Designing Trustworthy User-Agents for a Hostile Web

Usenix Security 2009

Eric Lawrence
Program Manager
Microsoft Corporation
About Eric…

● IE8 Program Manager - Security
● IE7 PM – Networking & Trust
● Developer of Fiddler, TamperIE, IEToys
IE 7 significantly reduced attack surface against the browser and local machine...
but...

- WebApp attacks (CSRF, XSS, ClickJacking, splitting) could become the next big vector of exploit.
- More high-value information is moving to the web.
- Social Engineering and exploitation of add-ons continues to grow.
- The Web platform itself is getting richer.
- and the next generation of attackers is coming out of grade school.
Worst of all, it turns out that crime *does* pay (quite well) after all.
Why is browser security so elusive?
Complexity.
The security architecture of the current web platform was largely an afterthought.
Maybe there’s a shortcut?
We could block nearly 100% of exploits by removing just one component from the system...
The Network cable
Or, we could block a majority of exploits by removing a different component from the system...
The user
So, if we re-architect everything, or get rid of the users, or get rid of the network, then security *might be* easy.
Security is straightforward.

Tradeoffs are complicated.
Yes, Microsoft is a big, influential company...
…but the Internet is bigger.
• Many hundreds of millions of users…
• From all over the world…
• Visiting billions of web pages…
• And most don’t really even know what a “browser” is!
The Web is surprisingly fragile.
For most web users, it’s all about value.
The browser that most users will ask for…

Race car
The browser that meets users security expectations…

Amphibious assault tank
Bad guys only need to find one way in…
Security Team’s Investments

- **Security Feature Improvements**
  - Create security features that address the top vulnerabilities today and in the future

- **Secure Features**
  - Reduce attack surface of existing code by closing legacy holes
  - Apply security-focused rigors against new code

- **Provide Security and Compatibility**
  - Users understand that improved security is a reason to upgrade
Threat Focus Areas

Address the evolving threat landscape

- Browser & Add-on Vulnerabilities
- Social Engineering
- Web App Vulnerabilities
ActiveX

ActiveX controls in CVE

- All ActiveX controls
- MSFT ActiveX controls


14 4 7 7 6 4 14 10 9 5 12 5 14 3 65 18 231 16
ActiveX Gauntlet

- Has control been flagged as unsafe? (ActiveX Killbits)
- Safe for scripting / initialization (IObjectSafety)
- Is control permitted to run in browser without prompt? (AX Opt-in)
- Is control permitted to run on this site? (PerSite AX)
Per-site ActiveX

- Helps prevent repurposing of ActiveX controls
Data Execution Prevention

- Mitigates many memory-related vulnerabilities by blocking code execution
- Other protections like ASLR, SAFESEH, GS, etc

![Webpage error]

Internet Explorer has closed this webpage to help protect your computer

A malfunctioning or malicious add-on has caused Internet Explorer to close this webpage.

What you can do:
- Go to your home page
- Try to return to ie8demos.com

More information

Windows Data Execution Prevention detected an add-on trying to use system memory incorrectly. This can be caused by a malfunction or a malicious add-on.

Other things you can do:
- Go online to learn about the Data Execution Prevention (DEP) security feature
Protected Mode

- Browser/Add-on Vulnerabilities

- IExplore.exe in Protected Mode
  - Integrity Control and UIPI
  - IEinstall.exe

- Install ActiveX Control
  - Change Settings, Drag & Drop

- Restricted Settings and Files
  - Cached Web Content

- Admin-Rights Access
  - HKEY_LOCAL_MACHINE
    - Program Files

- User-Rights Access
  - HKEY_CURRENT_USER
    - My Documents
    - Startup Folder

- Temporary Internet Files
- Untrusted Files and Settings
Protected Mode

- Loosely-coupled IE enables one frame to host both Low and Medium tabs
- Intranet Zone moved to Medium Integrity by default
- Silent Elevation List split
- Minor API improvements
  - DWebBrowserEvents2::NewProcess
  - IE[Get|Set]ProtectedModeCookie
  - IERefreshElevationPolicy (IE7 GDR)
  - *Other registry/filesystem helpers.*
What’s the best way to develop secure, performant, and reliable C/C++ code?
Don’t.
Non-Binary Extensibility
Accelerators

15802 NE 83rd Street
Redmond, WA 98052

Phone: (425) 702-1645
Fax: (425) 702-1645

Map with Live Search
WebSlices

Weather in San Jose, CA

54°F

Wind: 5 mph W

69° / 47° Humidity: 76%

70° / 46° 66° / 41° 59° / 41° 50° / 37°

Ten Day Forecast · Hourly Forecast · Weather Maps · Data provided by WDT

Helpful? Yes | No

Internet Explorer

Add a Web Slice

Get updated Web Slice content from this webpage and view it from your Favorites bar.

