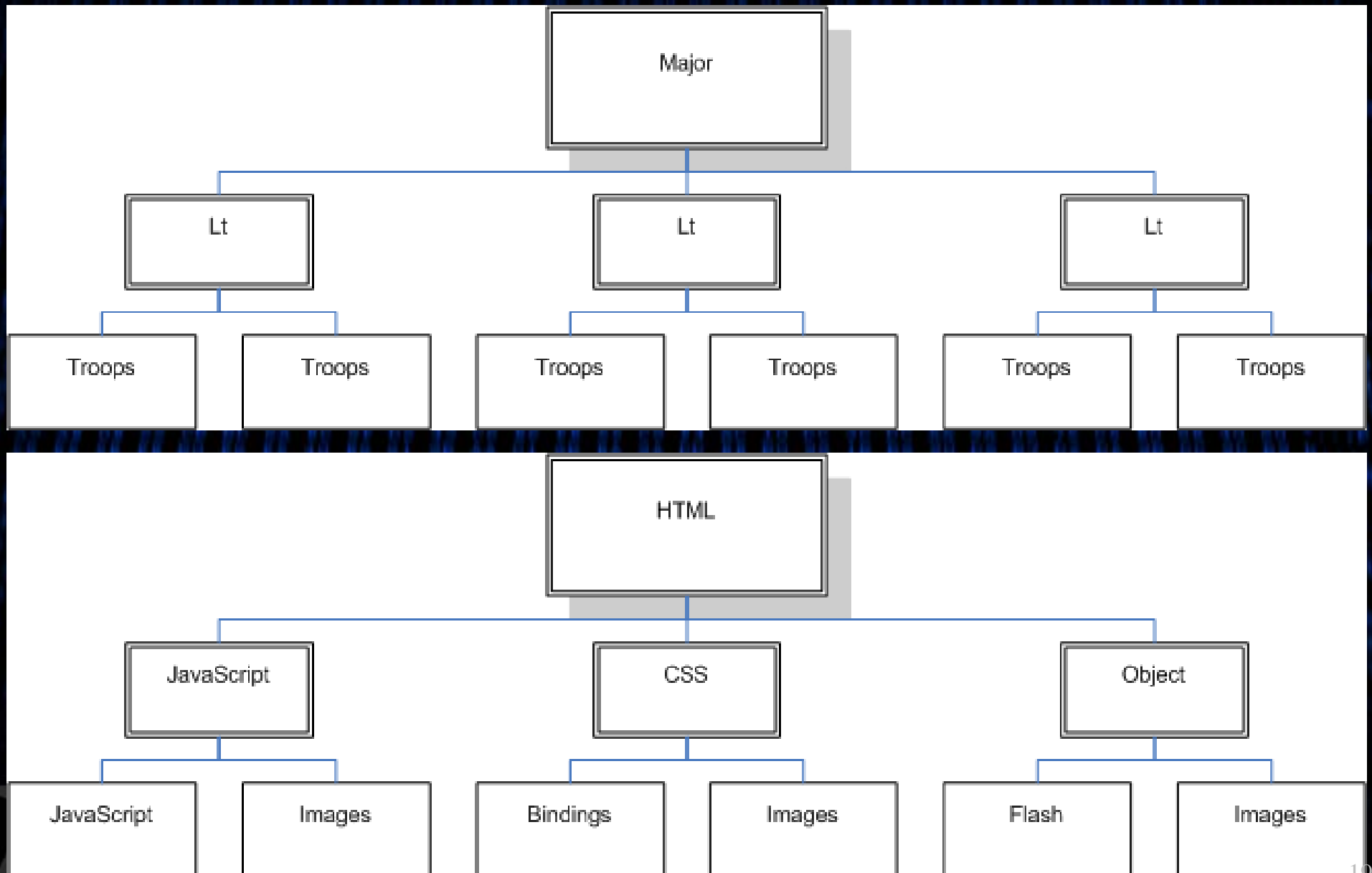
Fingerprints
SHA1 Fingerprint: 71:8D:CE:C9:B4:58:27:66:C0:44:A5:
MD5 Fingerprint: CA:4E:2A:59:E9:3C:96:AE:72:60:97:

