

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

New Foundations for Threat Modeling

SESSION ID:

ASEC-W02

Adam Shostack

@adamshostack
Microsoft



Agenda

- A simple approach to threat modeling
- Top 10 foundations
- Learning more

A SIMPLE APPROACH TO **THREAT MODELLING**

4 Questions

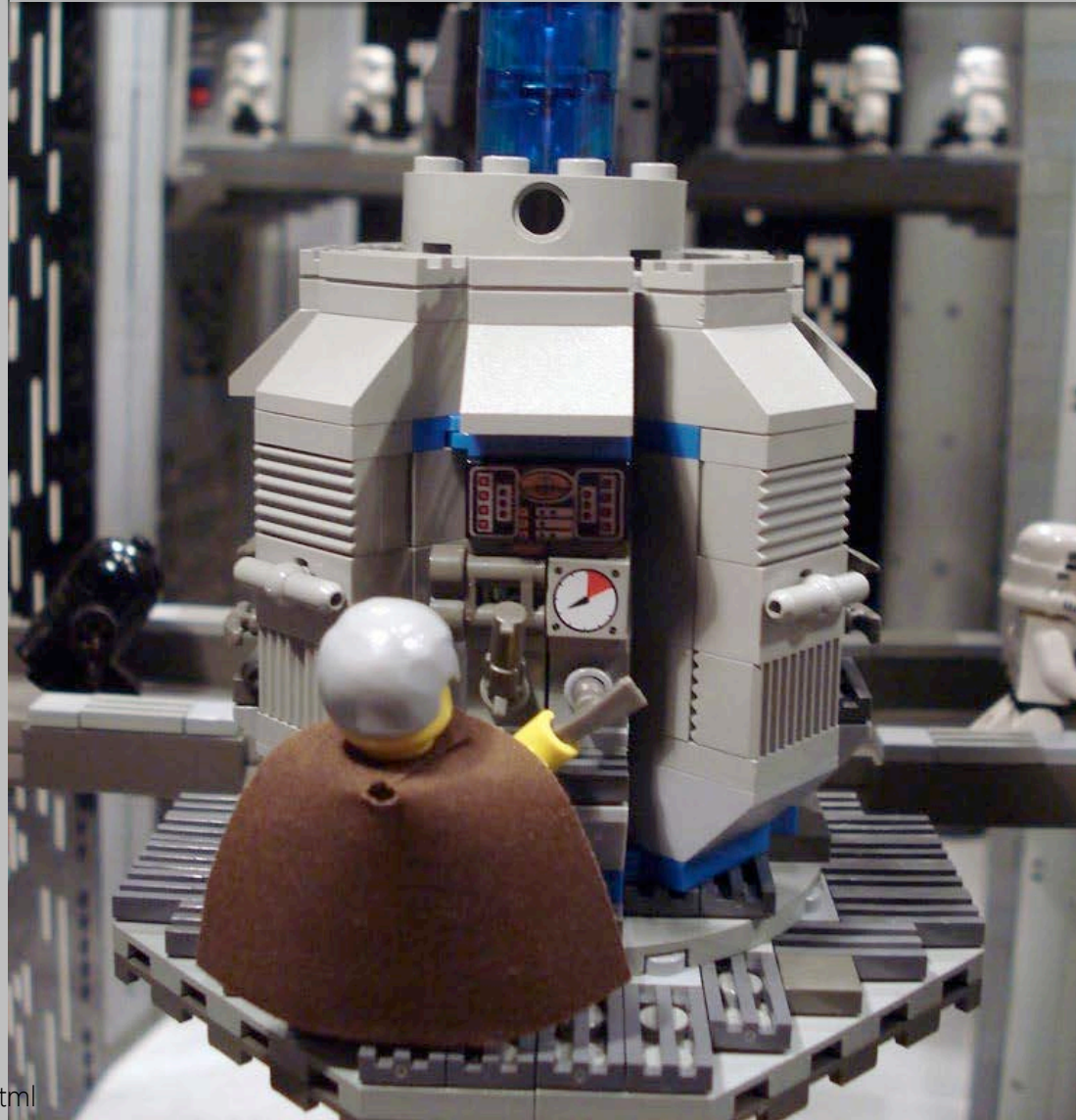
1. What are you building?
2. What can go wrong?
3. What are you going to do about it?
4. Did you do an acceptable job at 1-3?

