Advanced Threat Modeling: A Whiteboard Session

Mike Rothman, IANS Faculty

Agenda

- We have 90 minutes to dig into threat modeling and “A Whiteboard Session” indicates we are going to be doing some threat modeling
- First: The basics
  - Why threat model?
  - The threat modeling process
  - Where do threat actors fit in?
- Next: Threat modeling frameworks (and how to use them)
  - STRIDE (to understand the threat)
  - DREAD (to establish priority)
- Finish: Communicating findings
  - Getting the attention of people that (pretty much) don’t care

IANS

Threat Modeling Basics

Threat Modeling Overview

- What is threat modeling?
  - In short – the use of abstraction techniques to think about risk
- Threat modeling helps us think more “tactically and practically” about threats and security overall (optimally) BEFORE things get built
- Key considerations:
  - Threat actors
  - Attack techniques
  - Outcomes and risks
  - Countermeasures

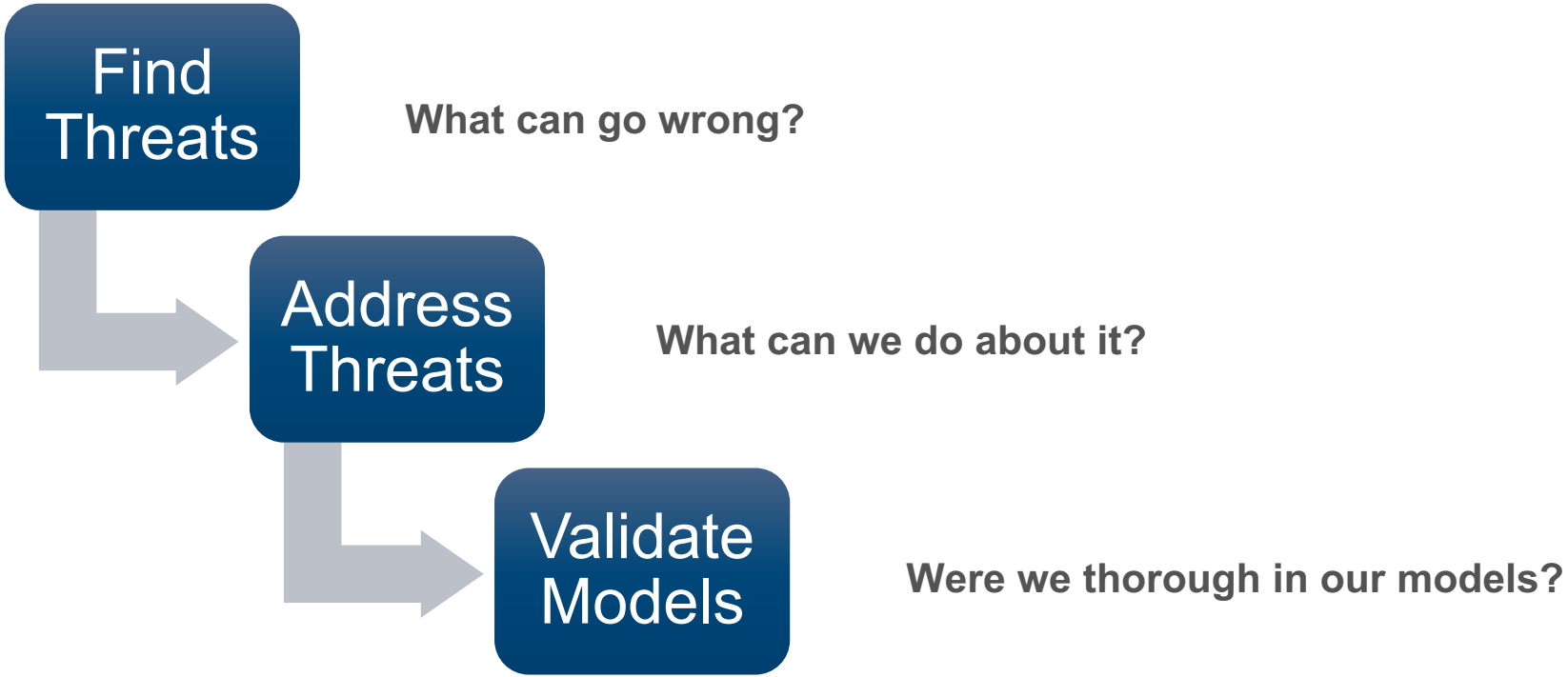
https://flic.kr/p/e61iS9

IANS

Why Threat Model?