Permanently store this exception

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

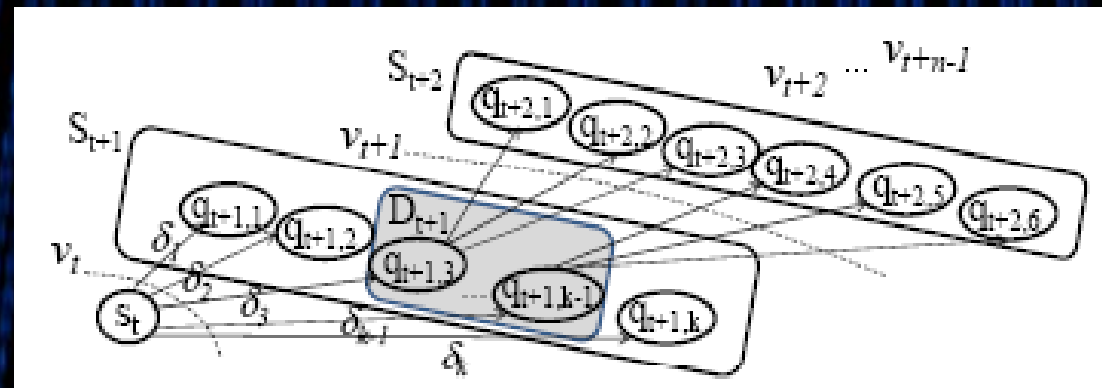


Major Problems To Overcome For Attackers

- ▣ Ciphpered 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)

