Attack Surface Reduction

What is Attack Surface?

- **Attack surface:** is the exposure to malicious activity.

- **Attack Surface Reduction:** Reducing the total reachable and exploitable vulnerabilities on a system, application or Network

Attack Surface Examples

- Examples of attack surface in the real world include:
  - Open ports on outward facing web and other servers, code listening on those ports
  - Services available on the inside of the firewall
  - Code that processes incoming data, email, XML, office documents, industry-specific custom data exchange formats (EDI)
  - Interfaces, SQL, web forms
  - An employee with access to sensitive information is socially engineered

Why Attack Surface Reduction?

Defending against the attack

Defending against the vector

Example: SQL Injection

- SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution.

- Common Expression used for SQL injection detection 'OR 1=1‘

- Any signature that evaluates to true will work

Tools and Techniques

Defending Against the Attack

- Intrusion Prevention System (IPS)
- Anti-virus
- Blacklist
- Patching
- Web Application Firewall (WAF)

Defending Against the Vector

- Least Privilege Configuration
- Disable Services
- Firewall
- Whitelist
- Code Changes
- Microsoft Enhanced Mitigation Experience Toolkit (EMET)

Attack Surface Reduction and Memory Attacks

- Memory attacks are popular right now
- Memory attack: Any attack where the attacker does not modify the hard disk in any way
- Because these attacks never touch disk, they are nearly impossible to detect or stop by “defending against the attack”

Three Types of Attack Surface

- **Network Attack Surface:** The attack is delivered via a network
- **Software Attack Surface:** The attack is delivered against software with a primary focus on web applications
- **Human Attack Surface:** The attack is delivered against a human in such forms as social engineering, errors, trusted insider, death and disease

Software Attack Surface

- We are spending more money to develop an increasing number of web applications that are often mission critical.
- At the same time attackers are getting better at exploitation of web applications.
- At the same time companies like Ameritrade and TJX have suffered massive data breaches leading to class action lawsuits and potentially, another wave of government regulations

