

# How To Make Threat Modeling Work For You

Tech Valley .NET User Group (TVUG)

Latham, NY • January 12, 2016

Robert Hurlbut

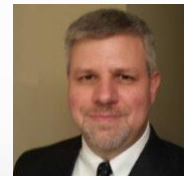
[RobertHurlbut.com](http://RobertHurlbut.com) • [@RobertHurlbut](https://twitter.com/RobertHurlbut)



## Robert Hurlbut

- **Independent Software Security Consultant and Trainer**

- Owner / President of Robert Hurlbut Consulting Services
- Microsoft MVP – Security Developer 2005-2009, 2015
- (ISC)2 CSSLP 2014-2017
- Group Leader – Boston .NET Arch Group, Amherst Sec Group
- Speaker at user groups, conferences, and other training events



- **Contacts**

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

## What is threat modeling?

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! 😊*

**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

**Important:** Be honest, leave ego at the door, no blaming!

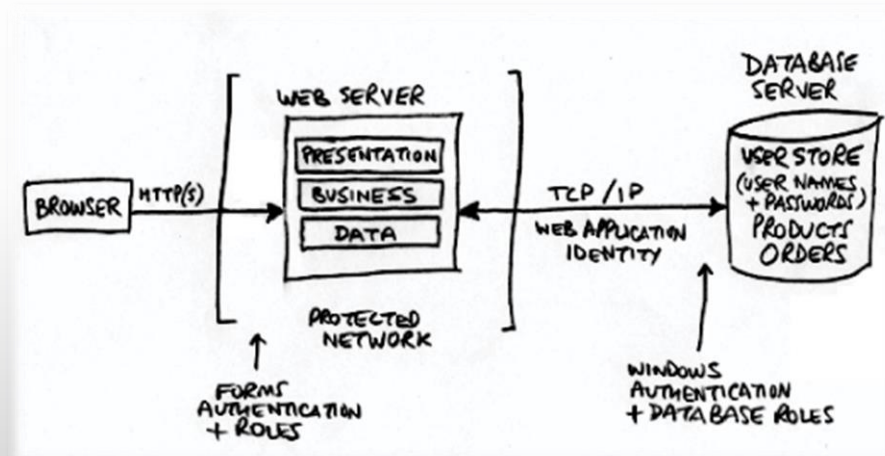
## Threat Modeling Process – Making it work

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

© 2016 Robert Hurlbut Consulting Services

15

## Draw your picture

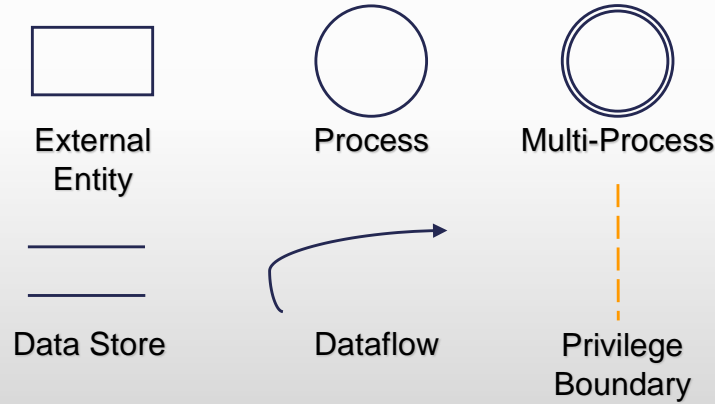


© 2016 Robert Hurlbut Consulting Services



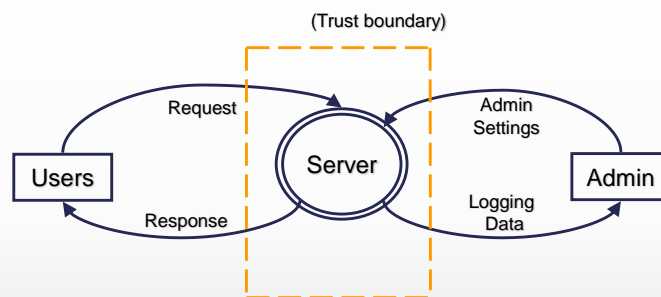
## Model the system

- DFD – Data Flow Diagrams (from Microsoft SDL)

