Threat Modeling:
Lessons from
Star Wars

Adam Shostack
@adamshostack
Agenda

• What is threat modeling?
• A simple approach to threat modeling
• Top 10 lessons
• Learning more
What is threat modeling?
A SIMPLE APPROACH TO THREAT MODELING
4 Questions

1. What are you building?
2. What can go wrong?
3. What are you going to do about it?
4. Did you do an acceptable job at 1-3?
What are you building?
Data Flow Diagrams are a great representation
What Can Go Wrong?
Remember STRIDE
Spoofing

Tampering

http://pinlac.com/LegoDSTractorBeam.htm
Repudiation

By Seb H http://www.flickr.com/photos/88048956@N04/8531040850/
Information Disclosure (and impact)
Elevation of Privilege

http://www.flickr.com/photos/prodiffusion/
4 Questions

1. What are you building?
2. What can go wrong?
3. What are you going to do about it?
4. Did you do an acceptable job at 1-3?
TOP TEN LESSONS
IT'S A TRAP!
Trap #1: “Think Like An Attacker”

- “Think like a professional chef”?
- Most people need structure
Trap #2: “You’re Never Done Threat Modeling”

Model → Identify Threats → Mitigate → Validate → Identify Threats → Mitigate → Validate → Identify Threats → Mitigate → Validate
 Trap #3: “The Way To Threat Model Is…”

• Too much focus on specifics of how
  – Use this framework (STRIDE)
  – With this diagram type
• Focus on what delivers value by helping people find good threats
• Focus on what delivers value by helping lots of people

Borrowing a line from the Perl folks...

*There’s more than one way to threat model*
Trap #3: Monolithic Processes

Model

Identify Threats

Mitigate

Validate

Privacy

Solove's Harms

Contextual Integrity

Attack Trees

CAPEC

STRIDE

DFD

Swim Lanes
Trap #3: “The Way To Threat Model Is...”

Security mavens

Experts in other areas
Trap #4: Threat Modeling as One Skill

• Technique: DFDs, STRIDE, Attack trees
• Repertoire:
  – SSLSpoof, Firesheep
  – Mitnick, Cuckoo's Egg
  – Conficker, Stuxnet and Crilock

• Frameworks and organization
  – Elicitation and memory for experts

There's Technique and Repertoire
Trap #5: Threat Modeling is Born, Not Taught

• Playing a violin...You need to develop and maintain muscles
• Beginners need easy and forgiving tunes
• Not everyone wants or needs to be a virtuoso

Threat Modeling Is Like Playing A Violin
We’ve got to give them more time!
Trap #6: The Wrong Focus

• Start from your assets
• Start by thinking about your attackers
• Thinking that threat modeling should focus on finding threats

• Remember trap #3: “The Way to threat model is”
• Starting from assets or attackers work for some people
Trap #7: Threat Modeling is for Specialists

• Version control:
  – Every developer, most sysadmins know some
  – Some orgs have full time people managing trees

• This is a stretch goal for threat modeling

Threat Modeling Is Like Version Control
Trap #8: Threat Modeling Without Context

• Some threats are “easy” for a developer to fix (for example, add logging)
• Some threats are “easy” for operations to fix (look at the logs)
• Good threat modeling can build connections
  – Security Operations Guide
  – Non-requirements
Trap #9: Laser-Like Focus on Threats

Interplay of attacks, mitigations and requirements
Trap #10: Threat Modeling at the Wrong Time

“Sir, we’ve analyzed their attack pattern, and there is a danger”
Summary

• Anyone can threat model, and everyone should
• The skills, techniques and repertoire can all be learned
• There are many traps

• Threat modeling is one of the most effective ways to drive security through your product, service or system
Call to Action

• Remember the 4 Questions
• Be proactive:
  – Find security bugs early
  – Fix them before they’re exploited
• Drive threat modeling through your organization
• Drive threat modeling throughout the profession
“All models are wrong, some models are useful”

— George Box
Questions?

• Please use the microphones
• Or tweet @adamshostack
• Or read the new book 😊
  – Threatmodelingbook.com
Resources: Additional Books

- *The Checklist Manifesto* by Atul Gawande
- *Thinking Fast & Slow* by Daniel Kahneman
- *The Cuckoo's Egg* by Cliff Stoll
- *Ghost in the Wires* by Kevin Mitnick
- *Understanding Privacy* by Dan Solove
- *Privacy in Context* by Helen Nissenbaum
Threat Modeling: Designing For Security

Part I: Getting Started
1. Dive in and threat model
2. Strategies for threat modeling

Part II: Finding Threats
3. STRIDE
4. Attack Trees
5. Attack Libraries
6. Privacy Tools

Part III: Managing and Addressing Threats
7. Processing and managing threats
8. Defensive Building Blocks
9. Tradeoffs when addressing threats
10. Validating threats are addressed
11. Threat modeling tools

Part IV: Threat modeling in technologies and tricky areas
12. Requirements cookbook
13. Web and cloud threats
14. Accounts and Identity
15. Human Factors and Usability
16. Threats to cryptosystems

Part IV: Taking it to the next level
17. Bringing threat modeling to your organization
18. experimental approaches
19 Architecting for success

Appendices
- Helpful tools, Threat trees, Attacker Lists, Elevation of Privilege (the cards), Case studies
Thank you!

Resources

• Star Wars: Episodes IV-VI
• Great Creative Commons Lego brick art:
  – http://pinlac.com/LegoDSTractorBeam.html
  – Seb H http://www.flickr.com/photos/88048956@N04/8531040850/
  – Kaitan Tylerguy http://www.flickr.com/photos/kaitan/3326772088/
  – http://www.flickr.com/photos/prodiffusion/
Different Threats Affect Each Element Type

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>S</th>
<th>T</th>
<th>R</th>
<th>I</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Entity</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Data Store</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Data Flow</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
This isn’t the reputation you’re looking for…