DISA's Application Security and Development STIG: How OWASP Can Help You

Jason Li
Senior Application Security Engineer
jason.li@aspectsecurity.com

AppSec DC
November 12, 2009

The OWASP Foundation
http://www.owasp.org
About Me

- Senior Application Security Engineer
  - Five different organizations
  - 12 applications validated against ASD STIG this year
  - CAT I’s in almost all of them!

- OWASP Global Projects Committee member
- Star Trek Fan
- Ballroom Dancer
About DISA

- Defense Information Systems Agency
- Part of the Department of Defense
- Administers and protects DoD command and control systems and enterprise infrastructure
About DISA STIGs

- Offers configuration guides and checklists for:
  - Databases
  - Operating Systems
  - Web Servers
  - Etc...

- Provides standard “findings” and impact ratings
  - CAT I, CAT II, CAT III
First draft November 2006; first release July 2008

129 requirements covering:

- Program Management
- Design & Development
- Software Configuration Management
- Testing
- Deployment
Application Security and Development STIG

- ASD STIG applies to “all DoD developed, architected, and administered applications and systems connected to DoD networks”
- Essentially anything plugged into DoD
Application Security and Development STIG

- Requirements can be extremely broad:
  - e.g. APP3510: The Designer will ensure the application validates all user input
  - e.g. APP3540: The Designer will ensure the application is not vulnerable to SQL Injection
Requirements can be extremely specific:

- e.g. APP3390: The Designer will ensure users accounts are locked after three consecutive unsuccessful logon attempts within one hour.
Requirements can be esoteric:

- e.g. APP3150: The Designer will ensure the application uses FIPS 140-2 validated cryptographic modules to implement encryption, key exchange, digital signature, and hash functionality.
Application Security and Development STIG

Requirements can be expensive:

- e.g. APP2120: The Program Manager will ensure developers are provided with training on secure design and coding practices on at least an annual basis
Lost in the Weeds
Roadmap to Success

Start Right

Improve Developer Awareness

Watch Out For Gotchas

Do Self Validation
Start Right

- Allocate Time
  - Proper allowances in scheduling are key!

- Improve Acquisitions
  - See
    - OWASP Secure Software Development Contract Annex

- Become Aware
  - See
    - OWASP Application Security Verification Standard
Improving Developer Awareness

- OWASP Top Ten provides a high level overview

- OWASP Development Guide provides more specific development guidance

- OWASP ESAPI Project provides standard controls
## Improving Developer Awareness

<table>
<thead>
<tr>
<th>OWASP Top Ten 2007</th>
<th>ASD STIG</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 – Cross Site Scripting</td>
<td>APP3580</td>
</tr>
<tr>
<td>A2 – Injection Flaws</td>
<td>APP3540, APP3570</td>
</tr>
<tr>
<td>A3 – Malicious File Execution</td>
<td>APP3740</td>
</tr>
<tr>
<td>A4 – Insecure Direct Object Reference</td>
<td>APP3450, APP3480, APP3620</td>
</tr>
<tr>
<td>A5 – Cross Site Request Forgery</td>
<td>N/A</td>
</tr>
<tr>
<td>A6 – Information Leakage and Improper Error Handling</td>
<td>APP3120, APP3620</td>
</tr>
<tr>
<td>A7 – Broken Authentication and Session Management</td>
<td>APP3460, APP3415, APP3420, APP3430</td>
</tr>
<tr>
<td>A8 – Insecure Cryptographic Storage</td>
<td>APP3210, APP3340</td>
</tr>
<tr>
<td>A9 – Insecure Communications</td>
<td>APP3250, APP3330</td>
</tr>
<tr>
<td>A10 – Failure to Restrict URL Access</td>
<td>APP3620</td>
</tr>
</tbody>
</table>
## Improving Developer Awareness

<table>
<thead>
<tr>
<th>OWASP Top Ten 2004</th>
<th>ASD STIG</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 2004 – Unvalidated Input</td>
<td>APP3510</td>
</tr>
<tr>
<td>A2 2004 – Broken Access Control</td>
<td>APP3470, APP3480</td>
</tr>
<tr>
<td>A3 2004 = A7 2007</td>
<td></td>
</tr>
<tr>
<td>A4 2004 = A1 2007</td>
<td></td>
</tr>
<tr>
<td>A5 2004 – Buffer Overflow</td>
<td>APP3590</td>
</tr>
<tr>
<td>A6 2004 = A2 2007</td>
<td></td>
</tr>
<tr>
<td>A7 2004 = A6 2007</td>
<td></td>
</tr>
<tr>
<td>A8 2004 = A8 2007</td>
<td></td>
</tr>
<tr>
<td>A9 2004 – Application Denial of Service</td>
<td>APP6080</td>
</tr>
<tr>
<td>A10 2004 – Insecure Configuration Management</td>
<td>APP3110, APP3290, APP3450, APP3470, APP3480, AP3500, APP6030,</td>
</tr>
<tr>
<td></td>
<td>APP6040, APP6050, APP6210, APP6240, APP6250, APP6260, APP6260</td>
</tr>
</tbody>
</table>
Improving Developer Awareness

- Use the OWASP Development Guide
- Provides background about key appsec areas

OWASP ESAPI Project

- Use standardized security controls
- Standardized library means faster development!

Custom Enterprise Web Application

Enterprise Security API

- Access Controller
- Reference Map
- Authenticator
- Encoder
- Encrypted Properties
- Encryptor
- Executor
- HTTP Utilities
- Intrusion Detector
- Log Factory
- Logger
- Randomizer
- Security configuration
- User
- Validator

http://www.owasp.org/index.php/ESAPI
ASD Gotchas

- APP3010: Label all external links
- APP3270: Identify classification of pages
- APP3440: Include the DoD Logon banner
- APP3530: Set charset in the Content-Header
- APP3320: Enforce DoD password policy
ASD Gotchas (cont.)

- APP3390: Lock users after 3 attempts w/in 1 hr
- APP3400: Do not allow automatic timed unlock
- APP3660: Show last and failed login details, including date, time and IP address
- APP3415: Enforce session idle timeout
- APP3420: Include a logout link
Do Self Validation

- ASD Checklist provides a starting point for tests

- Testers are often left unable to thoroughly test

### Boldy Go...

<table>
<thead>
<tr>
<th>Level</th>
<th>Program Management</th>
<th>Design &amp; Development</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>★ Allocate Time in Program Schedule ★ Distribute Secure Coding Guidelines</td>
<td>★ Use SSL with DoD Issued PKI Certificates ★ Fix Easy ASD Gotchas</td>
<td>★ Track Security Flaws ★ Create and Perform Security Tests</td>
</tr>
</tbody>
</table>
Summary

- Know the variety of ASD STIG requirements
- Leverage OWASP Projects:
  - Secure Software Development Contract Annex
  - Application Security Verification Standards
  - Top Ten
  - Development Guide
  - ESAPI
  - Testing Guide
Questions?

Contact: 
Jason Li
jason.li@aspectsecurity.com