Using and Customizing Microsoft Threat Modeling Tool 2016

Boston Code Camp 27
March 25, 2017
Robert Hurlbut

RobertHurlbut.com • @RobertHurlbut
Boston Code Camp 27 - Thanks to our Sponsors!

- Platinum 🔄 Microsoft

- Gold 🔄 HealthcareSource™ | NCache | NosDB

- Silver 🔄 BLUEMETAL | Robert Half Technology

- Bronze 🔄 RGood SOFTWARE | ROBERT HURLBUT Consulting Services | INFRAGISTICS

- In-Kind Donations 🔄 GrapeCity | steema software | VRKIX | WILEY
Robert Hurlbut

Software Security Consultant, Architect, and Trainer

Owner / President of Robert Hurlbut Consulting Services
(ISC)2 CSSLP 2014-2017
Co-host with Chris Romeo – Application Security Podcast

Contacts

Web Site: https://roberthurlbut.com
Twitter: @RobertHurlbut, @AppSecPodcast

© 2017 Robert Hurlbut Consulting Services
What is threat modeling?

Threat modeling helps you think strategically about your software design, in particular your secure software design.

A “way of thinking” tool – not automated security tool
What is threat modeling?

Threat modeling is:
Process of understanding your system and potential threats against your system

i.e. Critical Thinking about Security
What is threat modeling?

**Threat model includes:**
- understanding of system,
- identified threat(s),
- proposed mitigation(s),
- priorities by risk
Threat Modeling Vocabulary

* https://www.cigital.com/blog/threat-modeling-vocabulary/ (John Steven, Cigital)

© 2017 Robert Hurlbut Consulting Services
When? Make threat modeling first priority

In SDLC – Requirements and Design phase

Threat modeling uncovers new requirements
When? Make threat modeling first priority

Agile Sprint Planning - User Stories, Attacker Stories
Simple Tools

Whiteboard

Visio (or equivalent) for diagraming

Word (or equivalent) or Excel (or equivalent) for documenting
Threat Model Sample Worksheet

<table>
<thead>
<tr>
<th>ID</th>
<th>Risk Level (H, M, L)</th>
<th>Threat</th>
<th>Description / Impact</th>
<th>Countermeasures</th>
<th>Components Affected</th>
<th>Follow Up Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Other Tools

Microsoft Threat Modeling Tool 2016
ThreatModeler – Web Based (in-house) Tool
ThreadFix
IriusRisk Software Risk Manager
Threat Modeling Process

1. Draw your picture – understand the system and the data flows
2. Identify threats through answers to questions
3. Determine mitigations and risks
4. Follow through
Understand the system

DFD – Data Flow Diagrams (MS SDL)

- External Entity
- Process
- Multi-Process

- Data Store
- Dataflow

Trust Boundary / Attack Surface

© 2017 Robert Hurlbut Consulting Services
Identify threats

Most important part of threat modeling (and most difficult)
Many ways – determine what works best for your team
### STRIDE Framework – Data Flow

<table>
<thead>
<tr>
<th>Threat</th>
<th>Property we want</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>Authentication</td>
</tr>
<tr>
<td>Tampering</td>
<td>Integrity</td>
</tr>
<tr>
<td>Repudiation</td>
<td>Non-repudiation</td>
</tr>
<tr>
<td>Information Disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Availability</td>
</tr>
<tr>
<td>Elevation of Privilege</td>
<td>Authorization</td>
</tr>
</tbody>
</table>
Mapping STRIDE to OWASPTOP 10

<table>
<thead>
<tr>
<th>OWASPTopTen2013</th>
<th>STRIDE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 - Injection</td>
<td>Tampering, Spoofing</td>
</tr>
<tr>
<td>A2 – Broken Auth. &amp; Session Management</td>
<td>Elevation of Privileges, Spoofing, Information Disclosure</td>
</tr>
<tr>
<td>A3 – Cross-Site Scripting (XSS)</td>
<td>Tampering, Spoofing</td>
</tr>
<tr>
<td>A4 – Insecure Object References</td>
<td>Privilege Escalation, Information Disclosure</td>
</tr>
<tr>
<td>A5 - Security Misconfiguration</td>
<td>Information Disclosure (and others)</td>
</tr>
<tr>
<td>A6 – Sensitive Data Exposure</td>
<td>Information Disclosure</td>
</tr>
<tr>
<td>A7 – Missing Function Level Access Control</td>
<td>Privilege Escalation, Information Disclosure</td>
</tr>
<tr>
<td>A8 - Cross Site Request Forgery (CSRF)</td>
<td>Tampering, Spoofing, Elevation of Privileges</td>
</tr>
<tr>
<td>A9 - Using Components with Known Vuln.</td>
<td>All</td>
</tr>
<tr>
<td>A10 – Unvalidated Redirects and Forwards</td>
<td>Spoofing, Tampering</td>
</tr>
</tbody>
</table>
Microsoft Threat Modeling Tool 2016

Free 😊
Windows only 😞

Version History

2004, 2005: Threat Analysis & Modeling Tool (TAM) v1,v2:
Windows GUI
2011: SDL Threat Modeling Tool 3: Visio Plugin
...
2014: Microsoft Threat Modeling Tool 2014: Windows GUI
2015: Microsoft Threat Modeling Tool 2016: Windows GUI

Download: http://aka.ms/tmt2016
DFD Threat Modeling Logic

1. A SOURCE
   has a type ("Browser") and attributes
   has a parent ("Generic External Interactor") with attributes

2. Sends data via a DATA FLOW
   with a type ("HTTP") and attributes

3. That may crosses a TRUST BOUNDARY
   with a type ("Internet Boundary") and attributes

4. To a TARGET
   has a type ("WebApp") and attributes
   has a parent ("Generic Process") with attributes
DEMO

Microsoft Threat Modeling Tool 2016
Resources - Books

Threat Modeling: Designing for Security
Adam Shostack

Brook S.E. Schoenfield

Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis
Marco Morana and Tony UcedaVelez

Measuring and Managing Information Risk: A FAIR Approach
Jack Jones and Jack Freund

© 2017 Robert Hurlbut Consulting Services
Resources - Tools

Microsoft Threat Modeling Tool 2016

Open Threat Modeling Template
https://github.com/matthiasrohr/OTMT

Threat Model SDK (Java library)
https://github.com/stevespringgett/threatmodel-sdk

© 2017 Robert Hurlbut Consulting Services
Questions?

Contacts
Web Site: https://roberthurlbut.com
Twitter: @RobertHurlbut, @AppSecPodcast
Email: robert at roberthurlbut.com

© 2017 Robert Hurlbut Consulting Services