An Attack Surface Analysis of the Browser

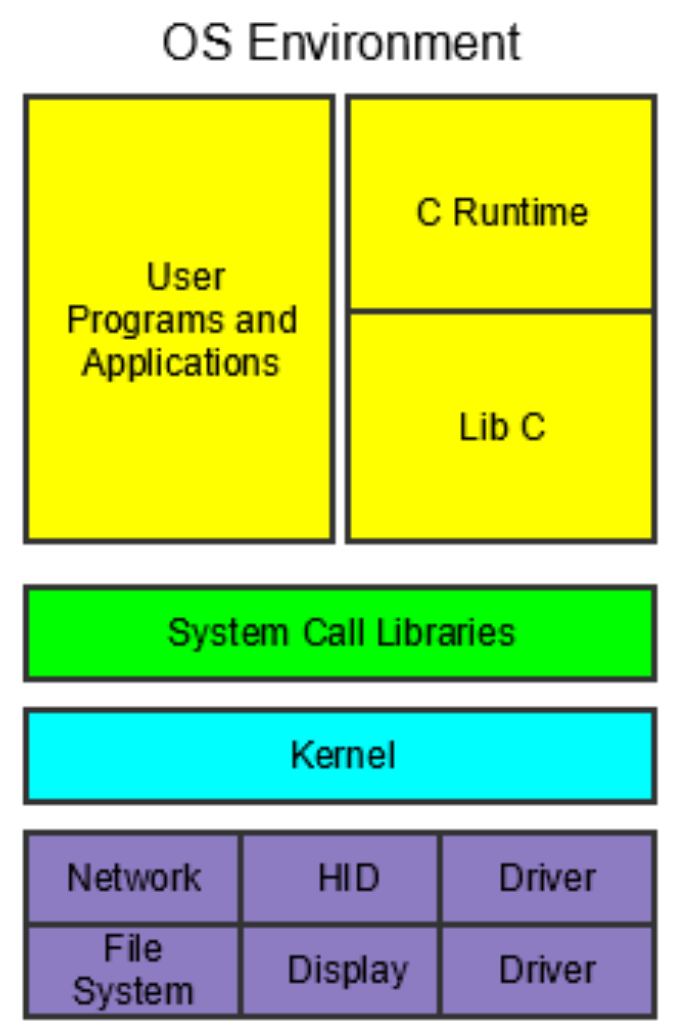
Review: Attack Surface Reduction Steps

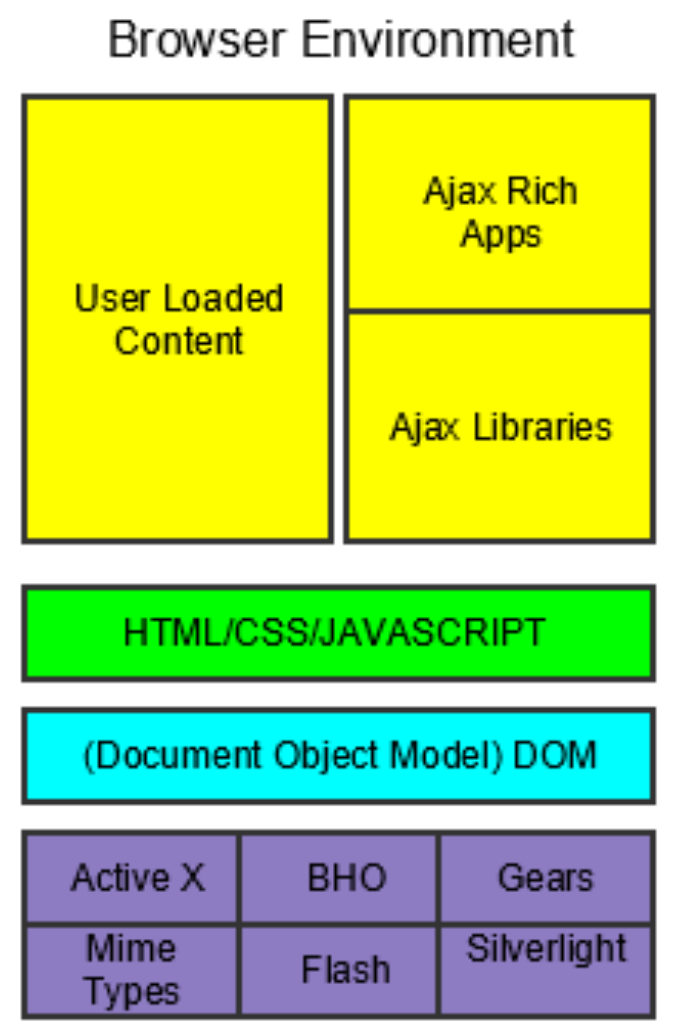
1. Define the application or system
2. Research the attack methodologies
3. Create a refined list of attack vectors that are utilized by the above attack methodologies
4. Determine the optimal way to restrict or disable the available service vector

Step 1: We Chose The Web Browser

- Receives instructions from the internet and executes them
  - Uncontrolled instructions by defender
  - Some instructions tell the browser to execute additional instructions from untrusted locations and sources
  - Some instructions tell the browser to send TCP data to other network resources
  - Instructions are encrypted, often not allowing a defender to see the transmission
- The attack surface is continually increasing
- It often updates in the background without notification
- It depends on plugins (3rd party untrusted code) for effective use
  - The plugins are often more vulnerable than the original code
  - Every variant of this software has numerous vulnerabilities

A Browser / Operating System Comparison





The browser architecture is important to understand when discussing exploits.

The browser architecture is very similar to the way an operating system works.

