How to Make Threat Modeling Work for You

Robert Hurlbut
RobertHurlbut.com • @RobertHurlbut
Robert Hurlbut

- **Independent Software Security Consultant and Trainer**
  - Owner / President of Robert Hurlbut Consulting Services
  - (ISC)2 CSSLP 2014-2017
  - Speaker at user groups and conferences

- **Contacts**
  - Web Site: [https://roberthurlbut.com/](https://roberthurlbut.com/)
  - LinkedIn: [https://www.linkedin.com/in/roberthurlbut/](https://www.linkedin.com/in/roberthurlbut/)
  - Twitter: [@RobertHurlbut](https://twitter.com/@RobertHurlbut)
  - Email: robert at roberthurlbut.com
  - Slides Location: [https://roberthurlbut.com/training/presentations](https://roberthurlbut.com/training/presentations)
What is threat modeling?

Threat modeling is the process of understanding your system and potential threats against your system.

A threat model allows you to assess the probability, potential harm, and priority of threats. Based on the model you can try to minimize or eradicate the threats.
Jonathan Marel @jonathanmarcil  June 26, 2014
Threat modeling is valuable, training is key, security
team must take the lead, partnership with devs =
shared vision, build it in

Brook Schoenfield @BrkSchoenfield  June 29, 2015
As I practice it, threat modeling cannot be the
province of a tech elite. It is best owned by all of a
development team.
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)
Definitions

Threat
An adversary’s goal
Definitions

Vulnerability

A flaw in the system that could help a threat agent realize a threat
Definitions

Attack

When a motivated and sufficiently skilled threat agent takes advantage of a vulnerability
Definitions

Asset
Something of value to valid users and adversaries alike
When?

Make threat modeling part of your secure software and architecture design

What if I didn’t? It’s not too late to start threat modeling, but it will be more difficult to change major design decisions
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
Threat Modeling Process – Making it work

1. Draw your picture - model the system
2. List the elements – entities, processes, data, data flows
3. Identity the threats - Ask questions
4. Determine mitigations and risks
5. Follow through
Draw your picture
Model the system

• DFD – Data Flow Diagrams (from Microsoft SDL)
Model the System
Model the system

1. User
2. Authn Engine
3. Get Creds
4. Service
5. Mnmgt Tool
6. Data Files
7. Audit Engine
8. Admin
9. Credentials

(requested file(s))

(trust boundary)
Your threat model now consists of …

1. Diagram / visual model of your system
Identity the elements

External Entities:
Users, Admin

Processes:
Service, Authn Engine, Audit Engine, Mnmgt Tool

Data Store(s):
Data Files, Credentials

Data Flows:
Users <-> Service
Admin <-> Audit Engine
Your threat model now consists of …

1. Diagram / visual model of your system
2. Elements of your system and the interactions
Identify threats

Attack Trees
Threat Libraries (CAPEC, OWASP Top 10)
Checklists (ex: OWASP Application Security Verification Standard (ASVS))
Use Cases / Misuse Cases
Games: Elevation of Privilege (EoP), OWASP Cornucopia
STRIDE
P.A.S.T.A. – Process for Attack Simulation and Threat Analysis (combining STRIDE + Attacks + Risk Analyses)
OWASP Cornucopia

Suits:
Data validation and encoding
Authentication
Session Management
Authorization
Cryptography
Cornucopia

13 cards per suit, 2 Jokers
Play a round, highest value wins
STRIDE Framework* for finding threats

<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>

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

© Robert Hurlbut Consulting Services 2015
Identify Threats

Input and data validation
Authentication
Authorization
Configuration management
Sensitive data
Session management
Cryptography
Parameter manipulation
Exception management
Auditing and logging
Ask questions

How is authentication handled?
What about authorization?
Are we sending data in the open?
Are we using cryptography properly?
Is there logging? What is stored?
Etc.
One of the best questions …

Is there anything that keeps you up at night worrying about this system?
Your threat model now consists of …

1. Diagram / visual model of your system
2. Elements of your system and the interactions
3. Threats identified through answers to questions
Determine mitigations and risks

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

- What is the risk associated with the vulnerability?
Determine mitigations and risks

Risk Management
- Bug Bar (Critical / Important / Moderate / Low)
- FAIR (Factor Analysis of Information Risk) – Jack Jones
- Risk Rating (High, Medium, Low)
Risk Rating

Overall risk of the threat expressed in High, Medium, or Low.