What Can Go Wrong?
Remember STRIDE

Spooofing



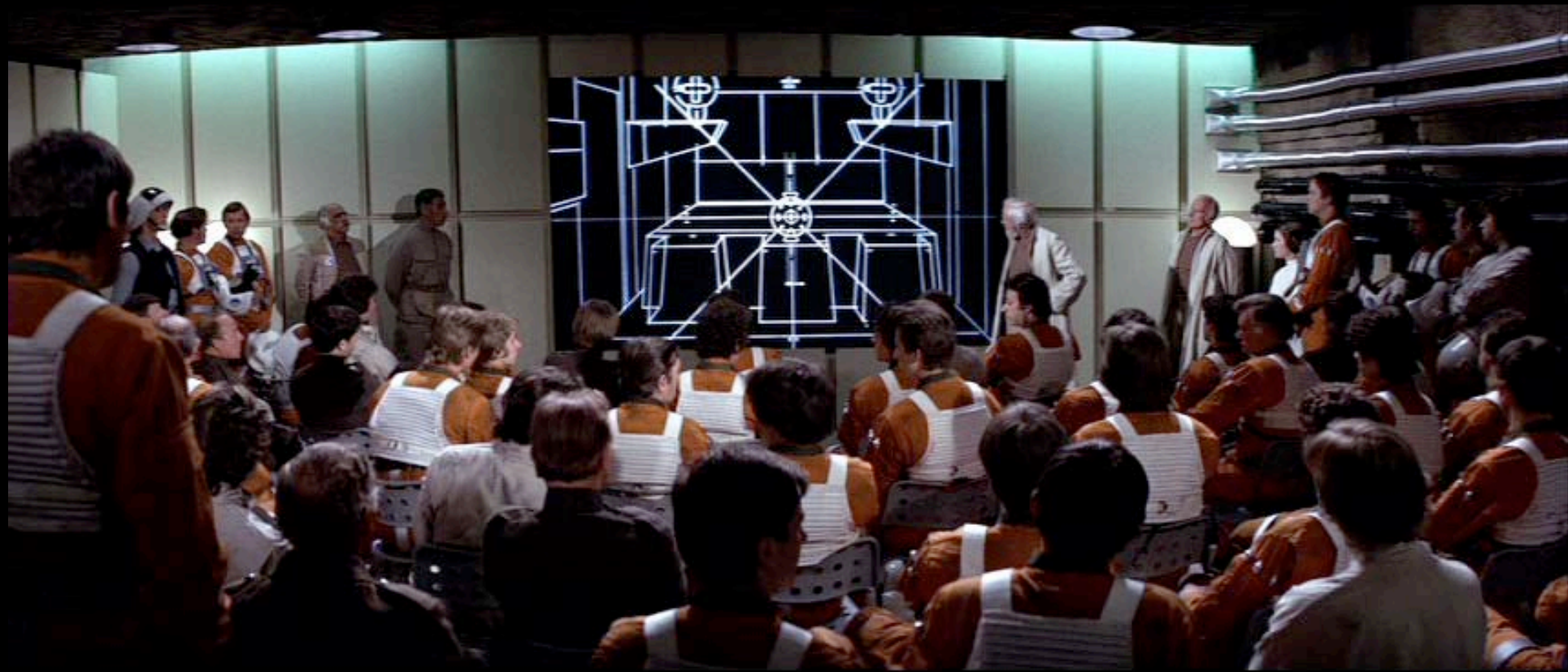
Tampering



Repudiation



Information Disclosure



Information Disclosure (and impact)