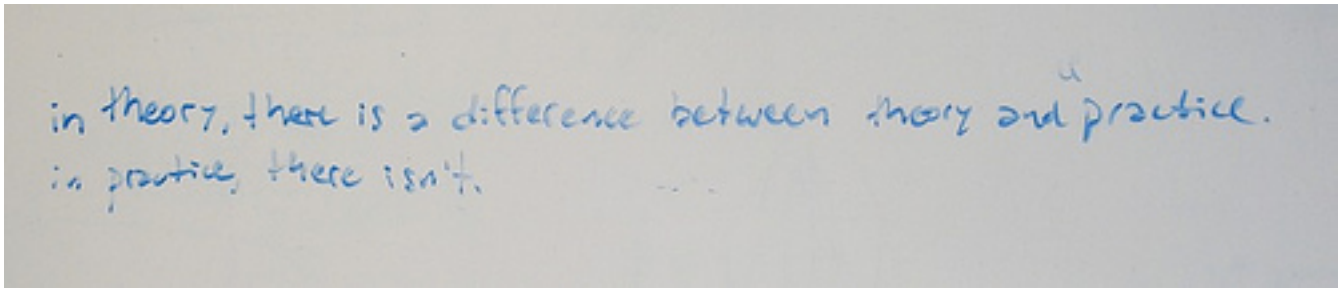
- Threat modeling helps you:
  - Identify threats your system(s) face
  - Educate business owners about risk in a more tangible way
  - Challenge assumptions (developers, architects, security)
- Threat modeling may help to:
  - Focus on appropriate controls (for the application and/or system)
  - Prioritize other security efforts (pen test, review, fuzzing)
- It’s important to document and communicate what you learn when assessing systems, processes and people

A Three-Step Framework



Finding Threats

- Now we have to ask the questions: “What can go wrong” and “How would it happen?”
- This is a brainstorming exercise, nothing more and nothing less
- Start with external entities in MOST cases
- Don’t ignore threats just because they seem less relevant right now
- Focus on practicality – what threats are feasible?
- Our models (STRIDE and DREAD) focus on this



https://flic.kr/p/6qqYwu

IANS

Addressing Threats

- Now we need to look at countermeasures and options for addressing the threats
- Emphasis should be on risk management and controls/processes/policies
- Focus should be on four key areas:
  - Mitigating threats
  - Eliminating threats
  - Transferring threats
  - Accepting risk
- There are many ways to address threats, at various levels of detail