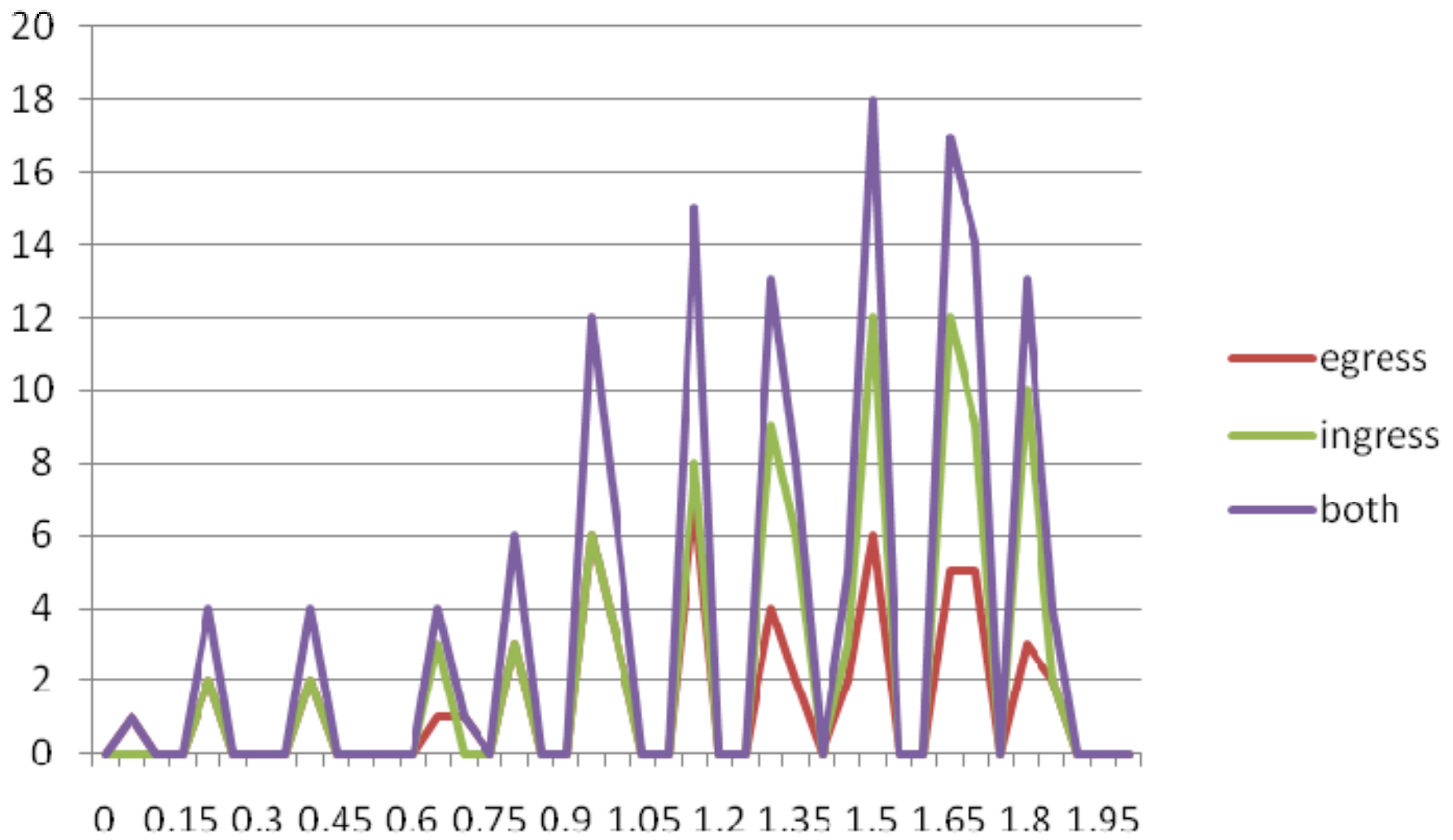
Timing and Directional Differences

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