Photo by Simon Liu <http://www.flickr.com/photos/si-mocs/6999508124/>

Denial of Service



Model by Nathan Sawaya
<http://brickartist.com/gallery/han-solo-in-carbonite/>

Elevation of Privilege



4 Questions

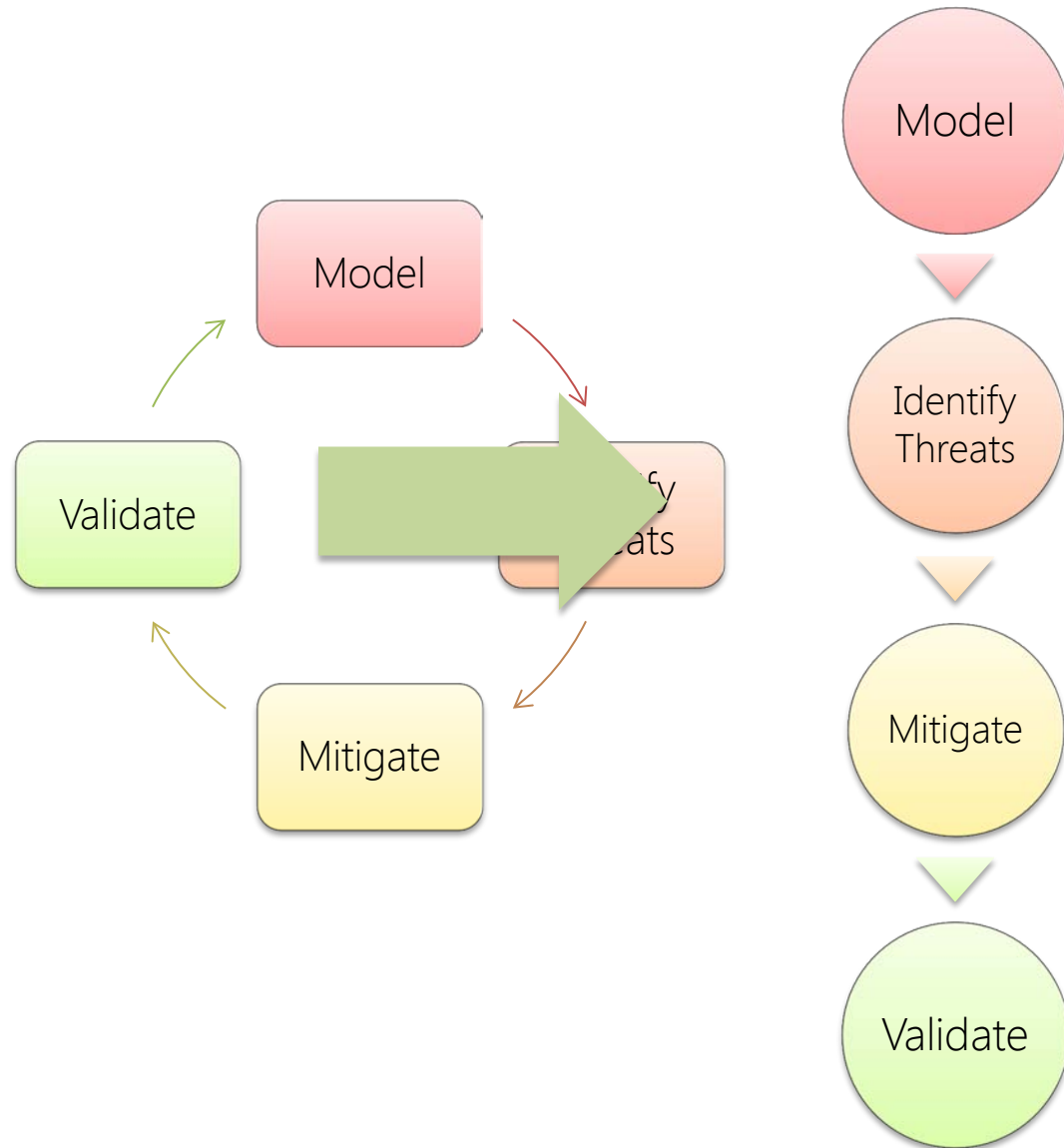
1. What are you building?
2. What can go wrong?
3. What are you going to do about it?
4. Did you do an acceptable job at 1-3?