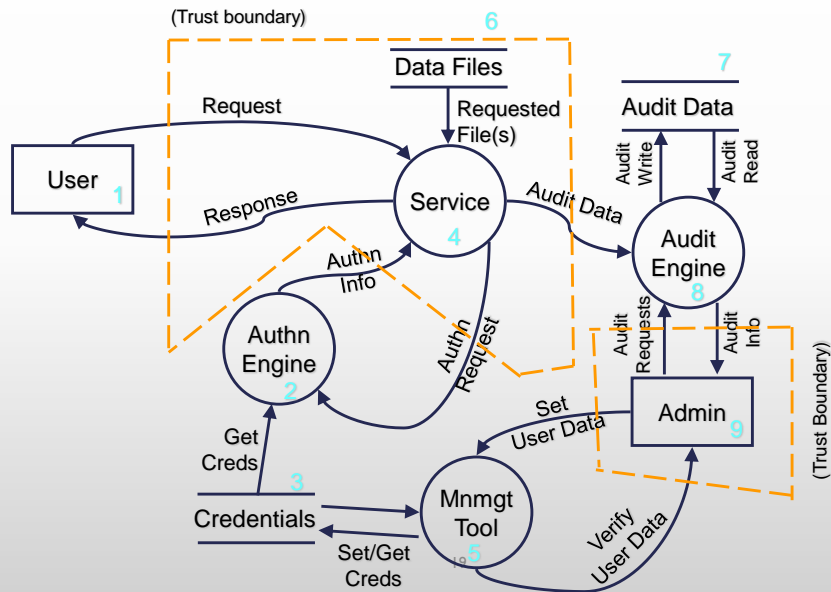


17

## Model the System



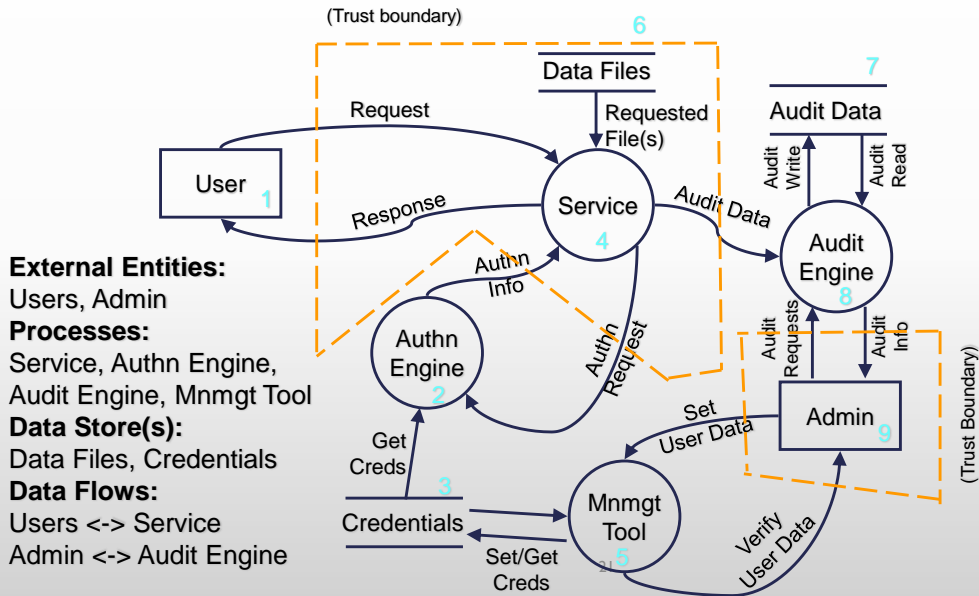
## Model the system



Your threat model now consists of ...

1. Diagram / visual model of your system

## Identity the elements



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 - Slide deck)

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  
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

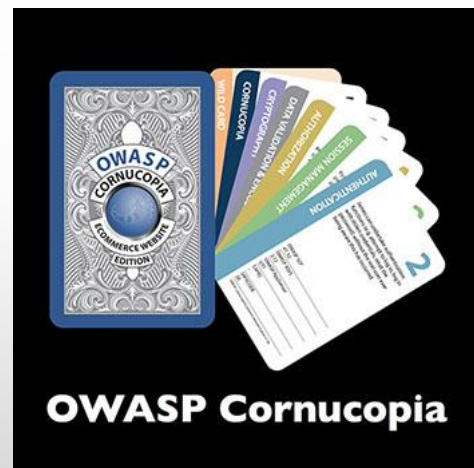
Authorization

Cryptography

Cornucopia

13 cards per suit, 2 Jokers

Play a round, highest value wins



## STRIDE Framework\* for finding threats

| Threat                 | Property we want |
|------------------------|------------------|
| Spoofing               | Authentication   |
| Tampering              | Integrity        |
| Repudiation            | Non-repudiation  |
| Information Disclosure | Confidentiality  |
| Denial of Service      | Availability     |
| Elevation of Privilege | Authorization    |