Risk is product of two factors:

- Ease of exploitation
- Business impact
# Risk Rating – Ease of Exploitation

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Description</th>
</tr>
</thead>
</table>
| **High**    | - Tools and exploits are readily available on the Internet or other locations  
              - Exploitation requires no specialized knowledge of the system and little or no programming skills  
              - Anonymous users can exploit the issue |
| **Medium**  | - Tools and exploits are available but need to be modified to work successfully  
              - Exploitation requires basic knowledge of the system and may require some programming skills  
              - User-level access may be a pre-condition |
| **Low**     | - Working tools or exploits are not readily available  
              - Exploitation requires in-depth knowledge of the system and/or may require strong programming skills  
              - User-level (or perhaps higher privilege) access may be one of a number of pre-conditions |
# Risk Rating – Business Impact

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Description</th>
</tr>
</thead>
</table>
| **High**    | • Administrator-level access (for arbitrary code execution through privilege escalation for instance) or disclosure of sensitive information  
• Depending on the criticality of the system, some denial-of-service issues are considered high impact  
• All or significant number of users affected  
• Impact to brand or reputation |
| **Medium**  | • User-level access with no disclosure of sensitive information  
• Depending on the criticality of the system, some denial-of-service issues are considered medium impact |
| **Low**     | • Disclosure of non-sensitive information, such as configuration details that may assist an attacker  
• Failure to adhere to recommended best practices (which does not result in an immediately visible exploit) also falls into this bracket  
• Low number of user affected |
# Example – Medium Risk Threat

<table>
<thead>
<tr>
<th>ID - Risk</th>
<th>RT-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Lack of CSRF protection allows attackers to submit commands on behalf of users</td>
</tr>
<tr>
<td>Description/Impact</td>
<td>Client applications could be subject to a CSRF attack where the attacker embeds commands in the client applications and uses it to submit commands to the server on behalf of the users</td>
</tr>
<tr>
<td>Countermeasures</td>
<td>Per transaction codes (nonce), thresholds, event visibility</td>
</tr>
<tr>
<td>Components Affected</td>
<td>CO-3</td>
</tr>
</tbody>
</table>
Your threat model now consists of …

1. Diagram / visual model of your system
2. Elements of your system and the interactions
3. Threats identified through answers to questions
4. Mitigations and risks identified to deal with the threats
Follow through

Document what you found and decisions you make
File bugs or new requirements
Verify bugs fixed and new requirements implemented
Did we miss anything? Review again
Anything new? Review again
Your threat model now consists of …

1. Diagram / visual model of your system
2. Elements of your system and the interactions
3. Threats identified through answers to questions
4. Mitigations and risks identified to deal with the threats
5. Follow through – a living threat model!
Your challenge

Add threat modeling to your toolkit

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

Many ways … just do it!
Resources - Books

 Threat Modeling: Designing for Security by Adam Shostack


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

 Measuring and Managing Information Risk: A FAIR Approach by Jack Jones and Jack Freund
Resources - Tools

Whiteboard
Visio (or equivalent)
Word (or equivalent)
Resources - Tools

Microsoft Threat Modeling Tool 2016 (New: 10/2/2015)

Threat Modeler Tool 3.0
http://myappsecurity.com

Elevation of Privilege (EoP) Game

OWASP Cornucopia
https://www.owasp.org/index.php/OWASP_Cornucopia

OWASP Application Security Verification Standard (ASVS)

OWASP Threat Modeling Cheat Sheet (work in progress)
https://www.owasp.org/index.php/Threat_Modeling_Cheat_Sheet

© Robert Hurlbut Consulting Services 2015
Questions?

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