Manage Your Risk With ThreatModeler

MyAppSecurity
50 Harrison Street, Suite 211D
Hoboken, NJ 07030
Phone: 201-632-3634
Sales: sales@myappsecurity.com
Introduction

Anurag “Archie” Agarwal, CISSP

– Founder MyAppSecurity
– Ex-Director - Education Services, WhiteHat Security
– 17 years of experience (Cisco, Citigroup, HSBC Bank, etc)
– Active in WASC and OWASP
– Published several articles on Secure Coding and SDL
– Project Leader – OWASP Threat Modeling Methodology
MyAppSecurity
Secure Your Applications

• End to End Software Security Risk Management Solution
• Key Services
  – Threat Modeling
  – Secure Architecture Review
  – Vulnerability Management
  – Training
hacked
“You cannot build secure systems until you understand your threats”
“Applications are built from individual features and each feature can be attacked. It is therefore important that you understand the components of the application”

- Cross-site scripting
- Session Hijacking
- Parameter Manipulation
- Buffer Overflow
- Password Guessing
- Account Enumeration
- SQL Injection
- Denial of Service
Threat Modeling pays for itself

• Number of Vulnerabilities = Negligible
• Competitive Advantage
• ROI Benefits

“Code fixes performed after release can result in 30 times the cost of fixes performed during the design phase.” (NIST)
BUILD YOUR OWN THREAT MODELING PRACTICE IN 7 EASY STEPS
Step 1 - Threat Library

• Build your own threat library
  – Existing threat libraries – CAPEC, WASC and OWASP
  – Custom threats

• Associate risk with threats to prioritize mitigation efforts
Step 2 - Secure Coding Standards

- Identify mitigation steps
  - Secure Coding Standards
    - OWASP Secure Coding Quick Reference Guide
    - OWASP Developers Guide
  - Security frameworks
    - OWASP ESAPI
    - Microsoft Enterprise Library
    - Microsoft AntiXSS Library
    - Custom/Home grown
- Associate mitigation steps with threats
Step 3 - Intelligence

- Build a library of reusable Threat Patterns / Attack Trees
- Build a pre-defined reusable component library
Step 4 - Actionable Output

• Builds a comprehensive threat profile (ThreatMap) of the system which can be either used to understand the system or generate actionable output
  – High Value Targets
  – Data Flow
  – Threats to individual Components
  – Risk
  – Attack Trees
  – List of Mitigation Steps (Abuse Cases)
  – Security Assessment Checklist
  – List of Total vs. Open Vulnerabilities
Step 5 – Dashboard and Reporting

- Threat Management Console
  - Threat Portfolio
  - Threat Management / Vulnerability Management
  - Prioritize Mitigation

- Risk Dashboard
  - Top Ten Threats
  - Risk Profiling
  - Compliance Reporting
### Step 6 - Collaboration

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architects</td>
<td>• Provide functional information about their application.</td>
</tr>
</tbody>
</table>
| Security Professionals | • Vulnerability Management / Risk Management.  
                       | • Promote Security Standards throughout the organization.                     |
| Developers          | • Implement correct mitigation steps and security standards using Abuse Cases.  |
Step 7 - Scaling and Operationalizing

• Build a Threat Model in hours/days depending on the size of the application
• Updating a threat model is a matter of minutes.
• Effective Risk Management.
• Build reusable templates
• Scalable across thousands of applications.
Time for a Demo

Anurag Agarwal
MyAppSecurity
http://www.myappsecurity.com
anurag@myappsecurity.com
Phone - 201-632-3634