Step 2: Attack Methodologies

Step 2a. Define Attack Categories

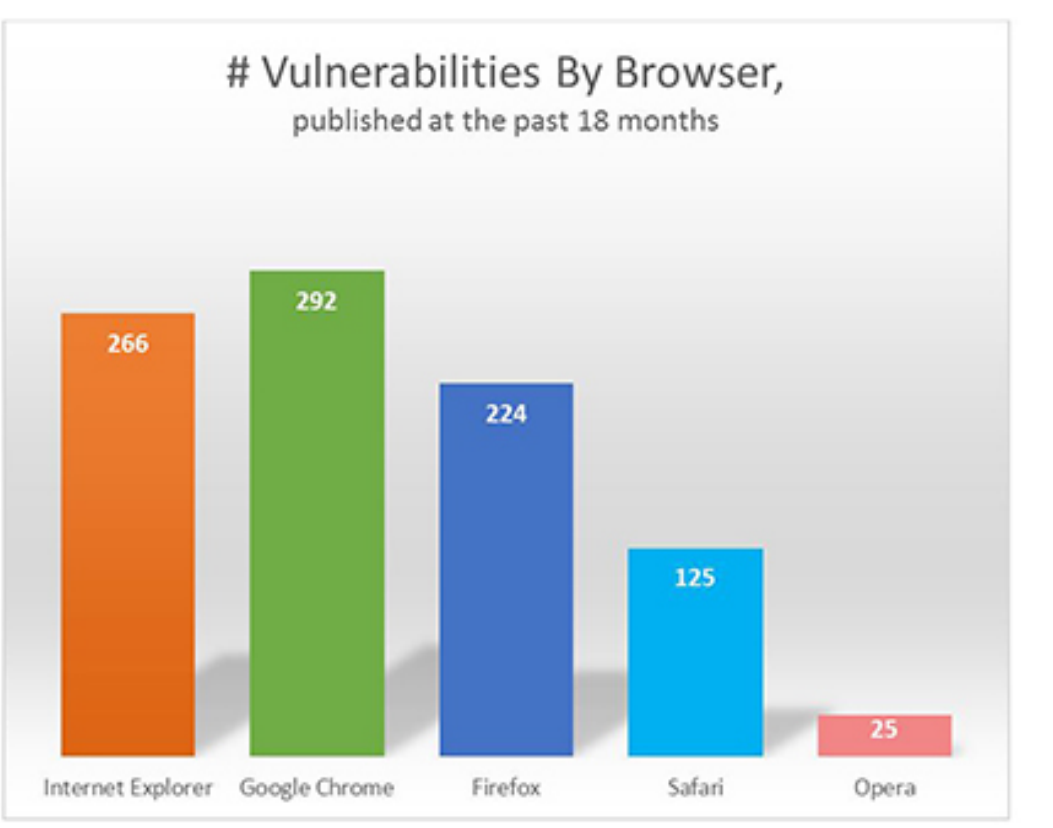
Matrix

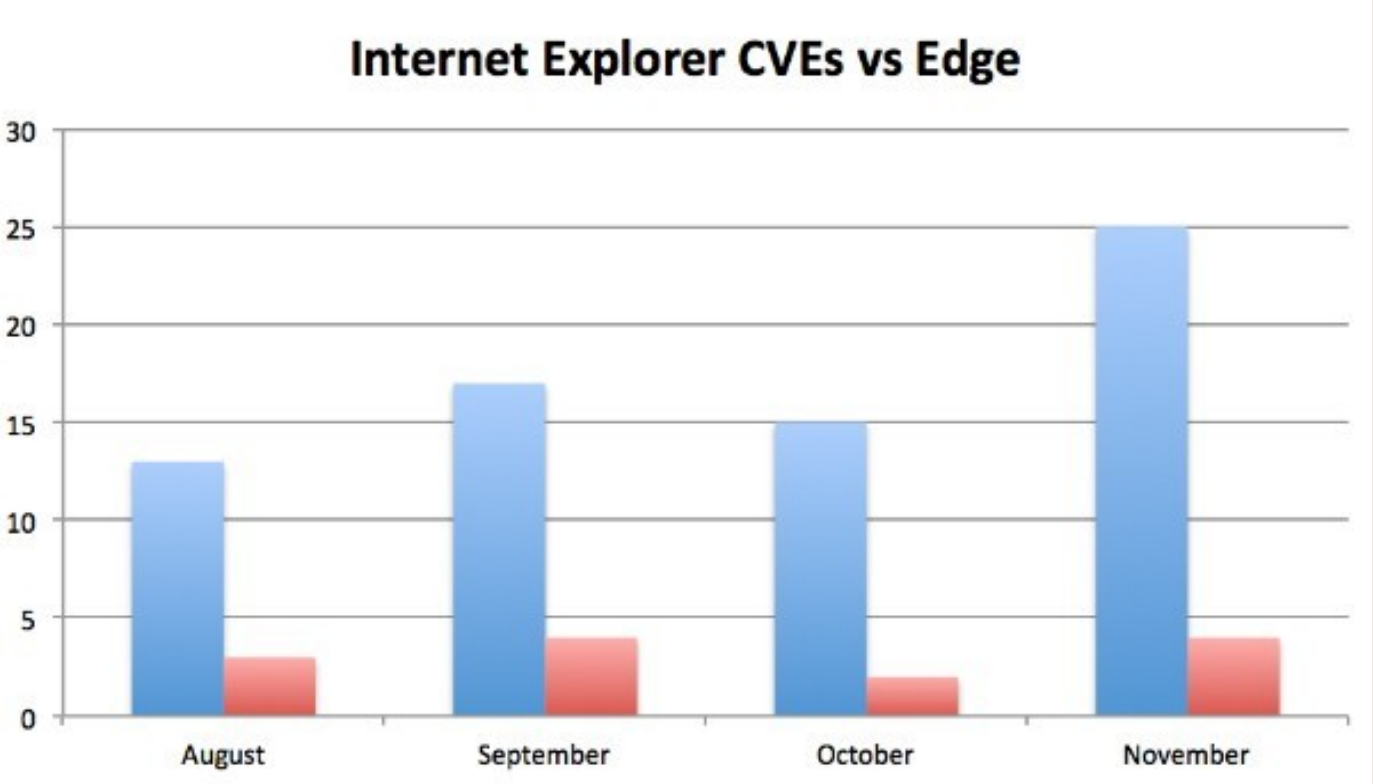
Plugins	Attacking ActiveX Controls	Active X
Web Application	Sending Cross-origin Requests, Enumerating Cross-origin Quirks, Preflight Requests, Implications, Cross-origin Web Application Detection, Discovering Intranet Device IP Addresses, Enumerating Internal Domain Names, Requesting Known Resources, Cross-origin Authentication Detection, Cross-site Request Forgery, Attacking Password Reset with XSRF, Using CSRF Tokens for Protection, Cross-origin Resource Detection, Cross-origin Web Application Vulnerability Detection	Bypass Same Origin Policy
User	Signed Java Applet, Bypass Anonymization	Java
Plugins	Attacking Java	
Network	Ping Sweeping using Java, Getting Shells	

User	Change page content, Capture user input, Log where user clicks, Log mouse events, Log form events, Log keyboard shortcuts, Tabnabbing, Phishing, Fake Software Update, Bypass Anonymization, Hack Password Managers	JavaScript
Browser	Bypassing Path Attribute Restrictions, Sidejacking Attacks, Attack Javascript, JavaScript Encryption, Java Heap, Abusing Schemes	
Extensions	Exploring Privileges, Attacking Extensions, Impersonating Extensions, Cross-context Scripting, Achieving OS Command Execution, Achieving OS Command Injection	
Plugins	Attacking Plugins, Bypassing Click to Play	
Network	Identifying the Hooked Browser's Internal IP, Identifying the Hooked Browser's Subnet, Ping Sweeping, Port Scanning, Bypassing Port Banning, Distributed Port Scanning, Fingerprinting Non-HTTP Services, Attacking Non-HTTP Services, NAT Pinning, Achieving Inter-protocol Communication, Achieving Inter-protocol Exploitation	

What Can I do?