TOP TEN FOUNDATIONS

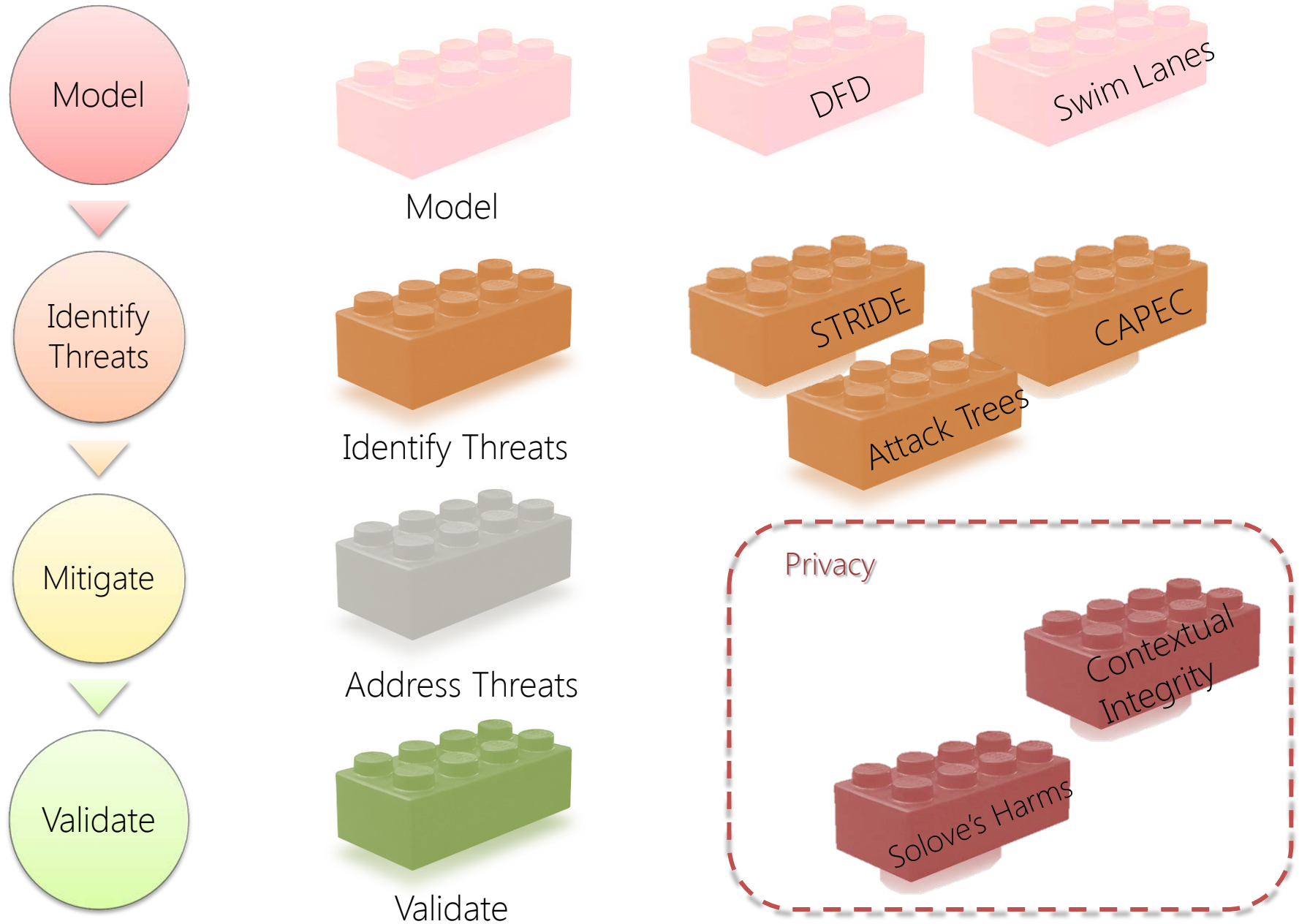
**IT'S
A
TRAP!**



Trap #1: You're Never Done



Trap #2: Monolithic Processes



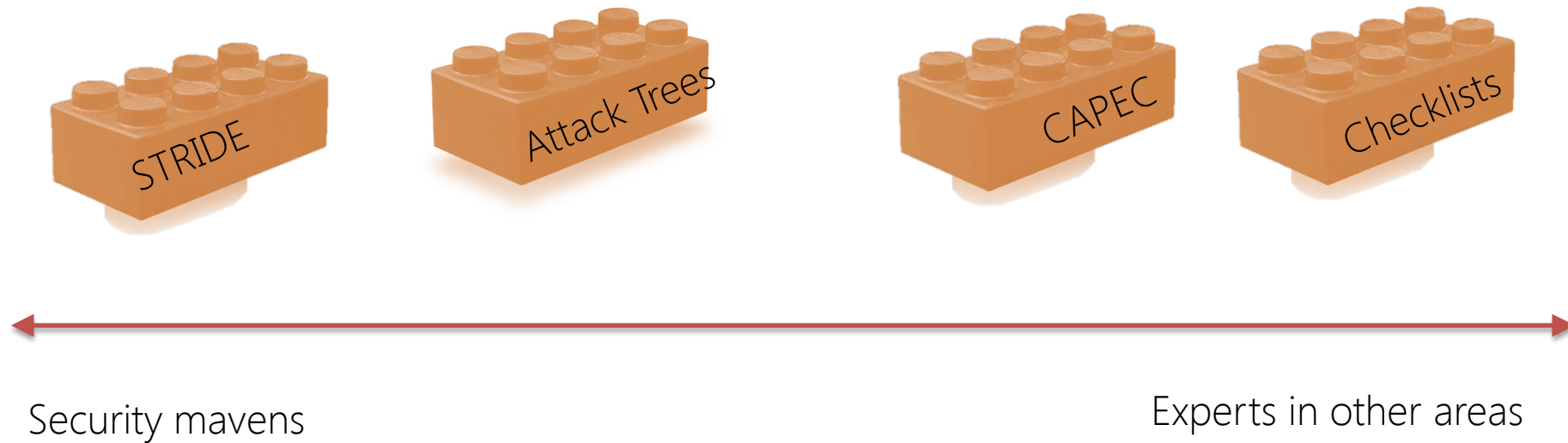
Trap #3: "The Way To Threat Model Is..."

- 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: "The Way To Threat Model Is..."



The Right Way Is The Way That Finds Good Threats

- Adam, 2010:
 - Asset-centric modeling stinks
 - Attacker-centric modeling stinks
- Saying “approach X stinks” stinks*

* Use of the word “stinks” is not approved for corporate slides, which ... is too bad

Trap #3: Focusing on Finding Threats

- Finding threats is a lovely thing if you're focused on security
- Addressing them is even better

The Right Way Is the Way That
Fixes Good Threats

