Fear and Loathing

(and some Hope)

Lucas Adamski

Mozilla Corporation

Declaratively Solving Web Security Problems

Fear

- Perception of "We Are Doomed"
- Endless parade of XSS, CSRF and overflows
- Nothing is being done about it
- Users are clueless
- "Dumbing down" of security

Fear Leads To

Loathing

- Standards + Security = Broken
- Software vendors aren't cooperating
- Users never learn
- Functionality and complexity increasing
- Rate of change accelerating

Standards & Security

- Security community isn't participating
- Politicized - vendor competition can limit search solution space
- Some things aren't well suited to standards - UI for example

Complexity Increasing

- Security community having a hard time tracking the complexity of the security models
- Gradual shift in leadership from researchers to software vendors in terms of mitigation

Software Vendor Cooperation

- Each vendor solving a problem differently is no solution at all - web developers are already overwhelmed by compatibility problems
- Example: cross-domain data loading mechanisms in the browser

Cross-Domain Loading

- Adobe Flash Player Cross-Domain Policy File (v1 and v2)
- Microsoft Silverlight (clientaccesspolicy.xml and crossdomain.xml)
- Java
- HTML - Cross Origin Resource Sharing (aka Access Control), etc.

Cross-Domain: Flash

- Flash Cross-Domain Policy File (crossdomain.xml)
- v1: automatically loaded from the root or explicitly from a subdirectory
- Grants access to that directory and below to listed domains or *
- Sends cookies
- v2: Implements much stricter controls on default policy file locations, MIME types and socket behaviors, and lots of other changes

Cross-Domain: Silverlight 2

- Implements clientaccesspolicy.xml
  - must be in root directory
  - specify which directories can be accessed
  - permit from specific domains or *
  - permit specific or all (safe) request headers
- Supports crossdomain.xml but only in the root, and only from all domains (*)
- Sends cookies

Cross-Domain: Java

- Java SE 6 update 10 Supports Flash crossdomain.xml
- ... in the root or an explicitly declared subdirectory
- ... but requires you to permit access from all domains (*)
- Coooookies? Apparently, yes.

Cross-Domain: HTML

- Cross-Origin Resource Sharing (CORS)
- Sends Origin request header
- Expects Access-Control-Allow-Origin response header with the requesting domain or *

CORS Continued

- Sends cookies
- ... except in IE8
- Uses XMLHttpRequest()
- ... except in IE8, where it uses XDomainRequest()

Cross-Window Messaging

- postMessage permits for uni- or bi-directional cross-frame messaging
- Sender calls window.postMessage('Hi there')
- Receiver registers for onmessage events and can verify the sender's domain before processing or discard for any reason

Software Continued

- Philosophies differ - minimal solution that is easily broadly implemented or a richer model that supports more use cases?
- Web app boundaries > domain boundaries
- “Perfect” is the enemy of “good” (but so is “simple”)

Users ≠ Security Experts

- Users aren't security experts
- Good!
- Any security model that requires users to master security is doomed to fail

Users and Dialogs

- Security dialogs are a symptom of a flawed security model
- Don’t ask users to choose between “broken” and “unsafe”

Change Accelerating

- Unavoidable (only security people believe you can travel back in time)
- If you don't support developers building complex apps, they will hack together alternatives that are worse than anything you can image (i.e. JSON via <SCRIPT src=...)

Hope

Standards

- Progress being made anyway
- Broad agreement on philosophies and goals (breadth vs complexity of solutions) would go a long way
- Perhaps enumerate which types of application architectures would have to be covered

Standard Progress

- JSON.parse
- Content Security Policy for XSS mitigation
- Strict Transport Security - force HTTPS
- Origin for CSRF mitigation

JSON.parse

- Native support for decoding and encoding of (strict) JSON strings
- Faster, more secure
- Not a replacement for <SCRIPT src=...
- Relies on an additional mechanism for cross-domain scenarios (ex. CORS)