Browser Choice

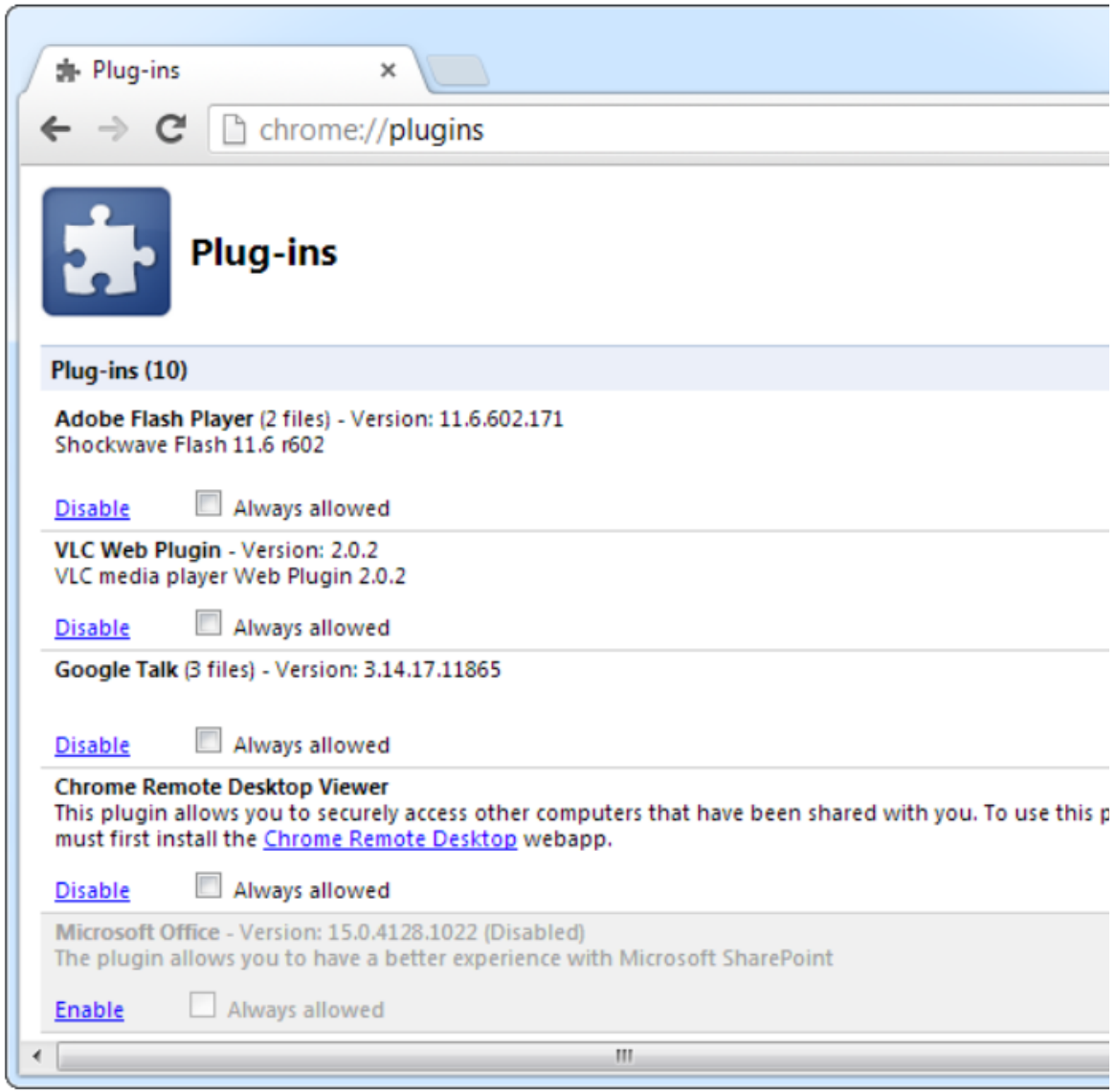


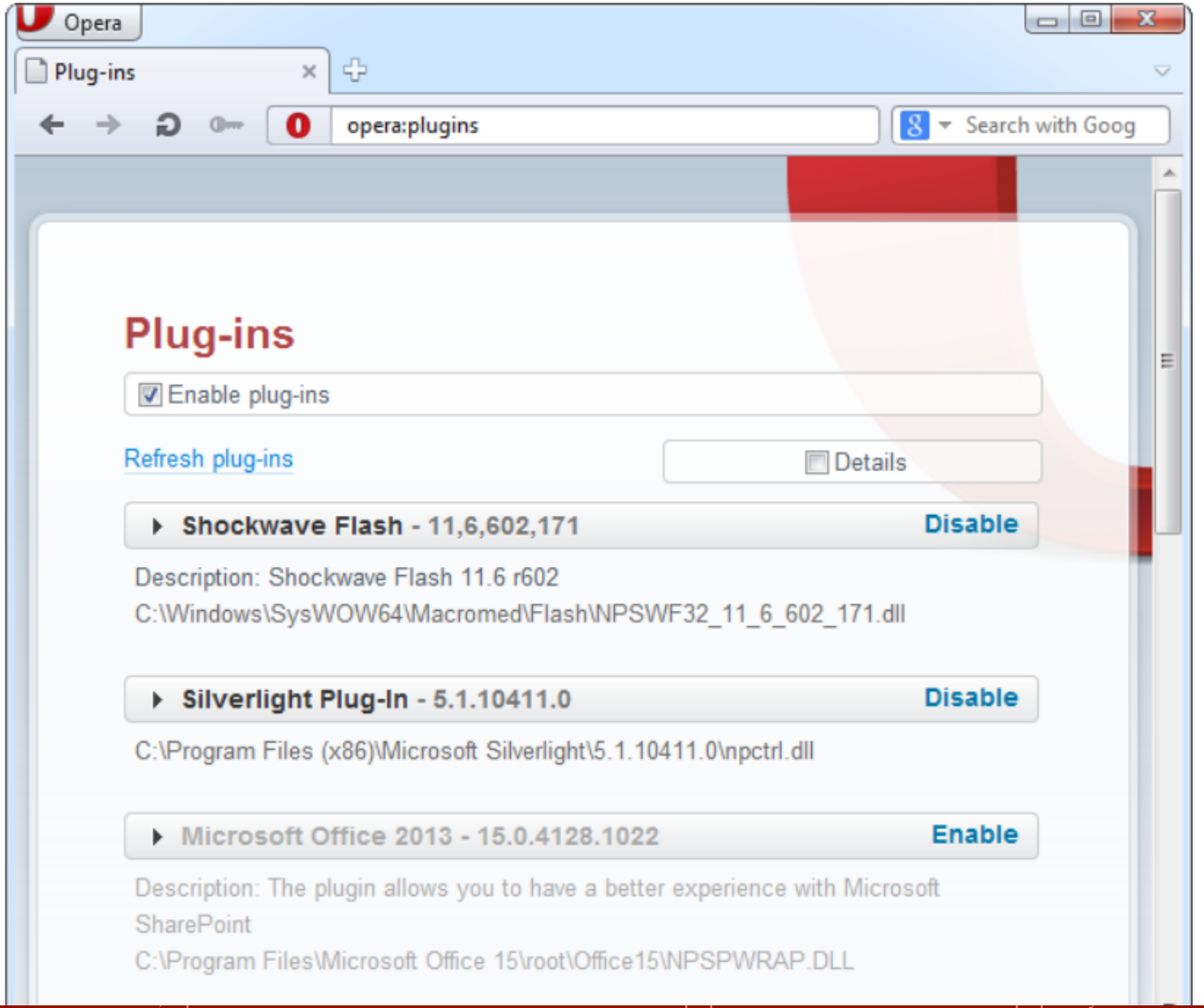


Internet Explorer Browser Plugins for Security

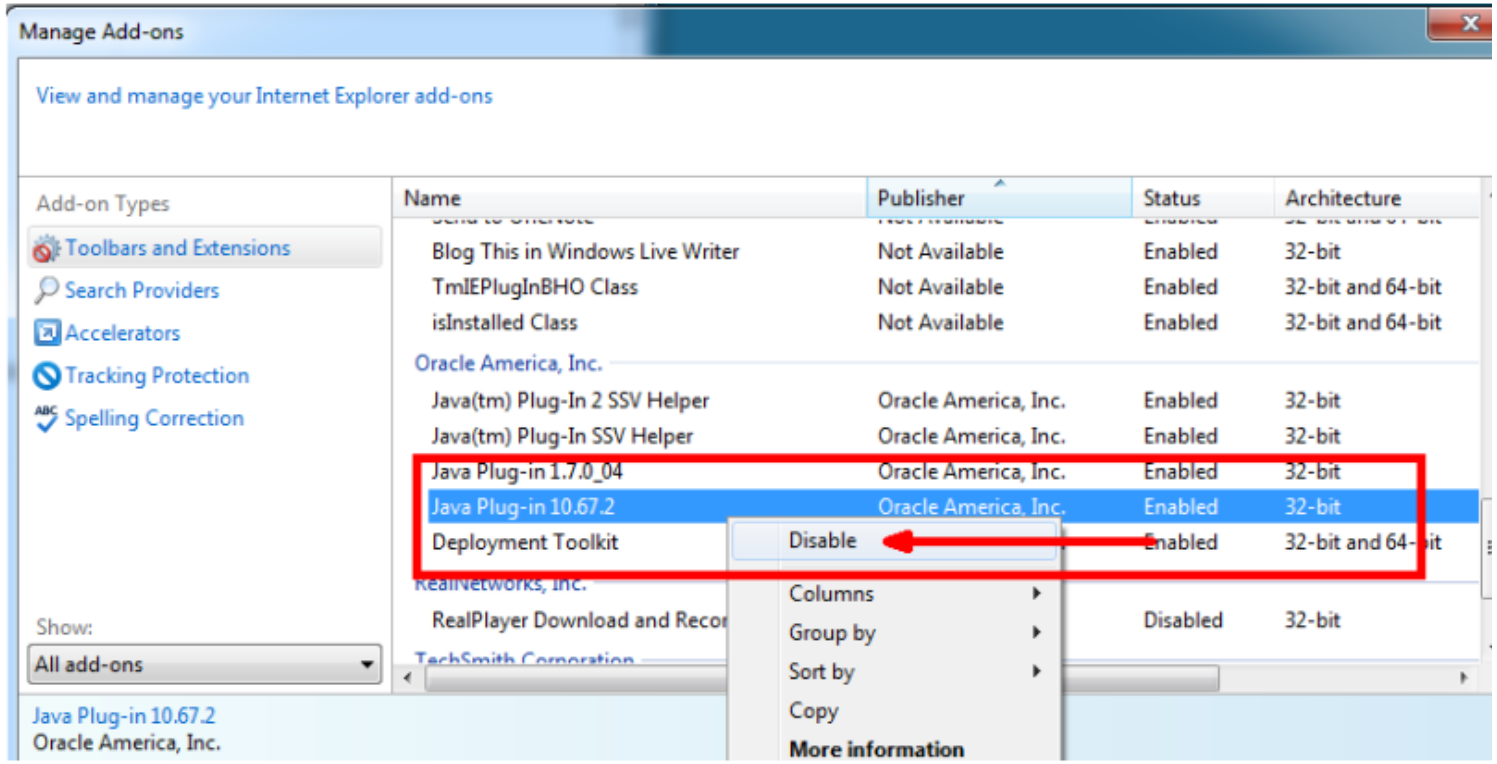
Plugin	Description
McAfee SiteAdvisor	IE Add-on lets you know whether a site is safe to surf based on McAfee's research.
Web of Trust	IE Add on let's you know if sites are safe to search based on user feedback.
LastPass	Replaces the automated password manager. Encrypts your password and stores it in an online database and replaces your multiple logins and passwords with a single master password.
Realtime Cookie & Cache Cleaner	Removes stored cookies and clears your browser cache as you surf.
Spywall Anti-Spyware	IE add on that sandboxes the browser keeping internet explorer from executing commands to the rest of the PC.
AdBlock Pro	AdBlock Pro stops the majority of web ads from appearing
Xss Filter	Limits Script Execution