Trap #4: 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 #4A: Threat Modeling in a Vacuum

- 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 #5: Threat Modeling is Born, Not Taught

- Playing a violin...You need to develop and maintain muscles
- Beginners need easy and forgiving tunes
- There's artistry...eventually

Threat Modeling Is Like Playing A Violin

We've got to give them more time!



Trap #6: Threat Modeling as One Skill

- Technique: DFDs, STRIDE, Attack trees
- Repertoire:
 - SSLSpooof, Firesheep
 - Mitnick, Cuckoo's Egg
 - Conficker, Stuxnet and Crilock
- Frameworks and organization
 - Elicitation and memory for experts

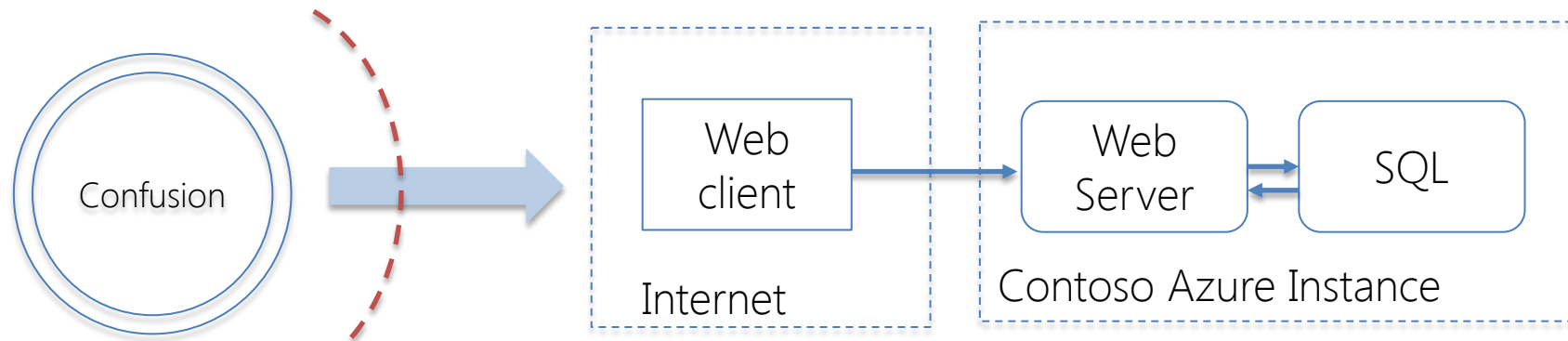
There's Technique and Repertoire

Trap #7: "Think Like An Attacker"