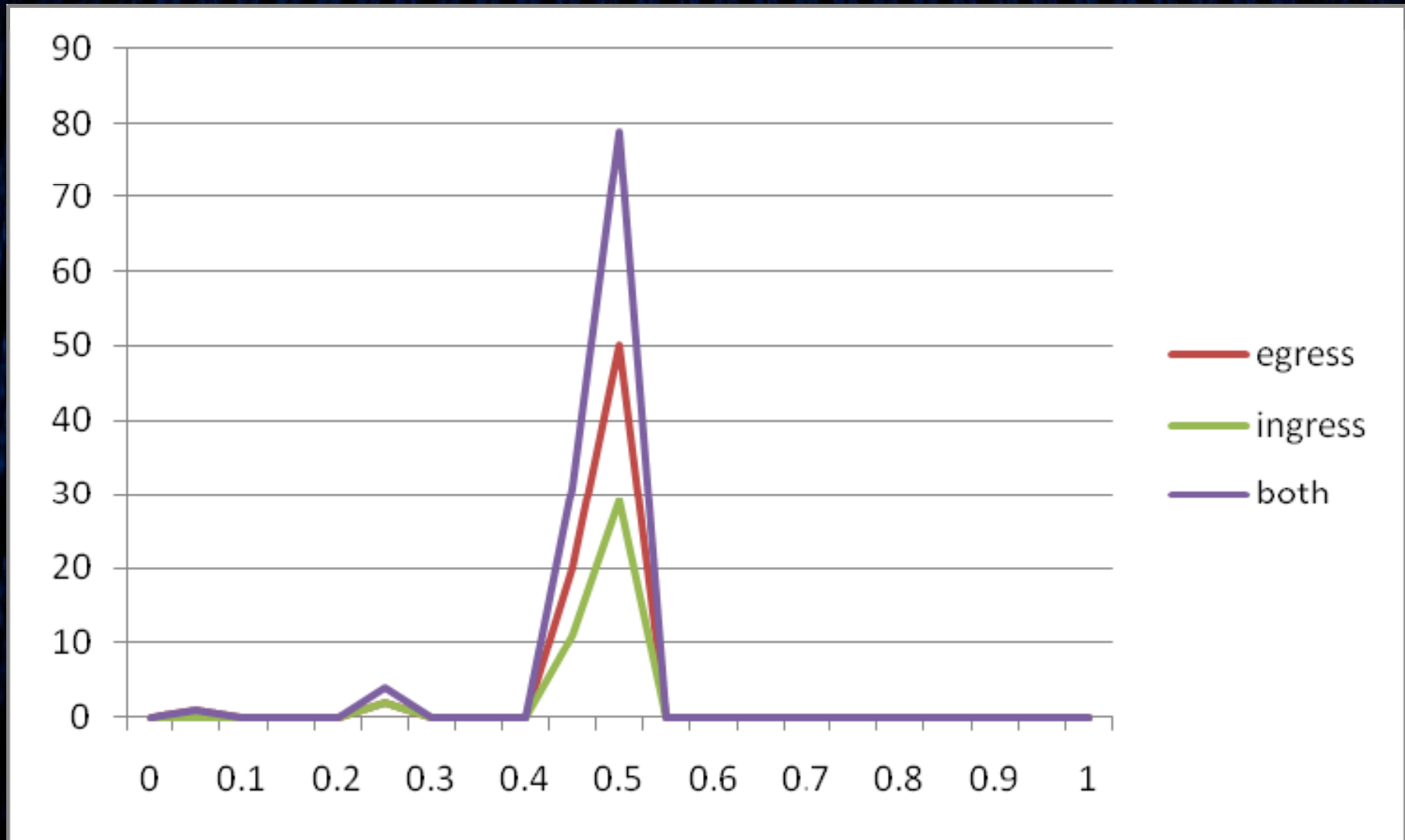


- ▣ Size Difference
- ▣ One way data/user or server initiated request
- ▣ Timed requests (long term analysis)

