Threat Modeling and Risk Analysis for Developers and Testers

Matt Trevors

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Agenda

• Who am I
• Why
• Terms
• OWASP Top 10
• STRIDE Threat Modeling
• OCTAVE Allegro Risk Analysis
• Mitigation Strategies
• Summary
When, What, and Why?

• Sooner rather than later
• Functional vs. Security Testing
Terms

• Threat
• Vulnerability
• Asset
• Risk
• Quantitative
• Qualitative
• STRIDE
• OCTAVE
The Open Web Application Security Project

- International Community
- Top 10 Lists (Web, Mobile, Proactive Controls, etc.)
- Tools (Zed Attack Proxy)
- Software Assurance Maturity Model (SAMM)

**OWASP Top 10 Web (2013)**

A1 - Injection
A2 - Broken Authentication and Session Management
A3 - Cross-Site Scripting (XSS)
A4 - Insecure Direct Object Reference
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross-Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards
## Threat Modeling with STRIDE

<table>
<thead>
<tr>
<th></th>
<th>S</th>
<th>T</th>
<th>R</th>
<th>I</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Entity</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data Flow</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Store</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

- Spoofing (Authentication)
- Tampering (Integrity)
- Repudiation (Non-repudiation)
- Information Disclosure (Confidentiality)
- Denial of Service (Availability)
- Elevation of Privilege (Authorization)
Threat Modeling with STRIDE

Is there a threat of a threat actor {S|T|R|I|D|E} a(n) {EE|Proc|DF|DS} by exploiting a(n) {A[1-10]} vulnerability?
OCTAVE Allegro

- Qualitative Risk Analysis (pinch of quantitative)
- Helps prioritize work
- 8 Steps
## OCTAVE Allegro - Risk Measurement Criteria

<table>
<thead>
<tr>
<th>Impact Area</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Safety</td>
<td>No, or negligible impact on patient treatment. Delay is less than ___ hours</td>
<td>Treatment of the patient aided by system components has been delayed more than ___ hours</td>
<td>Treatment of the patient aided by system components has been delayed more than ___ hours or delayed indefinitely</td>
</tr>
<tr>
<td>Regulatory/Legal Issue</td>
<td>No, or negligible impact on regulatory or legal standing</td>
<td>Issue requires legal and/or regulatory review requiring agencies and/or customers and/or the public to be notified</td>
<td>The issue requires legal and/or regulatory review requiring agencies and/or the public to be notified. The issue also requires corrective and preventative action that affects more than ____% of existing customers.</td>
</tr>
<tr>
<td>Brand Damage</td>
<td>Reputation is minimally affected; little or no effort or expense is required to recover.</td>
<td>Reputation is damaged, and some effort and expense are required to recover.</td>
<td>Reputation is irrevocably destroyed or damaged.</td>
</tr>
<tr>
<td>Loss of Productivity</td>
<td>Loss of less than ____% of development time to address issue over a period of ____ days</td>
<td>Loss of between ____% and ____% development time to address issue over a period of ____ days</td>
<td>Loss of greater than ____% development time to address issue over a period of ____ days</td>
</tr>
<tr>
<td>Customer Confidence</td>
<td>Less than ____% reduction in customers due to loss of confidence</td>
<td>____ to ____% reduction in customers due to loss of confidence</td>
<td>More than ____% reduction in customers due to loss of confidence</td>
</tr>
</tbody>
</table>
OCTAVE Allegro
OCTAVE Allegro

• Example
  – Spoofing -> External Entity
  – Multiply L/M/H damage for each Risk Measurement Criteria
    \((L = 1, M = 2, H = 3)\)
    - Patient Safety \((5) \times L = 5\)
    - Regulatory/Legal \((4) \times H = 12\)
    - Brand Damage \((3) \times M = 6\)
    - Productivity \((2) \times L = 2\)
    - Confidence \((1) \times H = 5\)
  – Total Risk Score = 30
  – Complete for each applicable STRIDE category/STRIDE entity
  – Order from highest to lowest Risk Score
Mitigation

- NIST SP 800-53 Controls Catalog
- ISO 27000 series (27002, 27034, etc.)
- FIPS 140-2
- IETF standards (OAuth 2.0, TLS, PBKDF2)

**DO NOT ROLL YOUR OWN！！！！！！**
Summary

• Familiarize with OWASP
• Create STRIDE DFD
• Define OCTAVE Allegro Risk Measurement Criteria
• Complete OCTAVE Allegro spreadsheets (STRIDE/OWASP)
• Calculate Risk Scores
• Sort/Rank based on Risk Scores (highest to lowest)
• Identify industry standard mitigations
• **Calculate effort (for planning purposes)**
• Practice, Practice, Practice… Training, Training, Training
The End

Thank You!