Name: Weather in San Jose, CA

From: http://search.live.com/webslices/answer.aspx?q=san jose weather...

What are Web Slices?

Add to Favorites Bar | Cancel

EnhanceIE.com - Your source for Internet Explorer Enhancements - Windows Internet Explorer 6.0 impoverished Edition

Weather in San Jose, CA

54°F Wind: 5 mph W

69° / 47° Humidity: 76%

Ten Day Forecast · Hourly Forecast · Weather Maps · Data provided by WDT

http://www.enhanceie.com/ie/
Visual Search Suggestions
Sometimes, threats are obvious...
...but bad guys are getting smarter...
Fake codecs and add-ons
Fake antivirus scanners & utilities
Try as we might...

...we haven’t figured out how to patch the user.
“Don’t ask my users to make security decisions.”

Policies include:

- Treat certificate errors as fatal
- Block insecure content
- Prevent bypass of SmartScreen Filter warnings
- Regulate ActiveX control install & availability

IE8 includes over 1400 group policy controls.
What if we can’t get rid of the user?
Do you want to run or save this file?

Name: zoneviewsetup.exe
Type: Application, 55.6KB
From: www.enhanceie.com

Run  Save  Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?
Do you want to run or save this file?

Name: zoneviewsetup.exe
Type: Application, 55.6KB
From: www.enhanceie.com

I'm Feeling Lucky  Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?
A more effective warning?
SmartScreen Download Block

Unsafe Download - Security Warning

This download has been reported as unsafe

The file you are downloading has been reported to be unsafe. The download website contains links to viruses or other software that can harm your computer or reveal your personal information.

For your safety, we recommend you cancel this file download.

Disregard and download unsafe file (not recommended)

Report that this download is safe

Cancel
This website has been reported as unsafe

207.68.169.170

We recommend that you do not continue to this website.

Go to my home page instead

This website has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

More information
Domain Highlighting
HTTPS - Extended Validation

- Supported by all modern browsers.
- Over 10,000 sites with extended validation certificates.
International Domain Names

- Protects against homograph style phishing attacks
- Unicode display restricted to user’s configured languages
HTTPS Mistakes
Insecure Login Form
Certificate Mismatch

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

- Click here to close this webpage.
- Continue to this website (not recommended).

More information

- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.
- If you choose to ignore this error and continue, do not enter private information into the website.
Mixed Content - Prompt

Security Warning

Do you want to view only the webpage content that was delivered securely?

This webpage contains content that will not be delivered using a secure HTTPS connection, which could compromise the security of the entire webpage.

More Info Yes No
Mixed Content Blocked

This page should be secure. The image below is not.
Mixed Content shown – No lock

This page should be secure. The image below is not.
Mitigating XSS
XSS Statistics

- XSS: 70%
- Info Leakage: 4%
- Content Spoofing: 6%
- SQL Leakage: 5%
- Predictable Resource Location: 5%
- HTTP Response Splitting: 5%
- Other: 6%

XSS Threats

Researcher Bryan Sullivan: “XSS is the new buffer overflow.”

- Steal cookies
- Log keystrokes
- Deface sites
- Misuse credentials
- Port-scan the Intranet
- Launch CSRF
- Steal browser history
- Abuse browser/AX vulnerabilities
- Evade phishing filters
- Circumvent HTTPS
- etc…
IE8 XSS Filter
Comprehensive XSS Protection

- Disable US-ASCII codepage
- Disable sniffing of UTF-7 codepage
- Fix other codepage-related bugs
- Disable CSS expression() in IE8 Standards mode
- Offer script-sanitization functions for sites building mashups
Securing Mashups
How are mashups built today?

• Cross-domain script inclusion
• IFRAMES

```html
<script type="text/javascript"
    src="http://syndication.example.com/pagead/show_ads.js">
</script>
```
**XDomainRequest**

- Enables web developers to more securely communicate between domains
- Provides a mechanism to establish trust between domains through an explicit acknowledgement of cross domain access
- **Access-Control-Allow-Origin** syntax standardized
**HTML5 postMessage()**

- Enables two domains to establish a trust relationship to exchange object messages.
- Provides a web developer a more secure mechanism to build cross-domain communication.
- Part of the HTML5 specification; supported by all latest-version browsers.
// Find target frame
var oFrame =
document.getElementsByTagName('iframe')[0];

// postMessage will only deliver the 'Hello'
// message if the frame is currently
// at the expected target site
oFrame.contentWindow.postMessage('Hello',
    'http://recipient.example.com');
// Listen for the event. For non-IE, use
// addEventListener instead.

document.attachEvent('onmessage',
    function(e){
        if (e.domain == 'expected.com') {
            // e.data contains the string
            // We can use it here. But how?
        }
    });
JavaScript Object Notation

```json
{
"Weather":
{

"City": "Seattle",
"Zip": 98052,
"Forecast": {

"Today": "Sunny",
"Tonight": "Dark",
"Tomorrow": "Sunny"

}

}

}```
Native JSON Support

- JSON.stringify()
- JSON.parse()

Based on ECMAScript 3.1; natively supported by modern browsers.
Client-side string sanitization, based on the Microsoft Anti-XSS Library.

