Building a Corporate Application Security Assessment Program

Rob Jerdonek and Topher Chung
Corporate Information Security
Intuit Inc.

OWASP
July 23, 2009

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

The OWASP Foundation
http://www.owasp.org
Steps to Building a Corporate Application Security Assessment Program

- Identify goals and objectives of the program
- Define process and methodology
- Record and track quantitative results.
- Use results to drive process and technology improvements.
Comparing Risk Across Applications

- **SafeGuard Index**
- **Risk Score**
Identify Goals of Assessment Program

- **Scale**: Provide high value assessment services across the entire company in a timely manner.

- **Consistency**: Unified approach to remove variability among different apps and business units.

- **Results**: Record and track quantitative results. Monitor trends over time.

- **Improvements**: Use results to drive technology and process improvements.

Note: Maps to Six Sigma methods (DMAIC and DMADV)
Examples of other goals and objectives

- Continuously improve the security posture of applications.
- Provide qualitative and quantitative risk analysis for applications.
- Help justify strategic investments to improve security.
- Keep applications in line with evolving industry best practices and regulatory landscape.
- Embed security into the SDLC.
Define Process and Methodology

Assessment Process requirements:

■ Consistent process among all applications.

■ Adaptable to uniqueness of each application (small, large, etc..)

■ Not dependent on any particular tool or technology.
Assessment Process - Two tracks

- Detailed Assessment
  - 3-4 weeks
  - White-box Testing
    - 80% manual
    - 20% automated

- Accelerated Assessment
  - 1 week
  - Black-box Testing
    - 80% automated
    - 20% manual

Determine Assessment Track for Application
Assessment Process - Results

Risk Metrics
How much risk is carried by the application? What is the business impact?
Benchmarking relative to other corporate apps

Vulnerability List
Vulnerabilities found and/or exploited during penetration testing

Threat List
Threat control deficiencies found from Architecture Interviews and Threat Analysis.

Recommendations
Actionable recommendations for any all threats & vulnerabilities
## Risk Metrics - Categories

### 9 Risk Categories

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Denial of Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Deployment</td>
</tr>
<tr>
<td>Database Security</td>
<td>Audit &amp; Logging</td>
</tr>
<tr>
<td>Data Validation</td>
<td>Cryptography</td>
</tr>
<tr>
<td>Communication</td>
<td></td>
</tr>
</tbody>
</table>

- All threats & vulnerabilities are put into the above categories.
- Risk scores are distributed among these categories
Allocation of Risk

![Bar chart showing percentage allocation of risk across various categories such as Authentication, Access Control, Database Security, Data Validation, Communication, Denial of Service, Deployment, Audit & logging, and Cryptography. The highest risk category is represented by purple and accounts for 37% of the total risk. Other categories include:
- Authentication: 5%
- Access Control: 9%
- Database Security: 8%
- Data Validation: 3%
- Communication: 6%
- Denial of Service: 16%
- Deployment: 12%
- Audit & logging: 2%
- Cryptography: 12%]
Application Assessment “Heat Map”

Total Risk vs Safe Guard Index

<table>
<thead>
<tr>
<th>Risk</th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Desired Quadrant

- Application #1
- Application #2

OWASP
Risk Metrics - Calculations

Total Risk Score = \( \text{Risk (Threats)}^+ \times \text{Risk (Vulnerabilities)} \)

Threat Risk is architectural risk.

Vulnerability Risk comes from vulnerabilities found during penetration testing.

Lower is better.

Safe Guard Index =

\( \frac{\text{Actual Control Rating}}{\text{Perfect Control Rating}} \times 100\% \)

Higher is better.
Threat analysis

Application looks like a soccer ball.

- Each patch on the ball is a threat surface.
- Each patch is examined for threat potential.
- How well does an application control the threat?
- Each patch is tested for security weaknesses.
- Currently 28 threat categories are examined.
Threat Analysis - DREAD

**Damage potential**: How great is the damage if the vulnerability is exploited?

**Reproducibility**: How easy is it to reproduce the attack?

**Exploitability**: How easy is it to successfully exploit this condition?

**Affected users**: As a rough percentage, how many users are affected?

**Discoverability**: How easy is it to find the vulnerability?
## DREAD Rating Criteria - Examples

<table>
<thead>
<tr>
<th>Rating Scale</th>
<th>8-10 (High)</th>
<th>4-7 (Medium)</th>
<th>1-3 (Low)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage Potential</td>
<td>Subvert security system, run as Admin, upload content</td>
<td>Leakage of sensitive information.</td>
<td>Leaking trivial information</td>
</tr>
<tr>
<td>Reproducibility</td>
<td>No timing window required.</td>
<td>Only within timing window.</td>
<td>Difficult to reproduce.</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Easily exploitable by novice.</td>
<td>Takes repeated steps by skilled attacker.</td>
<td>Requires extremely skilled attacker w/ indepth knowledge.</td>
</tr>
<tr>
<td>Affected Users</td>
<td>Impacts large user base.</td>
<td>Impacts only a small group of users.</td>
<td>Impacts very small group of users.</td>
</tr>
<tr>
<td>Discoverability</td>
<td>Found in most common features and very noticeable</td>
<td>Likely noticed by only a few users.</td>
<td>Obscure bug. Very unlikely to be discovered.</td>
</tr>
</tbody>
</table>
## Threat Analysis - Control Rating

<table>
<thead>
<tr>
<th>Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No security control implementation in place to mitigate the threat.</td>
</tr>
<tr>
<td>1-2</td>
<td>No security control implementation in place to mitigate the threat.</td>
</tr>
<tr>
<td>3-4</td>
<td>Security control implementation in place is in compliance with the information security policies. Scoring of 3 and 4 provides the degree to which it is policy compliant.</td>
</tr>
<tr>
<td>5</td>
<td>High degree of security control implementation in place to mitigate the threat. Complies with the industry standard best practices.</td>
</tr>
</tbody>
</table>
## Threat Analysis - Residual Risk

DREAD score if no control implemented

<table>
<thead>
<tr>
<th>Control Rating:</th>
<th>1-2</th>
<th>3-4</th>
<th>5-6</th>
<th>7-8</th>
<th>9-10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree to which security control is implemented</td>
<td>0</td>
<td>5</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Residual Risk = Remaining risk after accounting for control rating
Using Results to Drive Improvements

- Compare overall risk between BU’s.
- Compare risk among Applications in a single BU.
- Identify areas for application security improvements.
- Monitor performance over time.
Using Results to Drive Improvements (cont.)

- Use assessment results to target strategic investments in security:
  - Shared Security Components
  - Security Testing tools
  - Identity Management Infrastructure, etc…