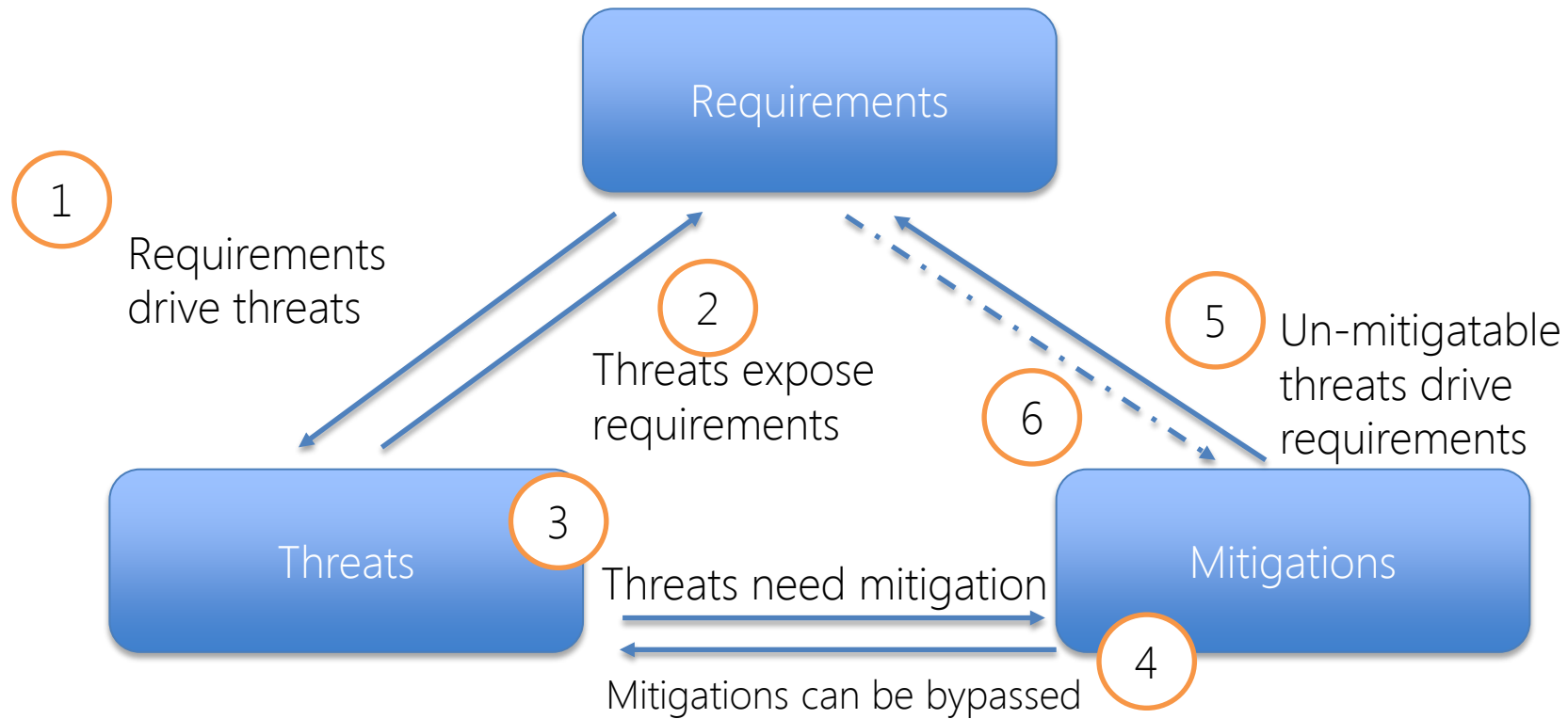
- "Think like a professional chef"
- Most people need structure

Trap #8: "The Model"

- At least two models
 - Model of the technology (software, system)
 - Model of the threats
 - Sometimes a model of the person
 - "Threat Modeling" sounds funny
- Speaking of DFDs
 - Everything in a labeled box boundary
 - Rounded rectangle processes



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"



Three bonus traps!