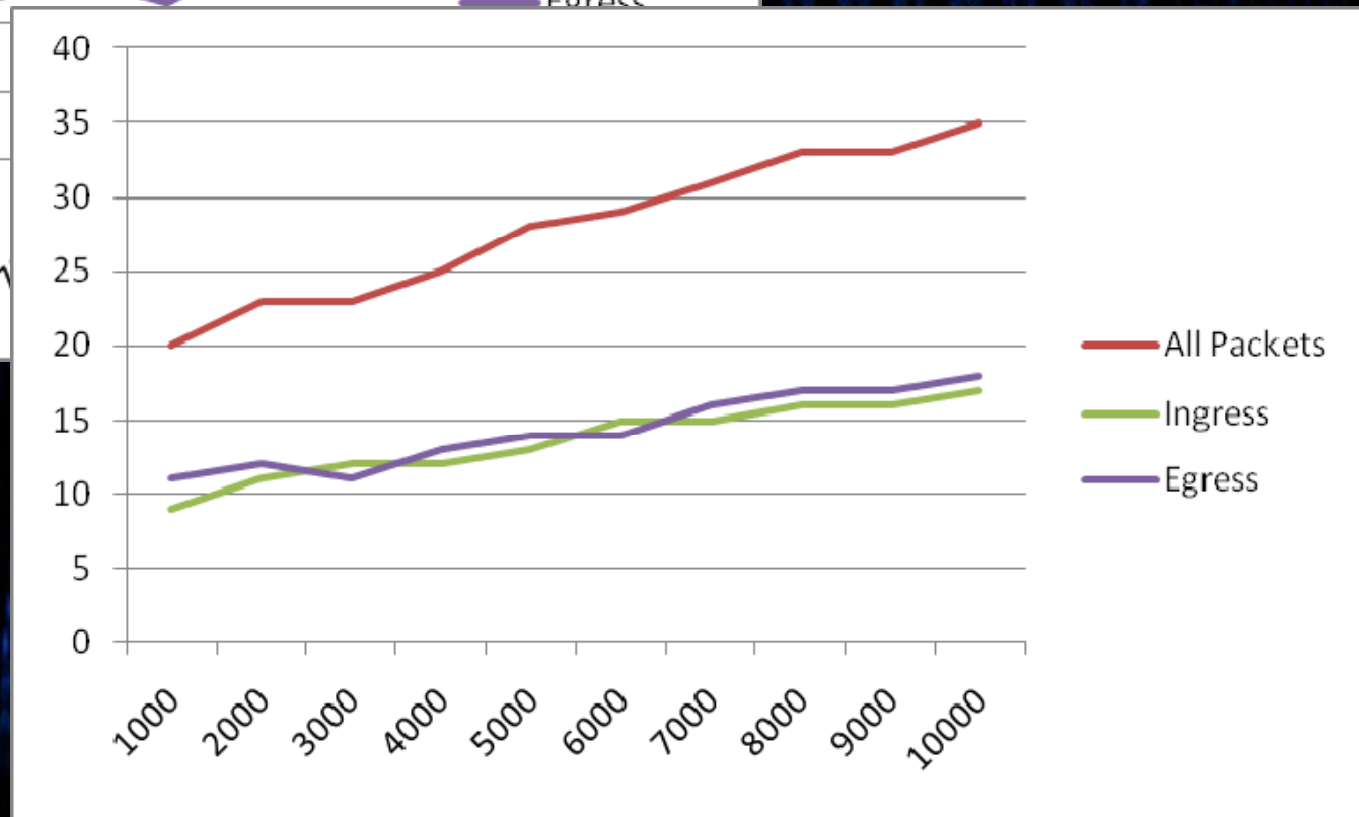
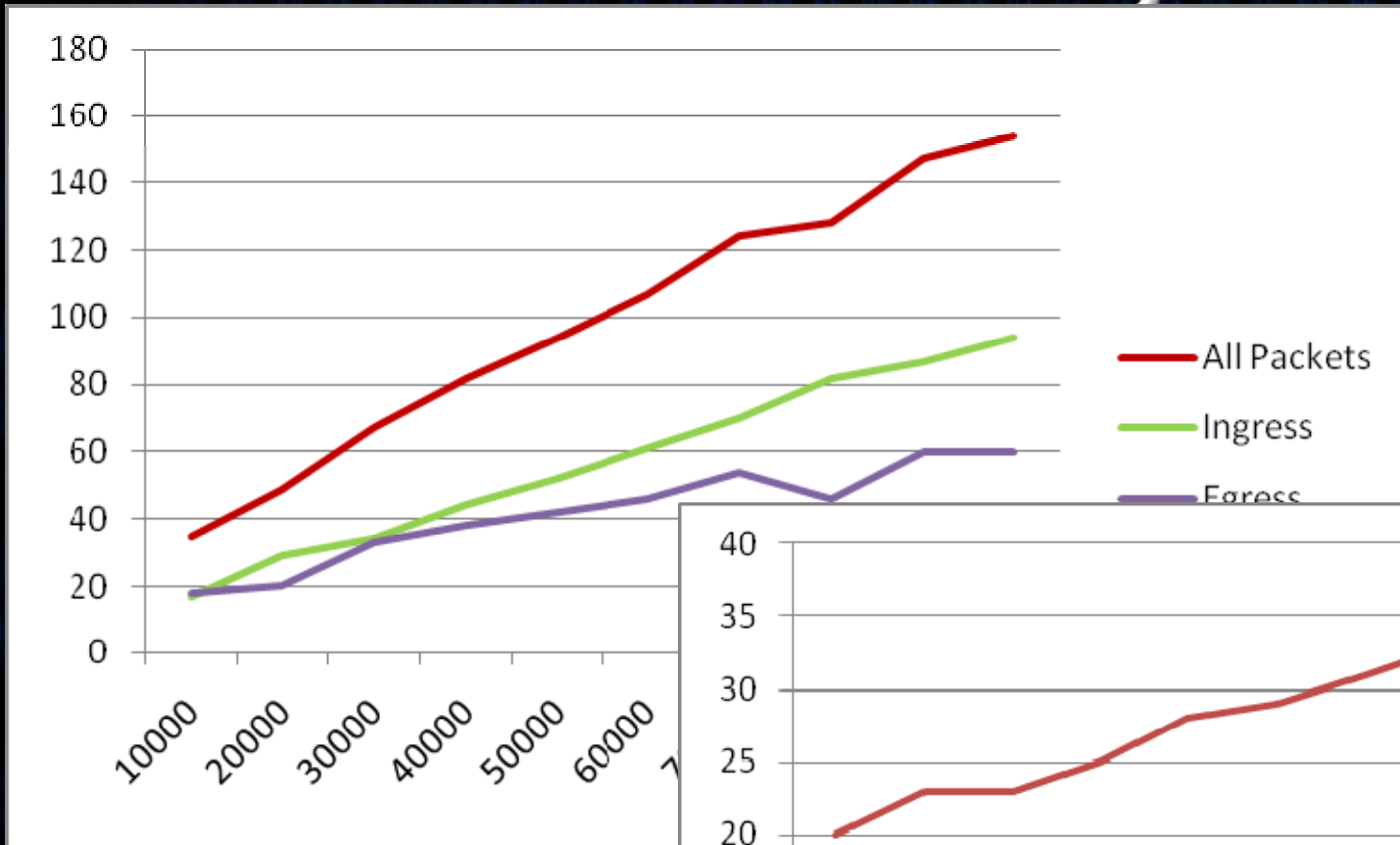
Content SSL Packets/Time GET Request (100K)