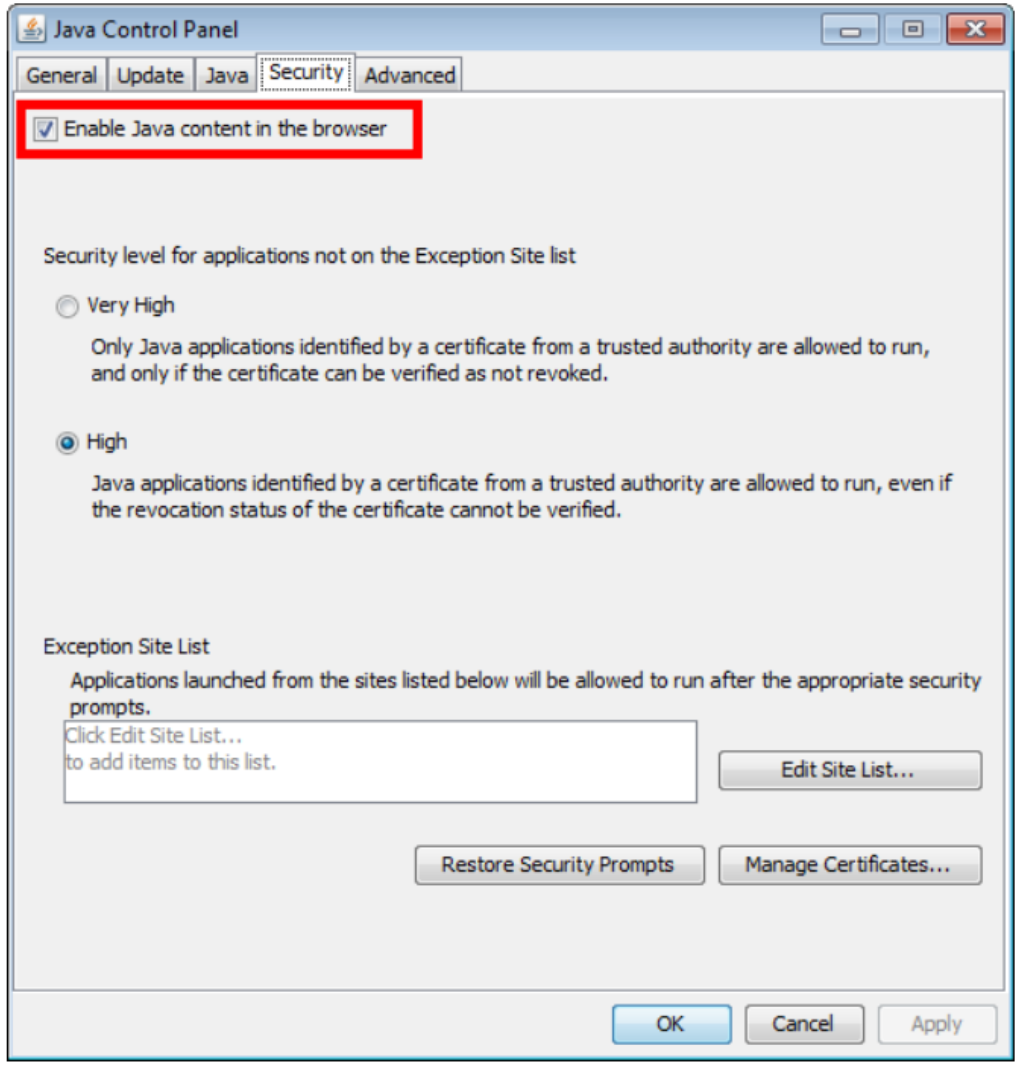
Sometimes Plugins are Hidden





Disable Add On (Java)





Microsoft's Guide to Reducing the Attack Surface of a Web Server

Figure 3.2 Reducing the Attack Surface of the Web Server

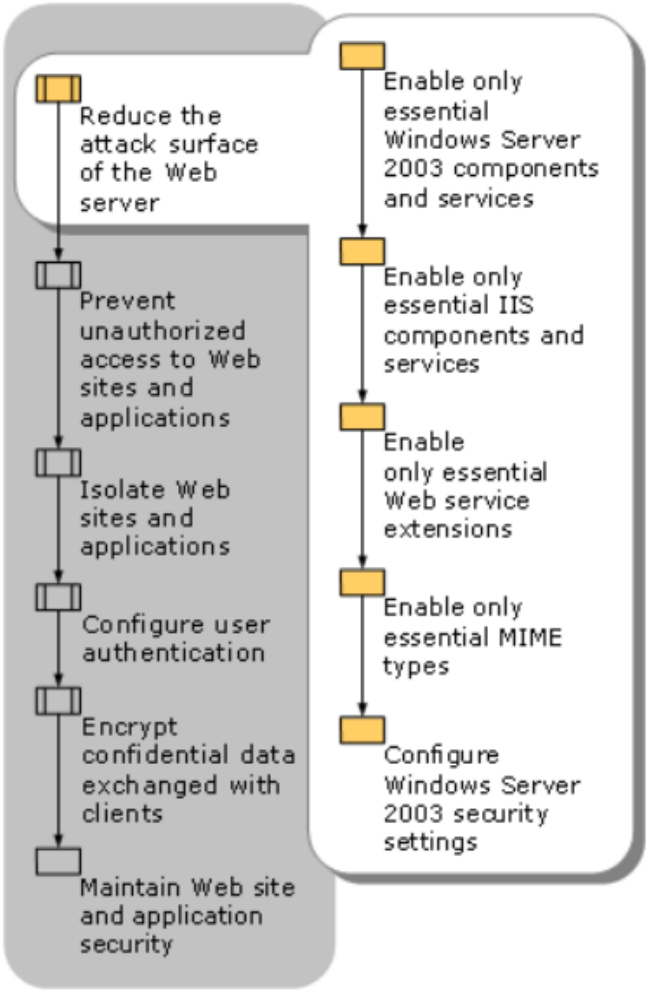


Table 3.1 Recommended Service Startup Types on a Dedicated Web Server

Service Name	Default Startup Type	Recommended Startup Type	Comment
Alerter	**Disabled**	No change	Notifies selected users and computers of administrative alerts.
Application Layer Gateway Service	**Manual**	No change	Provides support for application-level plug-ins and enables network and protocol connectivity.
Application Management	**Manual**	See comment	Provides software installation services for applications that are deployed in **Add or Remove Programs** in Control Panel. On a dedicated Web server, this service can be disabled to prevent unauthorized installation of software.
Automatic Updates	**Automatic**	See comment	Provides the download and installation of critical Windows updates, such as security patches and hotfixes. This service can be disabled when automatic updates are not performed on the Web server.

https://technet.microsoft.com/en-us/library/cc785139(v=ws.10).aspx

Web Application Protection

- https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
- https://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet
- https://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet
- https://www.owasp.org/index.php/AJAX_Security_Cheat_Sheet
- https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
- https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet

Least Privilege

- The role of system administrator should be limited to as small a group as possible.
- Implement fine grained access privileges when a specific task requires elevated privileges
- Separate system administration from regular account requirements
- Separate the system administrator and audit/logging functions.
- Never browse the web as an administrator

Enforcing Least Privilege (NSA Recommendations)

- **Windows AppLocker:** Tie execution of an application to a particular user or group

- **Prevent Browser Internet Access:** In the high-privileged account, set the browser proxy to 127.0.0.1 to prevent the browser from accessing the Internet with elevated privileges.

- **Disable E-mail:** Do not enable e-mail for the high privileged accounts.