THREAT MODELING TECHNOLOGIES & TRICKY AREAS

Web Traps!

- Focusing on XSS or SQLi
 - These do not require threat modeling
- Unique problems of your unique technology
- Understand dependencies and trust boundaries

Cloud Traps!

- It's so complicated!
- Outsiders inside your trust boundary
 - Cloud provider ops team
 - Other cloud customers
- Legal threats
 - Forensics & chain of custody
 - Legal threats & "3rd party doctrine"

Human Factors Traps!

- Given a choice between security & dancing babies...
- Threat Modeling can use models of people
 - Behaviorist
 - Cognitive science
- Add people to your software diagrams
 - What's communicated and how?
 - What do you expect them to know?
 - What threats to perception or understanding?

Call to Action

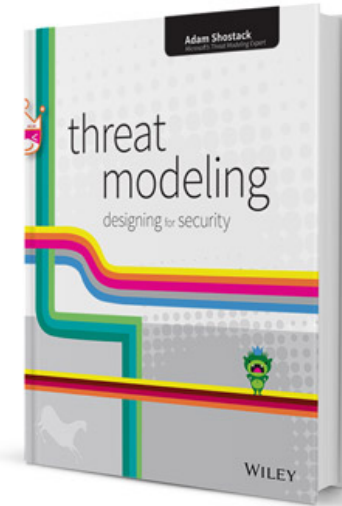
- Remember the 4 Questions
- Be proactive:
 - Find security bugs early
 - Fix them before they're exploited
- Drive threat modeling through your organization

“All models are wrong, some
models are useful”

— George Box

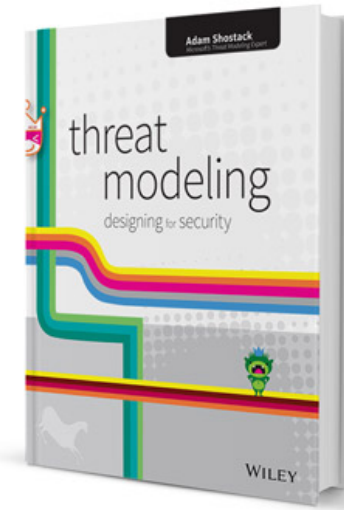
Questions?

- Please use the microphones
- Or tweet @adamshostack
- Or, heck, read the new book 😊
 - Threatmodelingbook.com



Resources

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


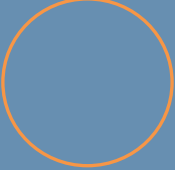


- Helpful tools, Threat trees, Attacker Lists, Elevation of Privilege (the cards), Case studies

Thank you!

- Star Wars: Episodes IV-VI
- Great Creative Commons Lego brick art:
 - Lego Envy, <http://www.eurobricks.com/forum/index.php?showtopic=64532>
 - <http://pinlac.com/LegoDSTractorBeam.html>
 - Seb H <http://www.flickr.com/photos/88048956@N04/8531040850/>
 - Simon Liu <http://www.flickr.com/photos/si-mocs/6999508124/>
 - Kaitan Tylerguy <http://www.flickr.com/photos/kaitan/3326772088/>
 - Nathan Sawaya, <http://brickartist.com/gallery/han-solo-in-carbonite/>
 - <http://www.flickr.com/photos/prodiffusion/>

BACKUP

Different Threats Affect Each Element Type

ELEMENT	S	T	R	I	D	E
 External Entity	✓			✓		
 Process	✓		✓	✓	✓	✓
 Data Store			✓	?	✓	✓
 Data Flow			✓		✓	✓

This isn't the reputation you're looking for...

Searches related to **threat modeling**

[threat modeling example](#) [why is threat modeling difficult to understand](#)

[threat modeling tool](#) [threat modeling tool software](#)

[threat modeling dread](#) [threat modeling ppt](#)

[threat modeling stride](#) [threat modeling book](#)