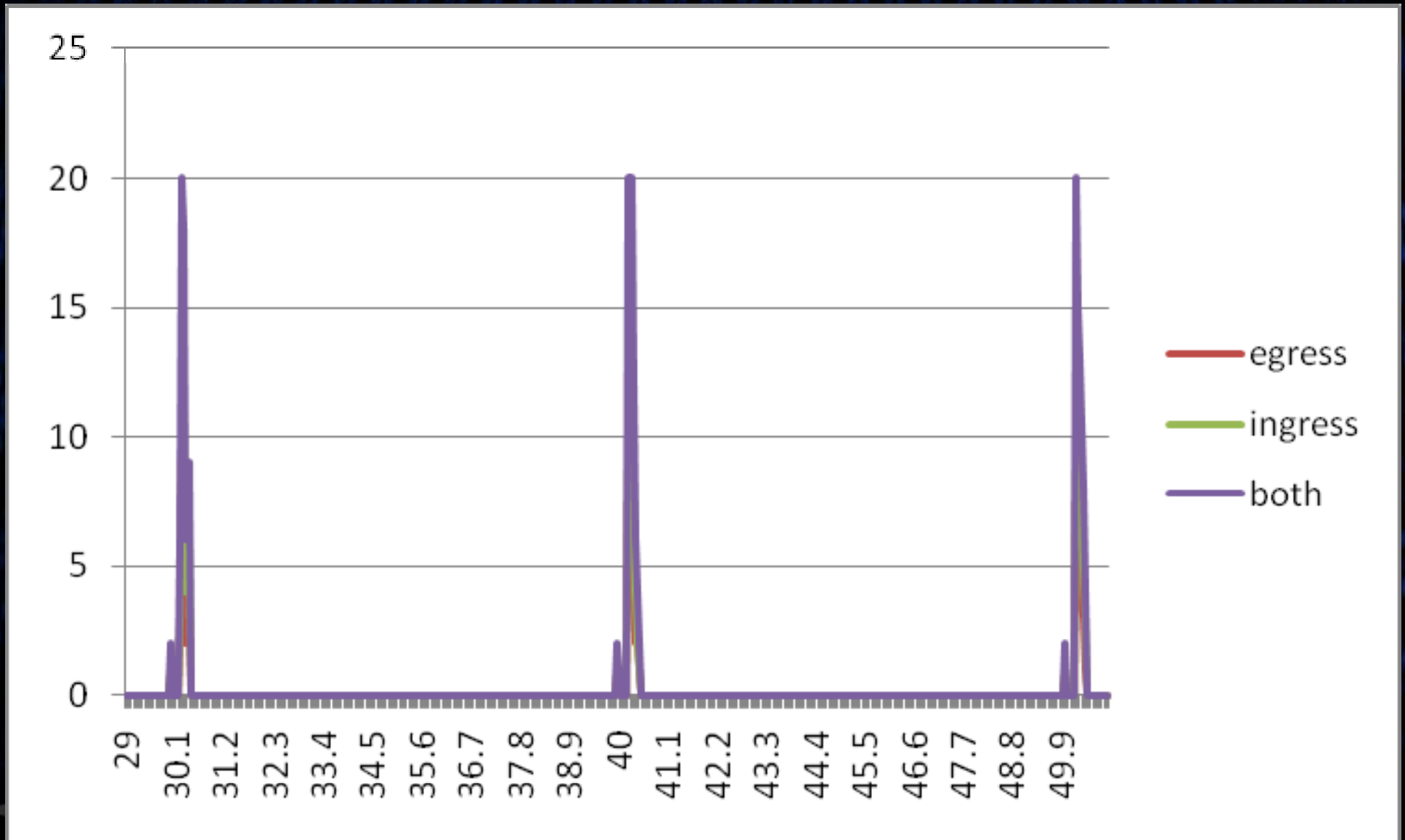
Typical SSL Packets/Time POST Request (100k)



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...