JSON is supposed to be

```
var data = ' { "responseData":
{"results": [
    {
        "SafeSearch":"true",
        "url":"http://www.arunranga.com/i.jpg",
    },
    {
        "SafeSearch":"false",
    "url":"http://www.badarunranga.com/evil.jpg",
    }
]}}';
```

var G_INCOMPAT = false;function GScript(src) {document.write('<' + 'script src="' + src + '"' +' type="text/javascript"><' + '/
script>');}function GBrowserIsCompatible() {if (G_INCOMPAT) return false;return true;}function GApiInit() {if (GApiInit.called)
return;GApiInit.called = true;window.GAddMessages && GAddMessages({160: '\x3cH1\x3eServer Error\x3c/H1\x3eThe server encountered a temporary
error and could not complete your request.\x3cp\x3ePlease try again in a minute or so.\x3c/p\x3e',1415: '.',1416: ',',1547: 'mi',1616: 'km',
4100: 'm',4101: 'ft',10018: 'Loading...',10021: 'Zoom In',10022: 'Zoom Out',10024: 'Drag to zoom',10029: 'Return to the last result',10049:
'Map',10050: 'Satellite',10093: 'Terms of Use',10111: 'Map',10112: 'Sat',10116: 'Hybrid',10117: 'Hyb',10120: 'We are sorry, but we don\x27t
have maps at this zoom level for this region.\x3cp\x3eTry zooming out for a broader look.\x3c/p\x3e',10121: 'We are sorry, but we don\x27t
have imagery at this zoom level for this region.\x3cp\x3eTry zooming out for a broader look.\x3c/p\x3e',10507: 'Pan left',10508: 'Pan right'
10509: 'Pan up',10510: 'Pan down',10511: 'Show street map',10512: 'Show satellite imagery',10513: 'Show imagery with street names',10806:
'Click to see this area on Google Maps',10807: 'Traffic',10808: 'Show Traffic',10809: 'Hide Traffic',12150: '%1$s on %2$s',12151: '%1$s on
%2$s at %3$s',12152: '%1$s on %2$s between %3$s and %4$s',10985: 'Zoom in',10986: 'Zoom out',11047: 'Center map here',11089: '\x3ca href\x3d
\x22javascript:void(0);\x22\x3eZoom In\x3c/a\x3e to see traffic for this region',11259: 'Full-screen',11751: 'Show street map with terrain',
11752: 'Style:',11757: 'Change map style',11758: 'Terrain',11759: 'Ter',11794: 'Show labels',11303: 'Street View Help',11274: 'To use street
view, you need Adobe Flash Player version %1$d or newer.',11382: 'Get the latest Flash Player.',11314: 'We\x27re sorry, street view is
currently unavailable due to high demand.\x3cbr\x3ePlease try again later!',1559: 'N',1560: 'S',1561: 'W',1562: 'E',1608: 'NW',1591: 'NE',
1605: 'SW',1606: 'SE',11907: 'This image is no longer available',10041: 'Help',12471: 'Current Location',12492: 'Earth',12823: 'Google has
disabled usage of the Maps API for this application. See the Terms of Service for more information: %1$s.',12822: 'http://code.google.com/
apis/maps/terms.html',12915: 'Improve the map',12916: 'Google, Europa Technologies',13171: 'Hybrid 3D',0: ''});if (!
GValidateKey("448e2ab522c62f7b67cdc1d149460205c4218e74")) {G_INCOMPAT = true;alert("This web site needs a different Google Maps API key. A
new key can be generated at http://code.google.com/apis/maps/.");return;}}var GLoad;(function() {var jslinker={version:"175",jsbinary:
[{id:"maps2",url:"http://maps.gstatic.com/intl/en_us/mapfiles/178b/maps2/main.js"},{id:"maps2.api",url:"http://maps.gstatic.com/intl/en_us/
mapfiles/178b/maps2.api/main.js"},{id:"gc",url:"http://maps.gstatic.com/intl/en_us/mapfiles/178b/gc.js"},{id:"suggest",url:"http://
maps.gstatic.com/intl/en_us/mapfiles/178b/suggest/main.js"},{id:"adsense",url:"http://maps.gstatic.com/intl/en_us/mapfiles/178b/adsense.js"}
{id:"pphov",url:"http://maps.gstatic.com/intl/en_us/mapfiles/178b/pphov.js"}]};GLoad = function(callback) {var callee = arguments.callee;var
apiCallback = callback;GApiInit();var opts = {public_api:true,export_legacy_names:true,tile_override:[{maptype:0,min_zoom:7,max_zoom:7,rect:
[{lo:{lat_e7:330000000,lng_e7:1246050000},hi:{lat_e7:386200000,lng_e7:1293600000}},{lo:{lat_e7:366500000,lng_e7:1297000000},hi:
{lat_e7:386200000,lng_e7:1320034790}}],uris:["http://mt0.gmaptiles.co.kr/mt/v=kr1.11\x26hl=en\x26src=api\x26","http://mt1.gmaptiles.co.kr/mt
v=kr1.11\x26hl=en\x26src=api\x26","http://mt2.gmaptiles.co.kr/mt/v=kr1.11\x26hl=en\x26src=api\x26","http://mt3.gmaptiles.co.kr/mt/
v=kr1.11\x26hl=en\x26src=api\x26"],mapprint_url:"http://www.gmaptiles.co.kr/mapprint"},{maptype:0,min_zoom:8,max_zoom:9,rect:[{lo:
{lat_e7:330000000,lng_e7:1246050000},hi:{lat_e7:386200000,lng_e7:1279600000}},{lo:{lat_e7:345000000,lng_e7:1279600000},hi:
{lat_e7:386200000,lng_e7:1286700000}},{lo:{lat_e7:348900000,lng_e7:1286700000},hi:{lat_e7:386200000,lng_e7:1293600000}},{lo:
{lat_e7:354690000,lng_e7:1293600000},hi:{lat_e7:386200000,lng_e7:1320034790}}],uris:["http://mt0.gmaptiles.co.kr/mt/v=kr1.11\x26hl=en
\x26src=api\x26","http://mt1.gmaptiles.co.kr/mt/v=kr1.11\x26hl=en\x26src=api\x26","http://mt2.gmaptiles.co.kr/mt/v=kr1.11\x26hl=en\x26src=ap
\x26","http://mt3.gmaptiles.co.kr/mt/v=kr1.11\x26hl=en\x26src=api\x26"],mapprint_url:"http://www.gmaptiles.co.kr/mapprint"},{maptype:
0,min_zoom:10,max_zoom:18,rect:[{lo:{lat_e7:329890840,lng_e7:1246055600},hi:{lat_e7:386930130,lng_e7:1284960940}},{lo:
{lat_e7:344646740,lng_e7:1284960940},hi:{lat_e7:386930130,lng_e7:1288476560}},{lo:{lat_e7:350277470,lng_e7:1288476560},hi:
{lat_e7:386930130,lng_e7:1310531620}},{lo:{lat_e7:370277730,lng_e7:1310531620},hi:{lat_e7:386930130,lng_e7:1320034790}}],uris:["http://
mt0.gmaptiles.co.kr/mt/v=kr1.11\x26hl=en\x26src=api\x26","http://mt1.gmaptiles.co.kr/mt/v=kr1.11\x26hl=en\x26src=api\x26","http://
mt2.gmaptiles.co.kr/mt/v=kr1.11\x26hl=en\x26src=api\x26","http://mt3.gmaptiles.co.kr/mt/v=kr1.11\x26hl=en\x26src=api
\x26"],mapprint_url:"http://www.gmaptiles.co.kr/mapprint"},{maptype:3,min_zoom:7,max_zoom:7,rect:[{lo:
{lat_e7:330000000,lng_e7:1246050000},hi:{lat_e7:386200000,lng_e7:1293600000}},{lo:{lat_e7:366500000,lng_e7:1297000000},hi:
{lat_e7:386200000,lng_e7:1320034790}}],uris:["http://mt0.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt1.gmaptiles.co.kr/
mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt2.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt3.gmaptiles.co.kr/mt/
v=kr1p.11\x26hl=en\x26src=api\x26"]},{maptype:3,min_zoom:8,max_zoom:9,rect:[{lo:{lat_e7:330000000,lng_e7:1246050000},hi:
{lat_e7:386200000,lng_e7:1279600000}},{lo:{lat_e7:345000000,lng_e7:1279600000},hi:{lat_e7:386200000,lng_e7:1286700000}},{lo:
{lat_e7:348900000,lng_e7:1286700000},hi:{lat_e7:386200000,lng_e7:1293600000}},{lo:{lat_e7:354690000,lng_e7:1293600000},hi:
{lat_e7:386200000,lng_e7:1320034790}}],uris:["http://mt0.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt1.gmaptiles.co.kr/
mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt2.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt3.gmaptiles.co.kr/mt/
v=kr1p.11\x26hl=en\x26src=api\x26"]},{maptype:3,min_zoom:10,rect:[{lo:{lat_e7:329890840,lng_e7:1246055600},hi:
{lat_e7:386930130,lng_e7:1284960940}},{lo:{lat_e7:344646740,lng_e7:1284960940},hi:{lat_e7:386930130,lng_e7:1288476560}},{lo:
{lat_e7:350277470,lng_e7:1288476560},hi:{lat_e7:386930130,lng_e7:1310531620}},{lo:{lat_e7:370277730,lng_e7:1310531620},hi:
{lat_e7:386930130,lng_e7:1320034790}}],uris:["http://mt0.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt1.gmaptiles.co.kr/
mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt2.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt3.gmaptiles.co.kr/mt/
v=kr1p.11\x26hl=en\x26src=api\x26"]},{maptype:3,min_zoom:7,max_zoom:7,rect:[{lo:{lat_e7:330000000,lng_e7:1246050000},hi:
{lat_e7:386200000,lng_e7:1293600000}},{lo:{lat_e7:366500000,lng_e7:1297000000},hi:{lat_e7:386200000,lng_e7:1320034790}}],uris:["http://
mt0.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt1.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://
mt2.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt3.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api
\x26"]},{maptype:3,min_zoom:8,max_zoom:9,rect:[{lo:{lat_e7:330000000,lng_e7:1246050000},hi:{lat_e7:386200000,lng_e7:1279600000}},{lo:
{lat_e7:345000000,lng_e7:1279600000},hi:{lat_e7:386200000,lng_e7:1286700000}},{lo:{lat_e7:348900000,lng_e7:1286700000},hi:
{lat_e7:386200000,lng_e7:1293600000}},{lo:{lat_e7:354690000,lng_e7:1293600000},hi:{lat_e7:386200000,lng_e7:1320034790}}],uris:["http://
mt0.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt1.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://
mt2.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt3.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26"]},{maptype:3,min_zoom:10,rect:[{lo:{lat_e7:329890840,lng_e7:1246055600},hi:
{lat_e7:386930130,lng_e7:1284960940}},{lo:{lat_e7:344646740,lng_e7:1284960940},hi:{lat_e7:386930130,lng_e7:1288476560}},{lo:
{lat_e7:350277470,lng_e7:1288476560},hi:{lat_e7:386930130,lng_e7:1310531620}},{lo:{lat_e7:370277730,lng_e7:1310531620},hi:
{lat_e7:386930130,lng_e7:1320034790}}],uris:["http://mt0.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt1.gmaptiles.co.kr/
mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt2.gmaptiles.co.kr/mt/v=kr1p.11\x26hl=en\x26src=api\x26","http://mt3.gmaptiles.co.kr/mt/
v=kr1p.11\x26hl=en\x26src=api\x26"]}],jsmain:"http://maps.gstatic.com/intl/en_us/mapfiles/178b/maps2.api/main.js",allow_max_zoom:true};var