\* Framework, not classification scheme. STRIDE is a good framework, bad taxonomy  
 © 2016 Robert Hurlbut Consulting Services

## 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

| Risk Rating   | Description  |
|---------------|--|
| <b>High</b>   | <ul style="list-style-type: none"> <li>Tools and exploits are readily available on the Internet or other locations</li> <li>Exploitation requires no specialized knowledge of the system and little or no programming skills</li> <li>Anonymous users can exploit the issue</li> </ul>                               |
| <b>Medium</b> | <ul style="list-style-type: none"> <li>Tools and exploits are available but need to be modified to work successfully</li> <li>Exploitation requires basic knowledge of the system and may require some programming skills</li> <li>User-level access may be a pre-condition</li> </ul>                               |
| <b>Low</b>    | <ul style="list-style-type: none"> <li>Working tools or exploits are not readily available</li> <li>Exploitation requires in-depth knowledge of the system and/or may require strong programming skills</li> <li>User-level (or perhaps higher privilege) access may be one of a number of pre-conditions</li> </ul> |

## Risk Rating – Business Impact

| Risk Rating   | Description  |
|---------------|--|
| <b>High</b>   | <ul style="list-style-type: none"> <li>Administrator-level access (for arbitrary code execution through privilege escalation for instance) or disclosure of sensitive information</li> <li>Depending on the criticality of the system, some denial-of-service issues are considered high impact</li> <li>All or significant number of users affected</li> <li>Impact to brand or reputation</li> </ul> |
| <b>Medium</b> | <ul style="list-style-type: none"> <li>User-level access with no disclosure of sensitive information</li> <li>Depending on the criticality of the system, some denial-of-service issues are considered medium impact</li> </ul>  |
| <b>Low</b>    | <ul style="list-style-type: none"> <li>Disclosure of non-sensitive information, such as configuration details that may assist an attacker</li> <li>Failure to adhere to recommended best practices (which does not result in an immediately visible exploit) also falls into this bracket</li> <li>Low number of user affected</li> </ul>  |

## Example – Medium Risk Threat

|                            |   |
|----------------------------|---|
| <b>ID - Risk</b>           | <b>RT-3</b>   |
| <b>Threat</b>              | Lack of CSRF protection allows attackers to submit commands on behalf of users  |
| <b>Description/Impact</b>  | 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 |
| <b>Countermeasures</b>     | Per transaction codes (nonce), thresholds, event visibility   |
| <b>Components Affected</b> | CO-3  |

© 2016 Robert Hurlbut Consulting Services

35

## 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

© 2016 Robert Hurlbut Consulting Services

36

## 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

*Adam Shostack*

Securing Systems: Applied Architecture and Threat Models

*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

© 2016 Robert Hurlbut Consulting Services

## Resources - Tools

Attack Trees – Bruce Schneier on Security

<https://www.schneier.com/attacktrees.pdf>

Microsoft Threat Modeling Tool 2016

<http://www.microsoft.com/en-us/download/details.aspx?id=49168>

Threat Modeler Tool 3.0

<http://myappsecurity.com>

© 2016 Robert Hurlbut Consulting Services

42

## Resources - Tools

### Elevation of Privilege (EoP) Game

<http://www.microsoft.com/en-us/download/details.aspx?id=20303>

### OWASP Cornucopia

[https://www.owasp.org/index.php/OWASP\\_Cornucopia](https://www.owasp.org/index.php/OWASP_Cornucopia)

### OWASP Application Security Verification Standard (ASVS)

[https://www.owasp.org/index.php/Category:OWASP\\_Application\\_Security\\_Verification\\_Standard\\_Project](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)

### OWASP Proactive Controls (especially current 2016 work)

[https://www.owasp.org/index.php/OWASP\\_Proactive\\_Controls](https://www.owasp.org/index.php/OWASP_Proactive_Controls)

## Questions?

- **Contacts**

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

