# How to Make Browsers Safer Using Virtualization

Seth Misenar

September 2009

GIAC GSEC, GCIA, GCIH, GCWN, GCFA, GPEN, GWAPT

# Objective

- Browsers now represent critical infrastructure that provide access to sensitive data.
- Browsers and Web Applications have extended far beyond their original use case.
- Enterprises have little choice in browser.
- Attacks against the browser are commonplace.
- Typical one-size fits all approaches to browser security are insufficient.
- Virtualization offers a compelling and different approach to browser security.

# Browser Security Landscape

- The attack surface provided by our browsers has grown exponentially.
  - 3rd party tools/frameworks such as Java, Flash, Acrobat, Quicktime, Silverlight, etc. are increasingly required for site/ application functionality
- Attackers have found ways to monetize these attacks against browsers.
  - More believable phishing
  - Stealing privileged credentials from the browser
  - Enticing the purchase of crimeware
  - Drive-by downloads to install bots

# Browser Security Landscape (2)

- Universal script/active content blocking hinders usability
  - Browsing without any scripting breaks the majority of web applications.
- Site whitelisting/blacklisting isn't sufficient protection
  - 77% of malicious content hosted on trusted legit sites (Websense: State of Internet Security 2008 Q3-Q4)
  - 70 of top 100 sites contain or redirect to malware (Websense: State of Internet Security 2008 Q3-Q4)
  - 1.3% of Google searches return >= 1 malicious URL (All Your iFRAMEs Point to Us by Provos, Mavrommatis, Rajab, Monrose)

# Internet Explorer

- Internet Explorer is the *de facto* browser representing 66% of the market share (http://marketshare.hitslink.com)
- Enterprises typically don't choose Internet Explorer, they simply don't have an *enterprise-ready* choice other than IE.
- Central/Scalable Management is the most significant security feature
  - Security configuration can be centrally managed/mandated using Group Policy
  - Browser updates are handled in the same fashion as Windows updates.

# Internet Explorer - Challenges

- 287 new and distinct ActiveX vulnerabilities during 2008 (Symantec Internet Threat Report 2009)
  - Most represent memory corruption flaws that can allow arbitrary code execution
  - Rise in unauthorized file system access
  - Better default security in IE7 doesn't seem to have impeded attackers
- Updating 3rd party helper applications/components not as easy as IE patching
- Operating System Integration poses heightened risk.
- Still common to have users run Internet Explorer as an administrator
  - IE7/8 with UAC (Windows Vista/7) changes this, but….

# Firefox

- 2nd most popular browser with a 22% share of the market (http://marketshare.hitslink.com)
- Lack of central management represents the most significant enterprise-oriented shortcoming
  - Updates are user driven events
  - No means for centrally controlling the security configuration
  - Extension installation/configuration/update is user-driven
- If installed, typically does not replace Internet Explorer in enterprises
- Shorter time-to-patch after security vulnerabilities announced

# Firefox Extensions

- Simply moving to Firefox is not sufficient to greatly increase browser security over Internet Explorer
  - Secunia reports Firefox 3.0 has suffered 99 vulnerabilities
- **NoScript** – The most important security extension to Firefox.
- Main features include default blocking of Java, JavaScript, and Flash
- With some user awareness training, exceptions can usually be implemented by the end user rather easily
- Default blocking of scripts can reduce exposure to XSS
- **Firekeeper** – Coolest inactive extension that provides in-browser IDS functionality

# Firefox Extensions continued

- **WOT (Web of Trust)** – User driven content filter that integrates into Firefox
  - Ask user for verification before browsing to a site that is considered to be risky
  - Integrates into common webmail and search engine providers to give a visual indicator before the user follows a link
- **Request Policy** – Configures Firefox with a default deny stance for content being requested by other domains
  - Helps to protect against CSRF (Cross Site Request Forgery) attacks. (Some mistakenly believe NoScript protects against this.)
- **Many more**…

# Browser Security Needs

- Centralized Management of updates and configuration
- Protection against "drive-by downloads"
- Ability to run scripts/active content without as much risk
- Lower administrative overhead for exceptions to default security configuration
- Eased application of 3rd party updates
- Actual choice of a browser platform for enterprises
- Virtualization makes a compelling case on these fronts.

# Sandboxie

- Applies the sandbox security model and applies it to locally installed applications
- Not just for Internet Explorer (common misconception)
- Virtualized Registry/File System
  - Sandboxed application accesses virtualized copy of the Registry and File System
  - No permanent changes to Registry or File System (by default)
  - No read access (configurable)
- Drive-by Malware becomes a transient malware infection

# Sandboxie Configuration

- **File/Registry Integrity Controls**
  - **AutoDelete** – Forces the contents of the sandbox to be automatically deleted upon exiting the sandboxed program, blocking permanent writes
  - **AutoRecover** – Can allow for certain folder or registry paths to automatically be recovered upon exiting sandboxed program
    - Can be used in conjunction with AutoDelete to allow for granular control of what gets written permanently
- **Reduce impact of exploitation**
  - **DropAdminRights** – Strips admin privileges from any sandboxed process even if administrative user started the program
- **File/Registry Confidentiality Controls**
  - **ClosedFilePath** – Deny all access, including read, to files/folders in the path
  - **ClosedKeyPath** – Deny all access, including read, to keys in the path

# VMWare ThinApp

- Application Virtualization Tool – not just for browsers
  - Portable application packages are created which contain the application, all settings, and even the runtime environment
    - Administrative privileges are not required
    - Host file system does not have to be leveraged
- Browser can be streamed from network share
  - Per-user profiles and changes are stored in a sandbox stored locally or on a network share (many of the same benefits offered by Sandboxie)
- Application Sync helps to ensure deployed applications check in for updates at each runtime
  - Administrator centrally updates the application package, and all hosts will then run the updated package next time.

# ThinApp Continued

- Enterprises can manage one or simply a few browser configurations as ThinApp packages
  - Allows for installation/configuration/updating of extensions or 3rd party tools centrally in the ThinApp package
- New or different, possibly more secure browsers, can be deployed side-by-side with their predecessors
  - Ease compatibility and user acceptance testing
  - Internet Explorer 8 and 7 used simultaneously
- Broaden the choice of enterprise browser platform
  - Capabilities make Firefox enterprise ready by allowing for central configuration and updating of the browser and its extension/plugins

# Summary

- Threat agents see browsers as high value targets and can make money by attacking them
- Attack surface of our browsers has increased (AJAX, Flash/Flex/AIR, Silverlight)
- Browsers are incredibly hard to secure with built-in tools, if usability remains a goal
- Central patching (of the browser and all extensions/ supporting code), configuration, and management of browsers is a necessity
- Virtualization technologies such as Sandboxie and ThinApp offer a compelling alternative to the standard approach to browser security