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.caller.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

Examining Our History

▣ Identifying History

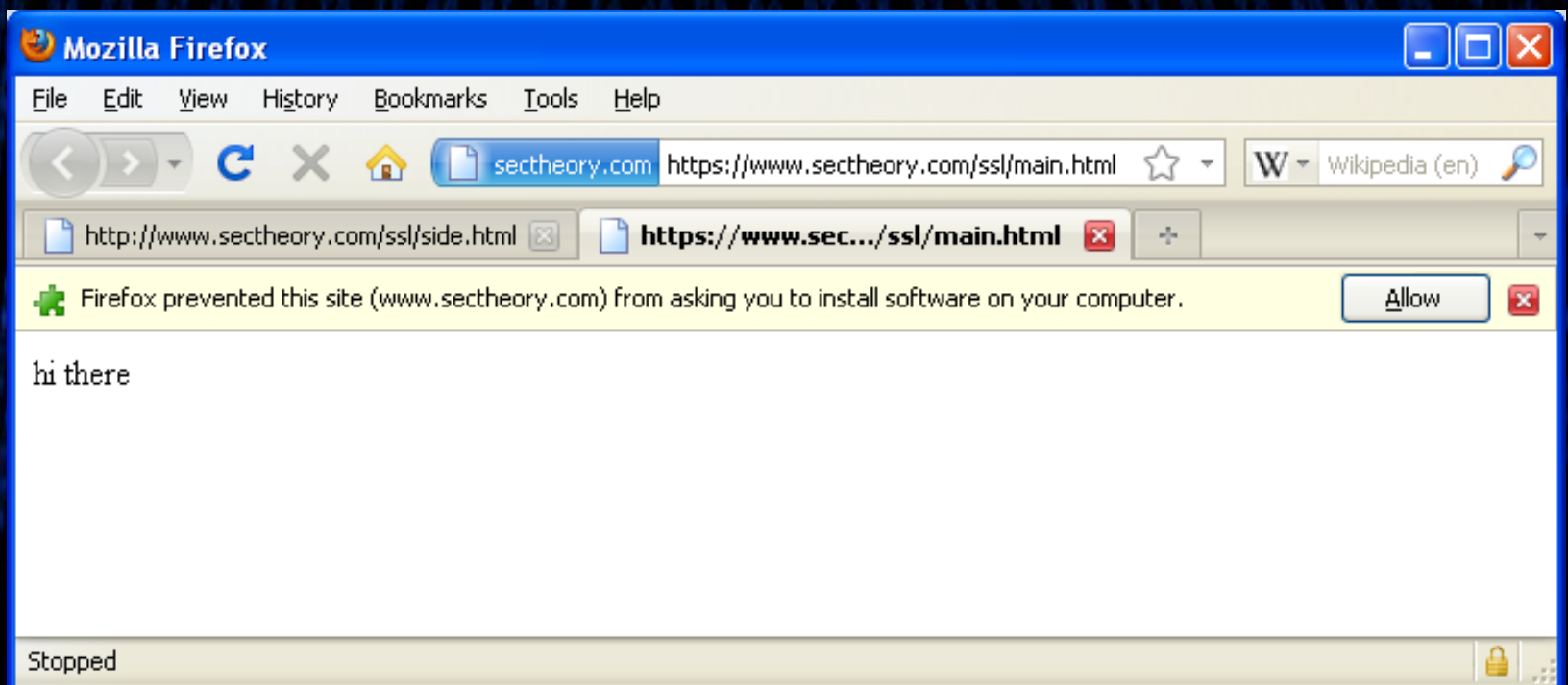
- ▣ Some products try to mask referrers but you can still use `document.referrer` in JS space except:
 - ▣ **SSL**
 - ▣ New frames
 - ▣ Bookmarks
 - ▣ `file:///`
- ▣ CSS history stealing (requires refresh/reload and won't work in future versions of FF)
- ▣ `history.length` upon entrance and exit

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 slooooooow from a victim's perspective