IANS

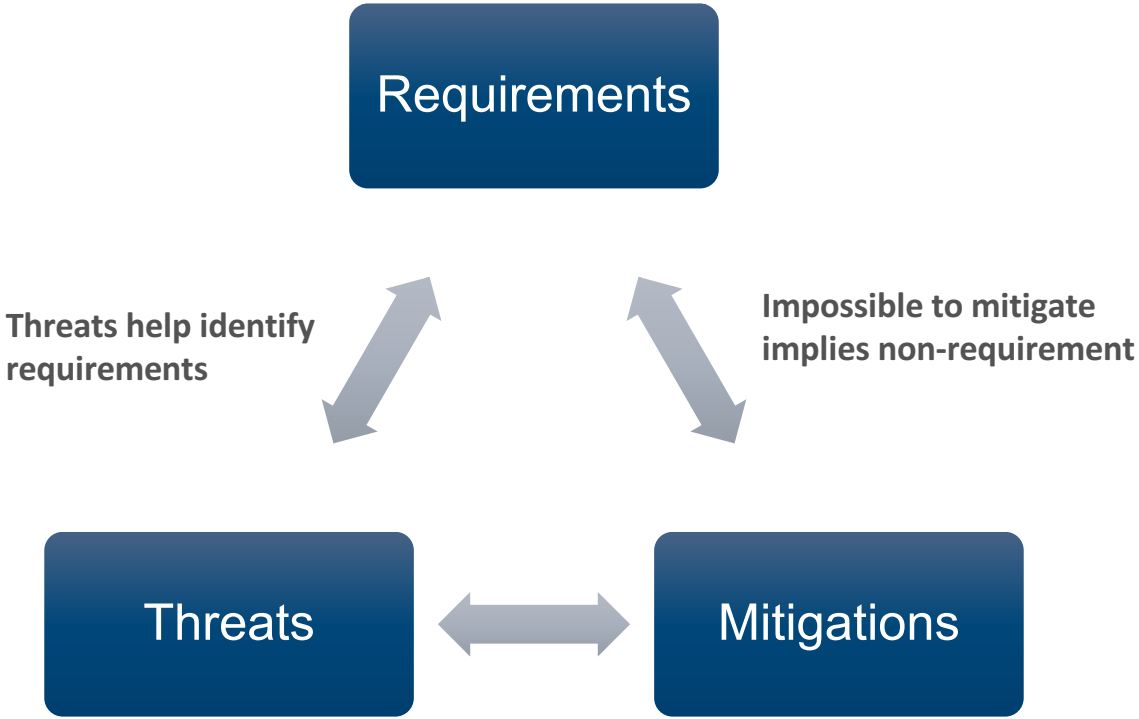
Validating Our Models

- This is really a “gut check”
  - Solicit feedback and input from other teams and groups
- Does the threat model make sense?
  - Does everyone understand and agree on the inputs?
  - Do the attacks and priorities match?
- Is the attack real or viable?
  - Does it reflect reality?

https://flic.kr/p/58ncUm

IANS

The Threat Modeling Process



Attack Libraries

- Attack libraries are much more detailed descriptions of threats and threat data
- Attack libraries should have the following considerations top of mind:
  - Audience
  - Level of detail for attack entries
  - Scope of application
- Can be similar to checklists (but these can be too rigid)
- CAPEC and OWASP Top 10 are good examples

Attack Libraries: CAPEC

- MITRE has created the Common Attack Pattern Enumeration and Classification (CAPEC) attack library
- Current version contains 504 attack entries
- Organized into groups:
  - Social engineering attacks
  - Supply-chain attacks
- Complete attack entries (not all are complete) include:
  - Severity
  - Prerequisites
  - Methods of attack

Attack Trees

- Attack trees are another way to perform threat modeling
- These can be applied to existing system models or created from scratch
- They can also be simple or complex
  - Back-of-the-napkin approaches
  - Detailed and extensive graphic diagrams in Visio and other tools
- Attack trees are really useful for visualizing threats, attacks and potential outcomes

Building Attack Trees

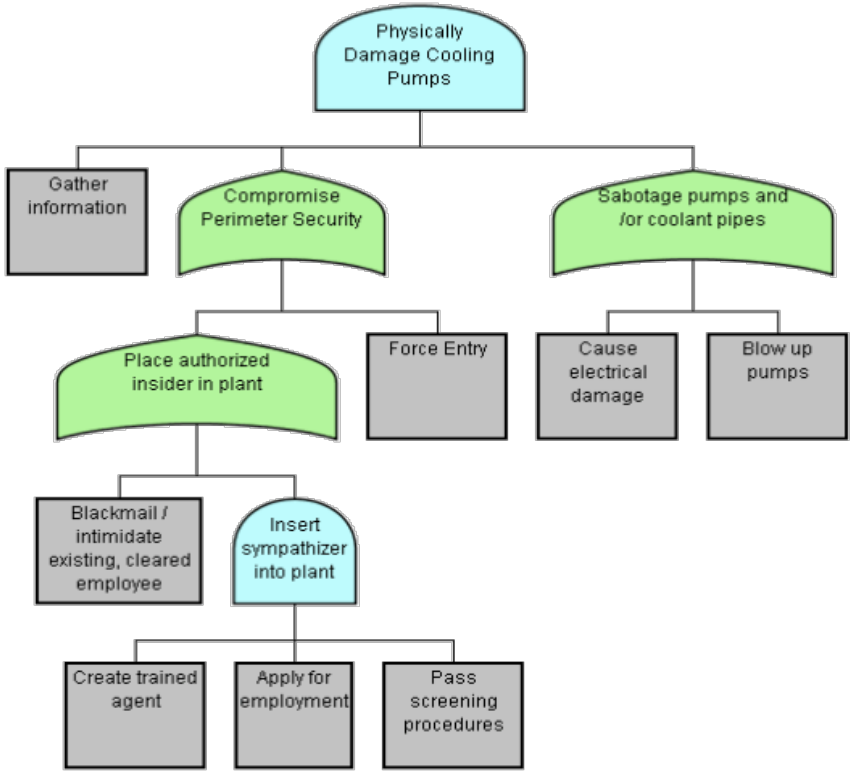
- Decide on a representation
- Create a root node
- Create sub-nodes
- Consider completeness
- “Prune” the tree
- Check the presentation