JSON Frankenstein

Content Security Policy

- Data ≠ Code
- Script must come from external files served from white-listed hosts
- No inline JavaScript, e.g. internal <script> nodes, javascript: URIs, event handling attributes
- No code from strings, a.k.a. eval() is evil
  - Strings easily tainted by attacker-controlled data

CSP Continued

- Only explicitly allowed content will load
  - Policies can be separately defined for many types of content, e.g. images, audio/video, plugin content, stylesheets
    - Framing behavior can also be restricted
- Debugging & logging capabilities

Strict Transport Security

- An HTTPS site can specify response header Strict-Transport-Security
- Subsequent visits will force HTTPS scheme
- Must specify Max-Age for policy enforcement
- Optionally choose to includeSubDomains

Origin for CSRF

- Origin aka Sec-From HTTP request header provides authentication information about the requesting site
- Similar to Referer without the privacy leakage implications
  - Not sent for anchor, window navigation, images, style sheets, etc.
- Attempts to reconcile with the Origin header from CORS, which may or may not work

Other Anti-Features

- Anti-clickjacking: X-FRAME-OPTIONS response header in IE8
  - ... but assumes single domain applications
- Anti-XSS: reflected XSS filter in IE8
- Anti-phishing
- Anti-malware

What to do?

Participate!

- Peer review of security models
- Discuss: WHATWG and W3C mailing lists
- Mozilla: mozilla.dev.security
- Download and test!
  - Content Security Policy!
  - Strict Transport Security Add-on

Software Vendors

- Vendors behaving badly (some still do)
- Vendors should embrace researchers and support them
  - Security bounty program at Mozilla