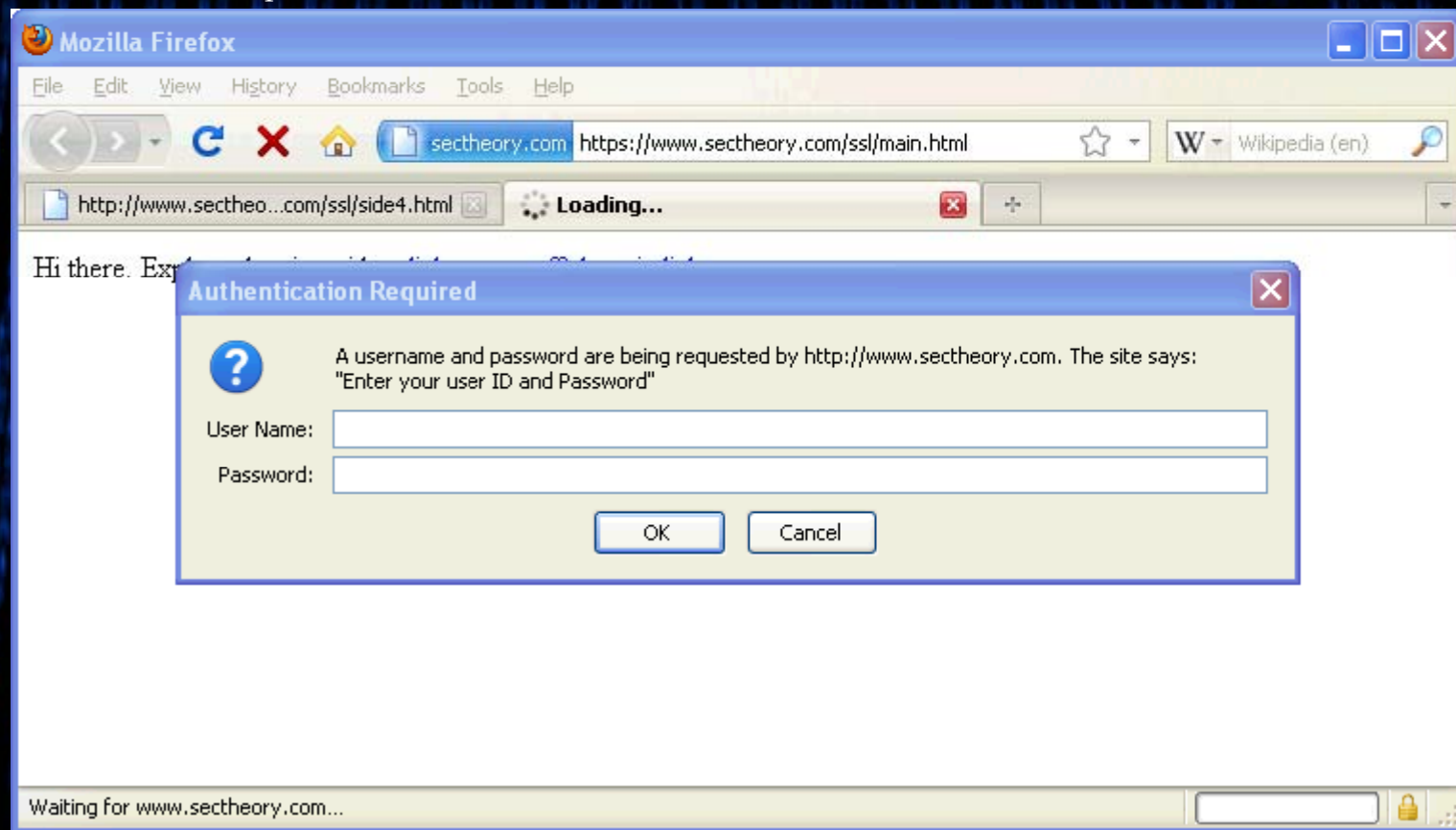
Using Delayed Popups

```
<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_\(XSHM\)](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

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.

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: aa

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](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...

Perspectives

Security Level

High Security

Percentage of notaries that must agree (quorum percentage): 75

Days of continuous agreement required (quorum duration): 2

Overriding Firefox Security Errors

Allow Perspectives to automatically override security errors

Permanently trust certificates validated by Perspectives

When to Contact Notaries

Contact Notaries for all HTTPS sites

Contact Notaries only when a website's certificate causes a security error

Always ask the user before contacting Notaries

OK

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

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.

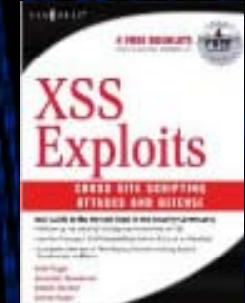
~~FUD~~ Free Zone

- ▣ 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/>

The logo for SecTheory Internet Security. The word "SecTheory" is written in a large, bold, italicized sans-serif font. Below it, the words "Internet Security" are written in a smaller, plain sans-serif font. A large, light gray, stylized graphic element, resembling a thick, irregular loop or a stylized letter 'S', is positioned behind the text, partially overlapping it.

SecTheory
Internet Security

*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/>