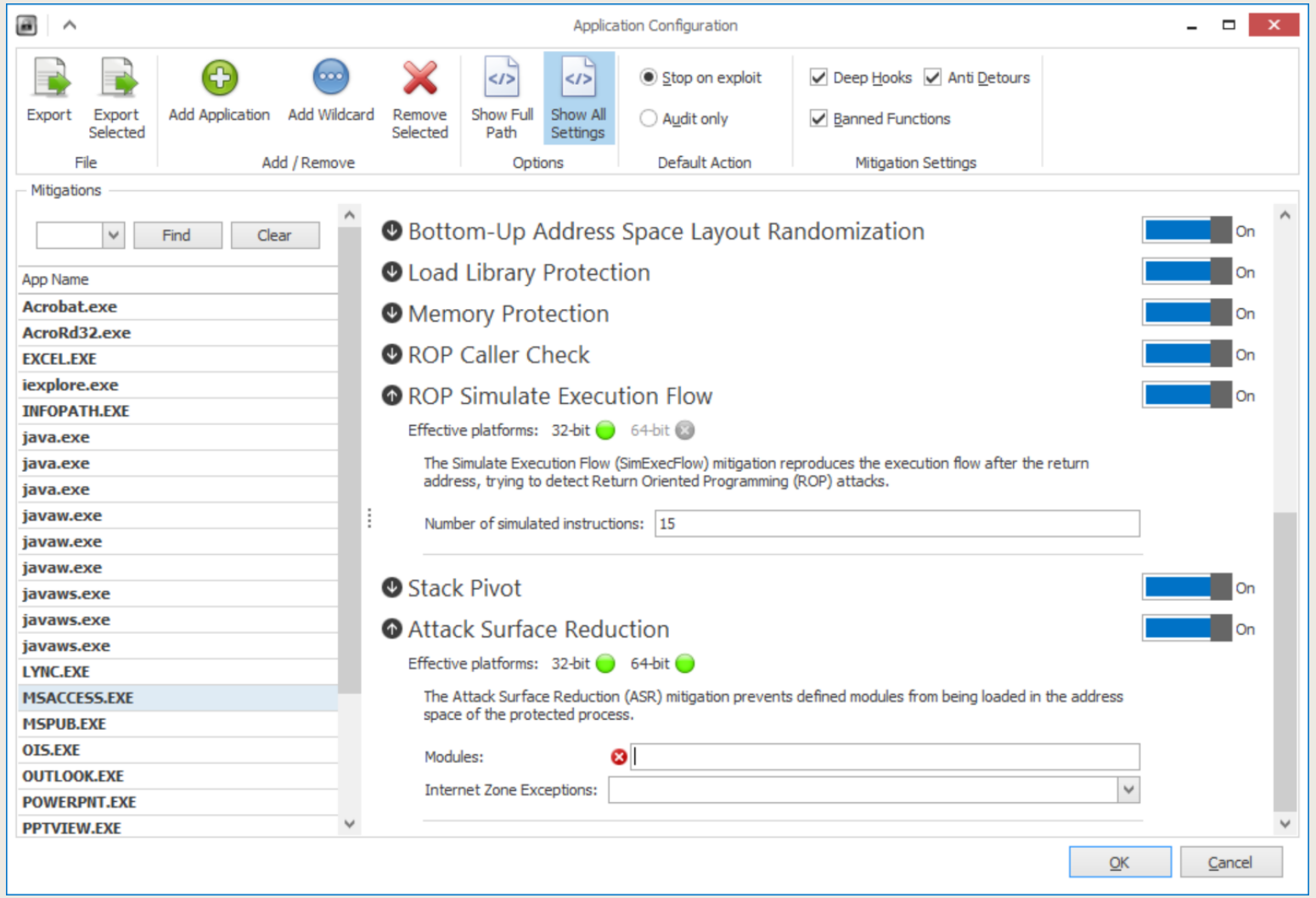
https://www.nsa.gov/ia/_files/factsheets/Final_49635NonInternetsheet91.pdf

Browser Attack Surface Reduction Techniques

Disable firewall traversal
Disable Network Prediction
Disable sharing with cloud peripherals
Disable Google Data Synchronization
Block desktop notifications, Disable pop-ups
Disable 3D Graphic APIs
Disable Javascript in all available locations
Disable Autocomplete on Forms
Update browser and plugins regularly
Block third party cookies
Disable Session Only Cookies
Disable background processing
Enable Revocation Checks for Certificates
Disable Search Suggestions
Disable Metrics Reporting
Set Home Page
Disable Incognito Mode

Disable cleartext passwords
Disable password manager
Disable Import of saved passwords
Set highest HTTP Authentication Scheme
Disable Outdated Plugins
User permission to run plugins
Disable automatic plugin search
Disable automatic plugin installation
Disable automatic plugin execution
Blacklist/whitelist plugins and extensions
Limit plugins to specific URL
Use Encrypted Searching
Enable Safe Browsing
Disallow Location Tracking
Save Browser History
Set the Default search provider name

EMET ASR



- Generic plugin blocker
- Works primarily with Internet Explorer
- Works with MS Office programs such as Word, Excel and Powerpoint.
- If a certain plugin is detected in a protected application ASR will not allow the specified plugin to load in the protected application.
- In Internet explorer the plugin can be blocked by security zone.

Demonstration