How To Make Threat Modeling Work For You

Strategic Approaches to Real-World Architecture Challenges
O’Reilly Software Architecture Online Conference
March 1, 2016
Robert Hurlbut
Robert Hurlbut

• **Software Security Consultant, Architect, and Trainer**
  • Owner / President of Robert Hurlbut Consulting Services
  • (ISC)2 CSSLP 2014-2017
  • Speaker at user groups, conferences, and other training events

• **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
What is threat modeling?

Something we all do in our personal lives …

… when we lock our doors to our house

… when we lock the windows

… when we lock the doors to our car
What is threat modeling?

When we think ahead of what could go wrong, weigh the risks, and act accordingly, we are “threat modeling”
What is threat modeling?

Threat modeling is:

- Process of understanding your system and potential threats against your system.

Threat model includes probability of threat, potential harm or impact, and priority and plan for mitigating the threats.
Michael Howard*  @michael_howard
Jan 7, 2015

A dev team with an awesome, complete and accurate threat model gets my admiration and not much of my time because they don’t need it! 😊

(* Co-author of Writing Secure Code (2nd Ed) and other books)
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

In SDLC – Requirements and Design phase

Threat modeling can uncover new requirements

Agile Sprint Planning

© 2016 Robert Hurlbut Consulting Services
When?

What if we didn’t?

It’s not too late to start threat modeling (generally)
It will be more difficult to change major design decisions
Either way, get started!
Typical Threat Modeling Session

Gather documentation

Gather your team:
    Developers, QA, Architects, Project Managers, Business Stakeholders (not one person’s job!)

Understand business goals and technical goals

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

Plan on 1-2 hour focused sessions at a time

Important: Be honest, leave ego at the door, no blaming!
Threat Modeling Process – Making it work

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

DFD – Data Flow Diagrams (MS SDL)

- External Entity
- Process
- Multi-Process
- Data Store
- Dataflow
- Trust Boundary

© 2016 Robert Hurlbut Consulting Services
Understand the System

Understand logical and component architecture of system
Understand every communication flow and valuable data moved and stored
Understand the system
Understand the system

External Entities:
Users, Admin

Processes:
Web App, Authn Svc, Audit Svc, Mnmgt Tool

Data Store(s):
Data Files, Credentials

Data Flows:
Users <-> Web App
Credentials
Admin <-> Audit Svc

© 2016 Robert Hurlbut Consulting Services
Your threat model now consists of …

1. Diagram / understanding of your system and the data flows
Identify threats

Most important part of threat modeling (and most difficult)

Many methods for identifying threats: Attack Trees, Threat Libraries, Checklists, Use/Misuse Cases, Threat Modeling Card Games, STRIDE, PASTA, …
Identify Threats – Common Areas

Input and data validation
Authentication
Authorization
Configuration management
Sensitive data
Identify Threats – Common Areas

Session management
Cryptography
Parameter manipulation
Exception management
Auditing and logging
Identity Threats - Ask Questions

Who would be interested in the application and its data (threat agents)?
What are the goals (assets)?
What are attack methods for the system we are building?
Are there any attack surfaces exposed - data flows (input/output) we are missing?
Identity Threats – Ask Questions

How is authentication handled between callers and services?
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 / understanding of your system and the data flows
2. 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><strong>Threat</strong></td>
<td>Lack of CSRF protection allows attackers to submit commands on behalf of users</td>
</tr>
<tr>
<td><strong>Description/Impact</strong></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><strong>Countermeasures</strong></td>
<td>Per transaction codes (nonce), thresholds, event visibility</td>
</tr>
<tr>
<td><strong>Components Affected</strong></td>
<td>CO-3</td>
</tr>
</tbody>
</table>
Your threat model now consists of …

1. Diagram / understanding of your system and the data flows
2. Threats identified through answers to questions
3. 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 / understanding of your system and the data flows
2. Threats identified through answers to questions
3. Mitigations and risks identified to deal with the threats
4. Follow through

A living threat model!

© 2016 Robert Hurlbut Consulting Services
Your challenge

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

Many ways … just do it!
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*
Resources - Tools

Whiteboard
Visio (or equivalent) for diagraming
Word (or equivalent) or Excel (or equivalent) for documenting
Resources - Tools

Microsoft Threat Modeling Tool 2016

Threat Modeler Tool 3.0
http://myappsecurity.com
Questions?

Contacts

Web Site: https://roberthurlbut.com
LinkedIn: https://www.linkedin.com/in/roberthurlbut
Twitter: @RobertHurlbut
Email: robert at roberthurlbut.com