Developing a Threat Modeling Mindset

NAISG Boston Chapter Meeting
March 8, 2016
Robert Hurlbut
RobertHurlbut.com • @RobertHurlbut
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

© 2016 Robert Hurlbut Consulting Services
Security mindset

Bruce Schneier talked about what it is and teaching it in 2008 and 2012:

“Security requires a particular mindset. Security professionals — at least the good ones — see the world differently.”*

(* See: https://www.schneier.com/blog/archives/2008/03/the_security_mi_l.html and https://www.schneier.com/blog/archives/2012/06/teaching_the_se.html)
Security mindset

Network Security
Auditing / compliance / risk
Application Security

Builders – development
Breakers – testing
Defenders – detection/response
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?

Historically, threat modeling came from military usage:
  Who is the enemy?
  What are their motives?
  What are their methods?
  Let’s plan our strategy / defense
A threat modeling mindset?

“By understanding the historical usage of threat modeling, security professionals at large can evolve a mindset built around strategy rather than segregated and disorganized knee-jerk responses.”*

(* Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis by Tony UcedaValez and Marco M. Morana)
A threat modeling mindset?

“By understanding the historical usage of threat modeling, security professionals at large can evolve a mindset built around strategy rather than segregated and disorganized knee-jerk responses.”

(* Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis by Tony UcedaValez and Marco M. Morana)

© 2016 Robert Hurlbut Consulting Services
A threat modeling mindset is …

“Understanding where we are” vs “we hope so or think so” in regards to security in our business

Strategy vs Reacting
A threat modeling mindset is …

Bridging gaps between builders, breakers, and defenders:

- Helps builders focus on security features
- Helps breakers know most critical attack surfaces
- Helps defenders understand critical attack patterns

And can help network, audit, compliance, etc. understand system
Where does threat modeling fit?

One of the application security tools – but different

We know about penetration testing, fuzzing, analysis / code reviews, detection (lots of automated tools)

Threat modeling is a process (not automated)
What is threat modeling?

Threat modeling is:

Process of understanding your system and potential threats against your system.
What is threat modeling?

**Threat model** includes:
- understanding of your system,
- identified threat(s),
- probability of threat(s),
- potential harm or impact, and
- priority and plan for mitigating the threat(s) based on risk
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 first priority:
In SDLC – Requirements and Design phase
Threat modeling uncovers new requirements
Agile Sprint Planning
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

Do it anyway!
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 (threat modeling must support goals, not other way around)

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!
Simple Tools

Whiteboard
Visio (or equivalent) for diagraming
Word (or equivalent) or Excel (or equivalent) for documenting

Look at Dinis Cruz’ Simple Threat Model One Page Template

http://blog.diniscruz.com/2016/03/simple-threat-model-template-good-place.html
Simple Threat Model – One Page
# Threat Model Sample Worksheet

<table>
<thead>
<tr>
<th></th>
<th>ID</th>
<th>Risk Level (H, M, L)</th>
<th>Threat</th>
<th>Description / Impact</th>
<th>Countermeasures</th>
<th>Components Affected</th>
<th>Follow Up Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Threat Model Worksheet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2016 Robert Hurlbut Consulting Services
Review Security Principles*

1. Secure the weakest link
2. Defend in depth
3. Fail securely
4. Grant least privilege
5. Separate privileges
6. Economize mechanisms

Review Security Principles*

7. Do not share mechanisms
8. Be reluctant to trust
9. Assume your secrets are not safe
10. Mediate completely
11. Make security usable
12. Promote privacy
13. Use your resources

Threat Modeling Process

1. Draw your picture – understand the system and the data flows
2. Identify threats 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

User

Web App

Authn Service

Credentials

Mnmgt Tool

Admin

Get Creds

Authn Request

Auth Info

Set/Get Creds

Set User Data

Request

Response

Requested File(s)

Audit Data

Audit Request

Audit Info

Audit Data

Audit Read

Audit Write

Audit Requests

Data Files

© 2016 Robert Hurlbut Consulting Services
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)

- Attack Trees (Bruce Schneier - Slide deck)
- Threat Libraries (CAPEC, OWASP Top 10, SANS Top 25)
- Checklists (OWASP Application Security Verification Standard (ASVS), OWASP Proactive Controls 2016)
- Use Cases / Misuse Cases
- Games: Elevation of Privilege (EoP), OWASP Cornucopia
- STRIDE
## STRIDE Framework – Data Flow

<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>
Identify Threats – Functional

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

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?
Scenario – Configuration Management

Data Files such as configuration files
Scenario – Configuration Management

System: Web application uses configuration files

Security principles:
   Be reluctant to trust, Assume secrets not safe

Questions:
   How does the app use the configuration files?
   What validation is applied? Implied trust?

Possible controls/mitigation:
   Set permissions on configuration files.
   Validate all data input from files. Use fuzz testing to insure input validation.
Your threat model now consists of …

1. Diagram / understanding of your system and the data flows
2. Identify threats 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>
Scenario – Configuration Management

System: Web application uses configuration files

Security principles:
   Be reluctant to trust, Assume secrets not safe

Questions:
   How does the app use the configuration files?
   What validation is applied? Implied trust?

Possible controls/mitigation:
   Set permissions on configuration files.
   Validate all data input from files. Use fuzz testing to insure input validation.

Risk Rating:
   We own the box (Medium/Low), Hosted on cloud (High)
Your threat model now consists of …

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

A living threat model!
Your challenge

Pursue a threat modeling mindset – secure design before new features, let threat modeling drive your testing and other review activities understand bigger picture
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

© 2016 Robert Hurlbut Consulting Services
Resources - Tools

Microsoft Threat Modeling Tool 2016

Threat Modeler Tool 3.0
http://myappsecurity.com
Resources - Tools

Attack Trees – Bruce Schneier on Security


Elevation of Privilege (EoP) Game


OWASP Cornucopia

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

OWASP Application Security Verification Standard (ASVS)


OWASP Proactive Controls 2016

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
Email: robert at roberthurlbut.com