https://flic.kr/p/4z51Xs

Attack Tree Specifics

- Create a root node:
  - Choose an attacker goal or high-impact action
  - Usually an OR model is more appropriate at this level
- Create sub-nodes:
  - Start with the idea of attacking a system:
    - Physical access
    - Software subversion
    - People subversion

Example (Simple)



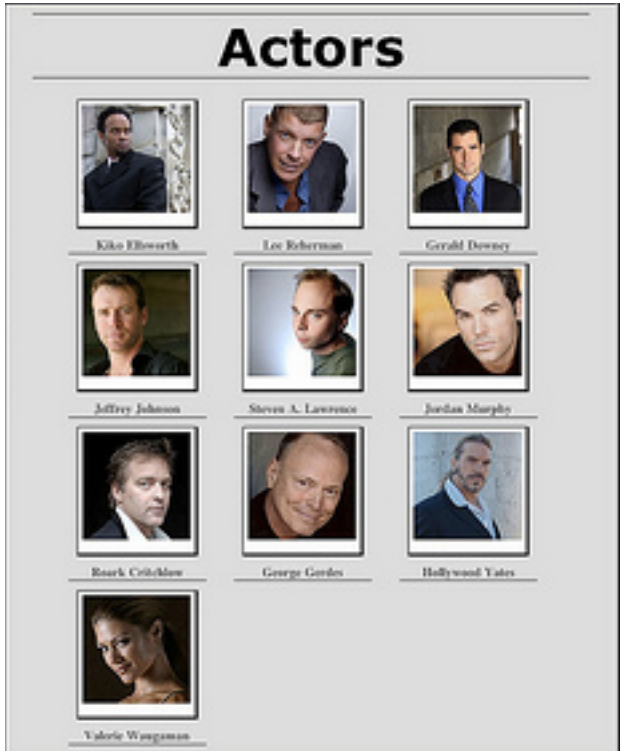
IANS

Tips on Attack Libraries/Trees

- Don’t be afraid to come up with an “anything goes” mentality at first
  - You can always prune things
- Unless you have a need to, use someone else’s attack libraries
  - At least as a starting point

Threat Actors

- Consider the adversaries when building the threat models
  - Reduce the attack surface
  - Add realism to the model
- Categorize threat actors:
  - Unsophisticated
  - Financially motivated
  - Competitors
  - Nation-states (if applicable)



https://flic.kr/p/86z4f6

Let's Build a Simple Attack Tree

- Attacker goal: Compromise an endpoint
- Focus the exercise based on the threat actor
  - First: Teen hacker using open source tools
- How would the attack tree change if the threat actor is a financially-motivated group?