```javascript
window.toStaticHTML(
  "This is some <b>HTML</b> with embedded script following... <script>alert('bang!'); </script>!"
);
```

returns:

```
This is some <b>HTML</b> with embedded script following... !
```
if (window.XDomainRequest){
    var xdr = new XDomainRequest();

    xdr.onload = function(){
        var objWeather = JSON.parse(xdr.responseText);

        var oSpan = window.document.getElementById("spnWeather");
        oSpan.innerHTML = window.toStaticHTML("Tonight it will be <b>
        objWeather.Weather.Forecast.Tonight +
        "</b> in <u>" + objWeather.Weather.City + "</u>.");
    }

    xdr.open("POST", "http://evil.example.com/getweather.aspx");
xdr.send("98052");
}
MIME-Sniffing

- No upsniff from image/*
- X-Content-Type-Options: nosniff
- Option to force file save:
  
  Content-Disposition: attachment; filename="file.htm";
  X-Download-Options: NoOpen
Best Practices

- Filter content using the Microsoft Anti-Cross Site Scripting Library.
- Use JSON, toStaticHTML for local content sanitization
- Specify encoding using in the Content-Type header:
  ```plaintext
  Content-Type: text/html; charset=UTF-8
  ```
- Use XDomainRequest and postMessage() rather than using `<SCRIPT SRC=>`
- Use HTTPOnly cookies
  ```plaintext
  Set-Cookie: secret=value; httponly
  ```
Design Flaws in the Web Platform
Privacy
File Upload Control

- Text input control now read-only

  ![Browse Button]

Server no longer gets full filename:

```
Content-Disposition: form-data;
    name="file1"; filename="File.zip"
```

Local JavaScript sees a fixed path for compatibility:

```
file1.value == "C:\fakepath\File.zip"
```
Enhanced Cleanup

**Browsing history**
Delete temporary files, history, cookies, saved passwords, and web form information.

- [x] Delete browsing history on exit

**Delete Browsing History**
- [x] **Preserve Favorites website data**
  Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.
- [x] **Temporary Internet files**
  Copies of webpages, images, and media that are saved for faster viewing.
- [x] **Cookies**
  Files stored on your computer by websites to save preferences such as login information.
- [x] **History**
  List of websites you have visited.
- [x] **Form data**
  Saved information that you have typed into forms.
- [x] **Passwords**
  Saved passwords that are automatically filled in when you sign in to a website you've previously visited.
- [x] **InPrivate Filtering data**
  Saved data used by InPrivate Filtering to detect where websites may be automatically sharing details about your visit.

**Delete**
**Cancel**
InPrivate™ Browsing

*Shared PC privacy*

- Browsing leaves no tracks locally (cookies, DOMStorage, cache, history, etc)

InPrivate™ Filtering

*Awareness and control of web profile aggregation*

- Assess, on an ongoing basis, user exposure to third-party content.
- Helps to prevent information disclosure by automatically blocking high-frequency third-party content from sites users visit.
InPrivate™ Browsing

InPrivate Browsing helps prevent Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data. Toolbars and extensions are disabled by default.

Learn more about InPrivate
Background on 3rd Party Aggregation

- Over time, users’ history and profiles can be surreptitiously aggregated
  - *Any* third-party content can be used like a tracking cookie
    - There is little end-user notification or control today
    - Syndicated photos, weather, stocks, news articles; local analytics, etc.…
  - Unclear accountability with third party security & privacy policies
Are we finished yet?
Questions?
dericlaw@microsoft.com
HTTP Response

- HTML MIME Type?
  - NO
  - YES
    - Different Referer?
      - NO
        - NO
        - NO
          - Signature match on HTTP response body?
            - YES
              - Log results and inform the user that a XSS attack has been blocked
            - NO
              - Neuter appropriate characters for each signature match
        - NO
          - Build a signature for each heuristic match
    - YES
      - YES
        - YES
          - Provide HTTP Response to Web Browser
      - NO
      - NO
      - NO
      - NO
  - NO
  - NO
  - NO