• **Independent Software Security Consultant and Trainer**
  – Owner / President of Robert Hurlbut Consulting Services
  – (ISC)2 CSSLP 2014-2017
  – Group Leader – Boston .NET Arch Group, Amherst Sec Grp
  – Speaker at user groups, conferences, and other 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
  – Email: robert at roberthurlbut.com
  – Slides Location: [https://roberthurlbut.com/training/presentations](https://roberthurlbut.com/training/presentations)
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

We threat model by thinking ahead of what could go wrong and acting accordingly
Threat modeling is the process of understanding your system and potential threats against your system. A threat model helps you assess the probability, potential harm, and priority of threats. Based on the model you can try to minimize or eradicate 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! 😊
As I practice it, threat modeling cannot be the province of a tech elite. It is best owned by all of a development team.
Identify threats your system faces

Challenge assumptions

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

Document what you have learned
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
Definitions

Attack

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

Something of value to valid users and adversaries alike
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
**Important:** Be honest, leave ego at the door, no blaming!
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)

- External Entity
- Process
- Multi-Process
- Data Store
- Dataflow
- Privilege Boundary
Model the system

[Diagram showing interactions between User, Service, Audit Engine, Admin, Authn Engine, Mnmgt Tool, and Data Files]

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

(Trust boundary)
1. Diagram / visual model of your system
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 (Bruce Schneier - Slidedeck)

Threat Libraries (CAPEC, OWASP Top 10, SANS Top 25)

Checklists (ex: OWASP Application Security Verification Standard (ASVS), OWASP Proactive Controls 2016)

Use Cases / Misuse Cases
Games:
Elevation of Privilege (EoP)
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

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

<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>
P.A.S.T.A. – Process for Attack Simulation and Threat Analysis

7 step process combining:

STRIDE + Attacks + Risk Analyses
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.
Is there anything that keeps you up at night worrying about this system?
1. Diagram / visual model of your system
2. Elements of your system and the interactions
3. Threats identified through answers to questions
• Mitigation Options:
  – Leave as-is
  – Remove from product
  – Remedy with technology countermeasure
  – Warn user

• What is the risk associated with the vulnerability?
Risk Management

Bug Bar (Critical / Important / Moderate / Low)

FAIR (Factor Analysis of Information Risk) – Jack Jones

Risk Rating (High, Medium, Low)
Overall risk of the threat expressed in High, Medium, or Low.

Risk is product of two factors:

- Ease of exploitation
- Business impact
<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 users affected |
<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
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
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!
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 diagramming
Word (or equivalent) or Excel (or equivalent) for documenting
Resources - Tools

Attack Trees – Bruce Schneier on Security


Microsoft Threat Modeling Tool 2016


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 Proactive Controls (especially current 2016 work)

https://www.owasp.org/index.php/OWASP_Proactive_Controls
• **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)