Threat Modeling Frameworks

The STRIDE Model

IANS

Spoofing

- Definition: Pretending to be someone/something else
- Property violated: Authentication
- Targets/victims: Processes, people, external entities
- Examples:
  - Claiming to be an exiled prince or a co-worker in a phishing email
  - Changing a source IP address when performing a denial-of-service attack

Tampering

- Definition: Modifying something stored, in network traffic or in memory (being processed)
- Property violated: Integrity
- Targets/victims: Data stores, data flows, processes
- Examples:
  - Changing a value in a spreadsheet
  - Manipulating packets in network traffic
  - Planting a backdoor in a binary

Repudiation

- Definition: Claiming you didn’t do something
- Property violated: Non-repudiation
- Targets/victims: Processes
- Examples:
  - “No, I didn’t trip over the power cord”
  - “That wasn’t me that sent that email”
  - “I never got that phone call”

Information Disclosure

- Definition: Information exposed or provided to someone not authorized to see it
- Property violated: Confidentiality
- Targets/victims: Processes, data stores, data flows
- Examples:
  - Data loss or breaches
  - Accidental exposure of HR data to employees
  - Illicit monitoring of credit card data in memory by malware

Denial of Service

- Definition: Taking or absorbing resources required to provide service
- Property violated: Availability
- Targets/victims: Processes, data stores, data flows
- Examples:
  - A program hogging memory or CPU
  - Overwhelming numbers of packets

Elevation of Privilege

- Definition: Allowing users to do something they're not allowed to do
- Property violated: Authorization
- Targets/victims: Processes
- Examples:
  - Regular users running programs as an admin
  - Remote users without privileges running code or accessing systems

STRIDE Examples

What Are You Going to Do About It?		
Spoofing	Authentication	• Passwords, multi-factor authentication • Digital signatures
Tampering	Integrity	• Permissions/ACLs • Digital signatures
Repudiation	Non-repudiation	• Secure logging and auditing • Digital signatures
Information disclosure	Confidentiality	• Encryption • Permissions/ACLs
Denial of service	Availability	• Permissions/ACLs • Filtering • Quotas
Elevation of privilege	Authorization	• Permissions/ACLs • Input validation

IANS

Let's Use STRIDE

- Threat models can be very useful to make risks against emerging technology "more real"
- Whiteboard example: IoT
- Use STRIDE to help a medical device maker understand how its pacemaker can be attacked
  - Consider remote monitoring (device phones home to transmit data)
  - Pacemaker connects to a device, which then sends information to the web service (which is then accessed by the doctor)

DREAD: Prioritizing the Threats

- Microsoft also came up with the DREAD model to quantify the risk (and help prioritize action)
  - **D**amage potential
  - **R**eproducibility
  - **E**xploitability
  - **A**ffected users
  - **D**iscoverability
- Awesome blog post to describe the process: https://blogs.msdn.microsoft.com/david_leblanc/2007/08/14/dreadful/

IANS

Using DREAD

- Quantify the rules that work for you – use them consistently
- Damage, reproducibility and affected users are measures of severity
  - But damage is a much more significant measure
- Severity = Damage + f(R, A)
  - If R + A > 4 (both high, or one high and the other at least medium), add 2
    else if R + A > 3 (one high, or both medium) add 1
    else add 0
- But what about exploitability and discoverability?
  - Exploitability is situational
  - Discoverability is subjective (and hard to gauge)

IANS

Using DREAD (continued)

- Quantify E & Di and use as magnifiers on severity
  - If E = high, Di = high, add 4
    else if one is high, other medium, add 3
    else if one is high, other low, add 2
    else if both medium, add 1
    else add 0
- Establish actions based on DREAD score
  - Development threat models (ignore, roadmap, patch, high-priority patch, RED ALERT)
  - System threat models (ignore, process change, workaround, URGENT FIX)
  - Consistently apply the scores to generate action; adapt the model as needed
- A note from David LeBlanc, originator of DREAD:
  "Warning! Do NOT apply this system, or any other system, without THINKING about it"