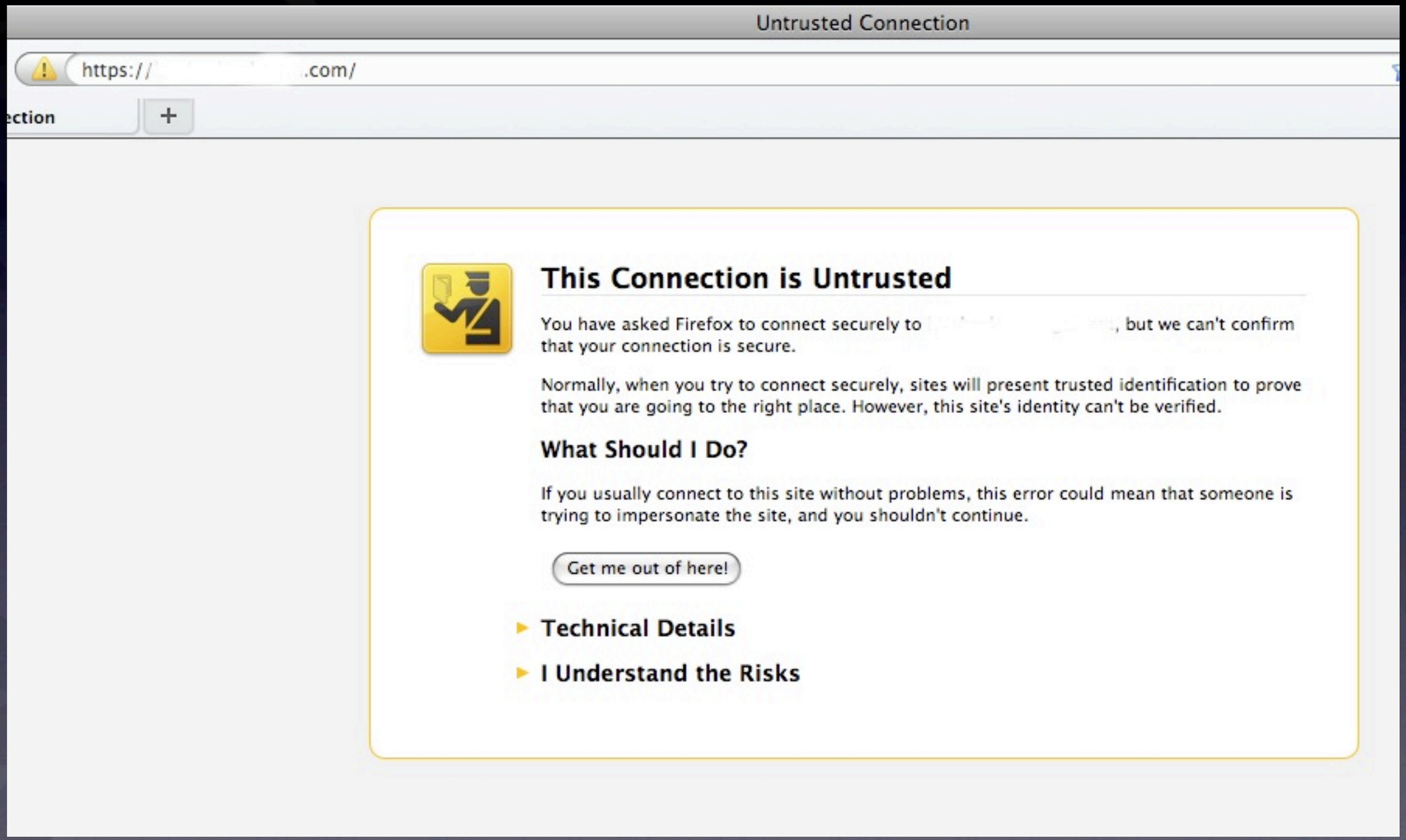
Security Researchers

- Practice responsible disclosure and embrace opportunities to contribute to the solution
- Please don't make assumptions; present findings.
- Universal Cross Site Side-Clickjacking? Spare us the hype!

Users

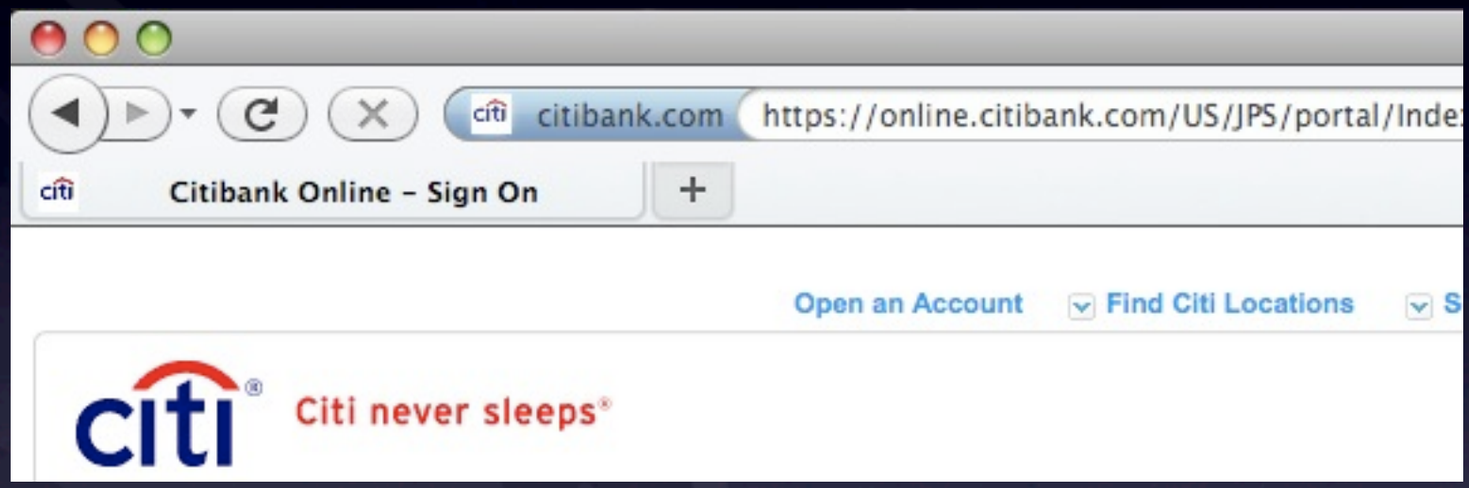
- Educate them as much as possible but don't expect them to become security experts - that's not their job
- Guide them forcefully towards correct decisions
- ... but don’t take away user choice entirely

