Is Threat Modeling For Me?

Security BSides Boston • May 9, 2015
Robert Hurlbut

RobertHurlbut.com • @RobertHurlbut
Robert Hurlbut

• **Independent Software Security Consultant and Trainer**
  • Owner / President of Robert Hurlbut Consulting Services
  • Speaker at user groups and conferences

• **Contacts**
  • Web Site: [http://roberthurlbut.com/](http://roberthurlbut.com/)
  • LinkedIn: [http://www.linkedin.com/in/roberthurlbut/](http://www.linkedin.com/in/roberthurlbut/)
  • Twitter: [@RobertHurlbut](http://twitter.com/@RobertHurlbut)
  • Email: robert at roberthurlbut.com
  • Slides Location: [http://roberthurlbut.com/training/presentations](http://roberthurlbut.com/training/presentations)
Threat modeling helps you …

Identify threats your system faces

Challenge assumptions

Prioritize other security efforts (pen test, review, fuzzing)

Document what you have learned
Definitions

• Threat Agent
  • Someone (or a process) who could do harm to a system (also adversary or attacker)
• Threat
  • An adversary’s goal
• Vulnerability
  • A flaw in the system that could help a threat agent realize a threat
• Asset
  • Something of value to valid users and adversaries alike
• Attack
  • When a motivated and sufficiently skilled threat agent takes advantage of a vulnerability
Getting started

• Gather documentation (requirements, high-level design, detailed design, etc.)

• Gather your team (don’t make this one person’s job only!)
  • Developers, QA, Architects, Project Managers, Business Stakeholders

• Understand business goals

• Understand technical goals

• Agree on meeting date(s) and time(s)

• Plan on 1-2 hours at a time spread over a week or weeks – keep sessions focused
What are you building?

What can go wrong?

What are you going to do about it?

Did you do a decent job of analysis?

* From Threat Modeling: Designing for Security by Adam Shostack
Threat Modeling Framework – Steps*

1. Model the system
2. Identify the threats
3. Address the threats
4. Validate your work

* From Threat Modeling: Designing for Security by Adam Shostack
Model the system

- DFD – Data Flow Diagrams (from Microsoft SDL)
Create the DFD

Users

Server

Admin

Request

Response

Admin Settings

Logging Data

© Robert Hurlbut Consulting Services 2015
Create the DFDs
Identify threats

- Attack Trees
- Threat Libraries (CAPEC, OWASP Top 10)
- Checklists
- Use Cases
- STRIDE
- P.A.S.T.A. – Process for Attack Simulation and Threat Analysis

© Robert Hurlbut Consulting Services 2015
STRIDE Framework* for finding threats

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

* Framework, not classification scheme. STRIDE is a good framework, bad taxonomy

© Robert Hurlbut Consulting Services 2015
Threat Trees

• A graphical representation of security-relevant pre-conditions in a system
• First outlined in Edward Amoroso’s “Fundamentals of Computer Security Technology”
• Based on hardware fault trees
• There are many “threat tree patterns”
Threat Tree Example

Threat #1
Obtaining authentication credentials over the network

and

1.1
Clear text credentials sent over the network

1.2
Attacker uses network monitoring tools

1.2.1
Attacker recognizes credential data
Threat Tree for Web Access Attack

Goal: Gain privileged access to Widget Web server

**AND** 1. Identify Widget domain name
2. Identify Widget firewall IP address
   - **OR** 1. Interrogate domain name server
   - 2. Scan for firewall identification
   - 3. Trace route through firewall to Web server
3. Determine Widget firewall access control
   - **OR** 1. Search for specific default listening ports
   - 2. Scan ports broadly for any listening port
4. Identify Widget Web server operating system and type
   - **OR** 1. Scan OS services' banners for OS identification
   - 2. Probe TCP/IP stack for OS characteristic information
5. Exploit Widget Web server vulnerabilities
   - **OR** 1. Access sensitive shared intranet resources directly
   - 2. Access sensitive data from privileged account on Web server
Threat Modeling Tools

• Whiteboard
• Visio (or equivalent)
• Word (or equivalent)
• Microsoft Threat Modeling Tool 2014
• Elevation of Privilege (EoP) Game
• TRIKE
• ThreatModeler (MyAppSecurity.com)
Consider Elevation of Privilege (EoP) game

- Great for teams new to threat modeling
- Everyone likes games

- Draw a diagram of your system
- Play / draw cards
- Apply what makes sense
Draw a diagram
EoP Game Example
Bob plays 10 of Tampering

An attacker can alter information in a data store because it has weak ACLs or includes a group which is equivalent to everyone ("all LiveID holders").

© Robert Hurlbut Consulting Services 2015
Charlie plays 5 of Tampering
Dan plays 8 of Tampering
Address the threats

• File bugs

• Mitigation Options:
  • Leave as-is
  • Remove from product
  • Remedy with technology countermeasure
  • Warn user

• What is the risk associated with the vulnerability?
Address the threats

• Risk Management
  • Bug Bar (Critical / Important / Moderate / Low)
  • FAIR (Factor Analysis of Information Risk) – Jack Jones
Validate your work

How well did you do?

When do you know you are done?

Filed bugs
Diagrammed the system(s)
Your challenge

Add threat modeling to your security toolkit

Consider threat modeling first (secure design, before new features, etc.)

Many ways … just do it!
Resources

• **Threat Modeling: Designing for Security** book by Adam Shostack

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

• **Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis** book by Marco Morana and Tony UcedaVelez (available June, 2015)
Resources - Tools

• Microsoft Threat Modeling Tool 2014
  

• Elevation of Privilege (EoP) Game
  

• Protection Poker paper by Laurie Williams, Michael Gegick, and Andrew Meneely
  
  http://collaboration.csc.ncsu.edu/laurie/Papers/essos09_submission_30.pdf
Questions?

• **Contacts**
  • Web Site: [http://roberthurlbut.com/](http://roberthurlbut.com/)
  • LinkedIn: [http://www.linkedin.com/in/roberthurlbut/](http://www.linkedin.com/in/roberthurlbut/)
  • Twitter: [@RobertHurlbut](http://twitter.com/RobertHurlbut)
  • Email: robert at roberthurlbut.com
  • Slides Location: [http://roberthurlbut.com/training/presentations](http://roberthurlbut.com/training/presentations)