Let's Use DREAD

- Scenario:
  - Financially-motivated threat actor
  - Moving to SaaS-based general ledger
  - Threat is a compromised endpoint, based on attack tree discussed earlier

https://flic.kr/p/KeHZH

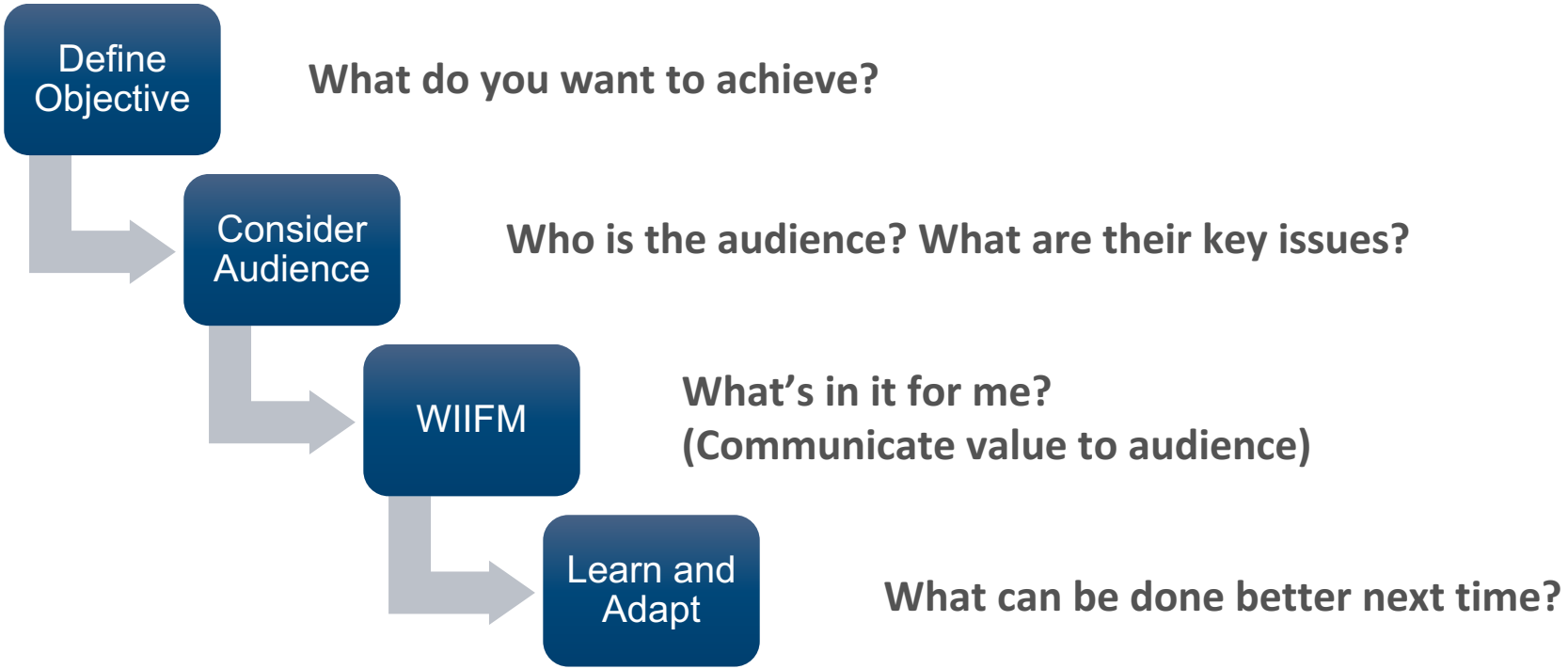
Now DREAD

- Now we can quantify the threat to determine what action to take…
- Evaluate each on high, medium, low.
  - **D**amage
  - **R**eproducibility
  - **E**xploitability
  - **A**ffected Users
  - **D**iscoverability
- **Take action**
  - **1:** Ignore
  - **2 – 4:** Process change
  - **5 – 8:** Workaround
  - **8 – 10:** URGENT FIX

IANS

Communications

Communicating the Threat Model



Communicating the Threat Model

- Best case: Threat modeling can be used to favorably impact security posture
- Not so best case: Use the threat model to communicate risk to business leaders (and cover your backside)
- It's striking a balance between being alarmist (Chicken Little) and creating urgency

Key Takeaways

- Threat modeling is a tool, like any other; know why you are using it, and how best to communicate the findings
- Threat modeling is subjective and will never find all of the threats; it's about illustrating risks, not being comprehensive
- Consistency in quantifying the evaluation of the threats is critical; strive to take the emotion out of prioritization
- Build credibility by promoting threat modeling wins (finding issues prior to release/breach/issue)

Questions?

info@iansresearch.com