Firefox 3 SSL UI

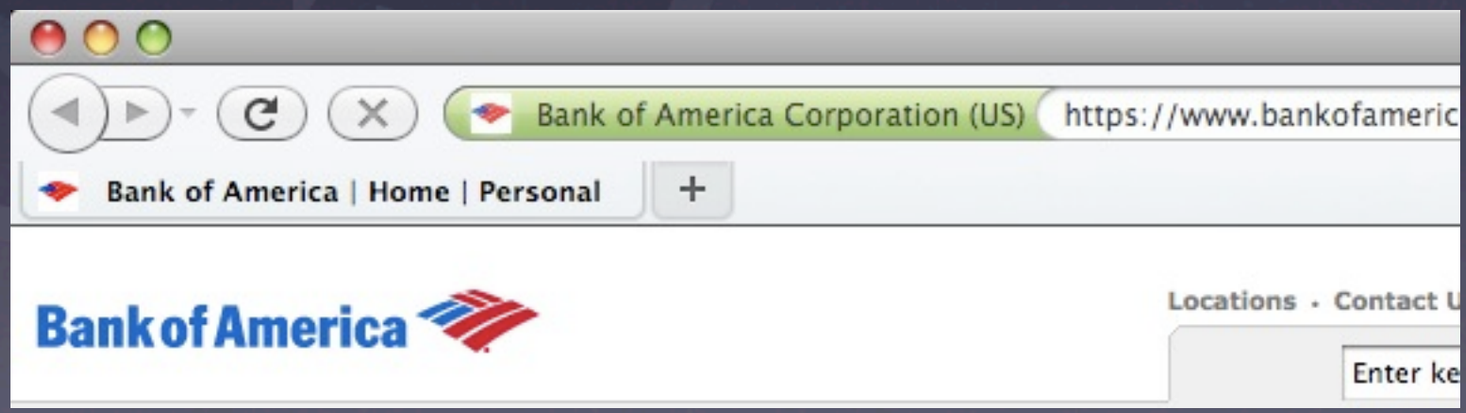


Site Authentication

DV Certificates



EV Certificates



Software Developers

- Security is a characteristic of a product vs. a gate to get through
- Evolution of security within companies: Incident Response ⇢ Penetration Testing ⇢ Security Review ⇢ Design Review ⇢ Requirements Gathering

Security Models

- When you implement new features, you need to have the patience to carefully consider the security model
- Iterating on security models is painful
- Taking away privilege even more so
- Best to start with minimal necessary privilege and add more later

Developer Summary

- Occam's Security Razor: Out of all equally effective solutions, the one requiring least privilege is best
- Security is not something you can "solve"
- Factor security in the cost of ownership - pre-allocate resources to supporting, fixing and updating. If you aren't willing or able to do so, **don't implement it**.

Surprise Test!

- Q: Which cross-domain loading mechanism sends cookies, supports policy files located in the root or explicit subdirectories, but requires you to grant access to all domains?
- A: Java's crossdomain.xml support

Questions?

References

- Download Firefox with CSP: http://blog.mozilla.com/security/2009/09/30/a-glimpse-into-the-future-of-browser-security/
- STS / ForceTLS Add-on: https://addons.mozilla.org/en-US/firefox/addon/12714
- Standards mailing lists: http://www.whatwg.org/mailing-list and http://lists.w3.org/
- Usenet: mozilla.dev.security

References

- Content Security Policy: https://wiki.mozilla.org/Security/CSP
- Origin (aka Sec-From): http://tools.ietf.org/html/draft-abarth-origin-05
- Strict Transport Security / ForceTLS: http://lists.w3.org/Archives/Public/www-archive/2009Sep/att-0051/draft-hodges-strict-transport-sec-05.plain.html
- JSON.parse: http://hacks.mozilla.org/2009/06/security-performance-native-json/
- IE8 XSS Filter: http://blogs.technet.com/srd/archive/2008/08/19/ie-8-xss-filter-architecture-implementation.aspx
- IE8 anti-clickjacking: http://blogs.msdn.com/ie/archive/2009/01/27/ie8-security-part-vii-clickjacking-defenses.aspx

References

- Flash crossdomain.xml: http://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
- Silverlight 2 cross domain loading: http://msdn.microsoft.com/en-us/library/cc197955%28VS.95%29.aspx
- Java cross domain loading: https://jdk6.dev.java.net/plugin2/#CROSSDOMAINXML
- W3C Cross Origin Resource Sharing: http://hacks.mozilla.org/2009/07/cross-site-xmlhttprequest-with-cors/
- XDomainRequest: http://msdn.microsoft.com/en-us/library/cc288060%28VS.85%29.aspx
- postMessage: http://www.whatwg.org/specs/web-apps/current-work/