Threat Modeling Workshop

CodeMash 2019
January 8, 2019
Robert Hurlbut
@RobertHurlbut

Bank of America

BANK OF AMERICA | MERRILL LYNCH | U.S. TRUST | BANK OF AMERICA MERRILL LYNCH

Who am I?

Robert Hurlbut
SVP, Threat Modeling Architect / Lead
Cyber Security Technology
Bank of America

Agenda

Why Threat Modeling?

What is Threat Modeling?

Threat Modeling Process

Hands-on Exercises / Labs

What's next?

Pre-Compiler Materials

https://github.com/rhurlbut/CodeMash2019

Why Threat Modeling?

Software Design

Determine requirements
Determine features
Build software people will use

Secure Software Design

Determine secure requirements
Determine secure features
Build software people will use
… and anticipate things going wrong

Example Secure Design Issue:
How to secure data in the cloud?

Storage?
Accessed?
Monitored?
Configured properly?

Threat Modeling helps us focus on these questions and answers to lead to secure design

Common data breach problem

Misconfigured AWS S3 Buckets

Impacted in 2017-2018 *:

- FedEx
- GoDaddy
- Accenture
- Verizon
- American voter data (198 million American voters)
- National Credit Federation
- Booz Allen Hampton
- Dow Jones
- Keeper and Blur (password managers)

* https://www.zdnet.com/article/security-lapse-exposes-198-million-united-states-voter-records/

Value of threat modeling

Ed Moyle (2017):

*"Very few organizations will have the time or resources to **threat model** their entire ecosystem. Assuming you do not have that luxury, you still can realize quite a bit of **value** just by adopting the mindset of looking for blind spots and questioning assumptions."* *

* (Quoted from an article by Ed Moyle: https://www.ecommercetimes.com/story/Invisible-Technologies-What-You-Cant-See-Can-Hurt-You-84852.html)

What is Threat Modeling?

What is threat modeling?

You probably (hopefully!) already do these in your security strategy:

- Penetration testing
- Vulnerability assessments
- DAST / SAST tools
- Other automated tools …

But, if not threat modeling – you are missing a lot!

What is threat modeling, continued?

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, continued?

When we ...

think ahead on what could go wrong

(i.e. the " what if" questions),

weigh the risks,

and act accordingly ...

... we are "**threat modeling**"

What is threat modeling, continued?

Threat modeling is:

Process of understanding your system and potential threats against your system

i.e. ***Critical Thinking*** about Security

Approaches to Threat Modeling

Asset-centric

Software-centric

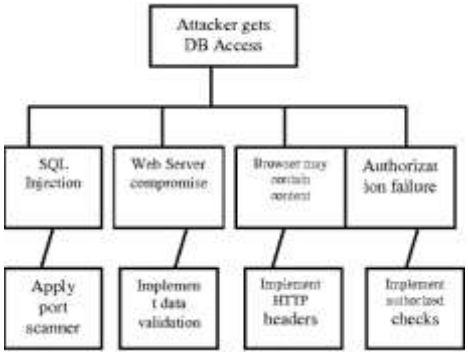
Attacker-centric

Approaches to Threat Modeling – Asset-centric

Assets

Things of value. For example: Databases which may contain credit card data, personal Identifiable Information (PII), etc.

Attack trees

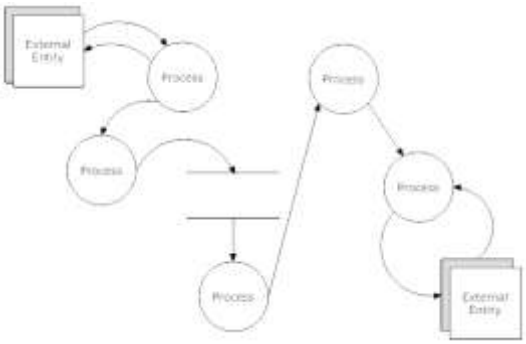


Approaches to Threat Modeling – Software-centric

Secure Design

Understanding secure activity within an architecture

DFDs



Approaches to Threat Modeling – Attacker-centric

Profiles	Patterns
Script Kiddie	Copies scripts – tries anything
Hacktivist	Political agenda – deface website
Nation-state attacker	Money, intellectual property theft - phishing

Threat Modeling your House

Asset-centric

Family, irreplaceable photos, valuable artwork

Software-centric

Physical features (front and back porch)

Attacker-centric

Who might break in, current security system

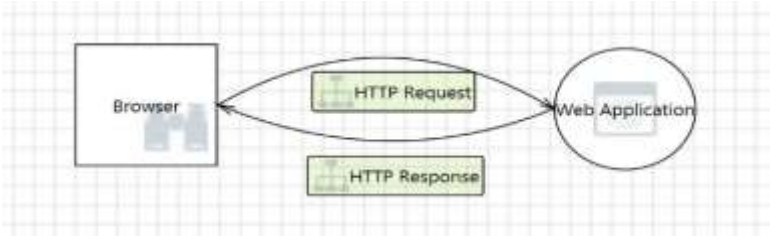
What is threat modeling?

Threat model includes:

understanding of system,
identified threat(s),
proposed mitigation(s),
priorities by risk

Threat Model – Example – Simple Web Application

Understanding of system (requirements, a diagram, etc.)



Identify threats - what could go wrong?

- Open HTTP connections -> attacker sees data in transit (Information disclosure)
- Open HTTP connections -> attacker changes data in transit (Tampering)
- Broken authentication -> attacker pretends to be someone else (Spoofing)
- Etc.

Proposed mitigations:

- HTTPS (encrypted connections)
- Strong authentication (2FA, centralized)

Priorities by Risk:

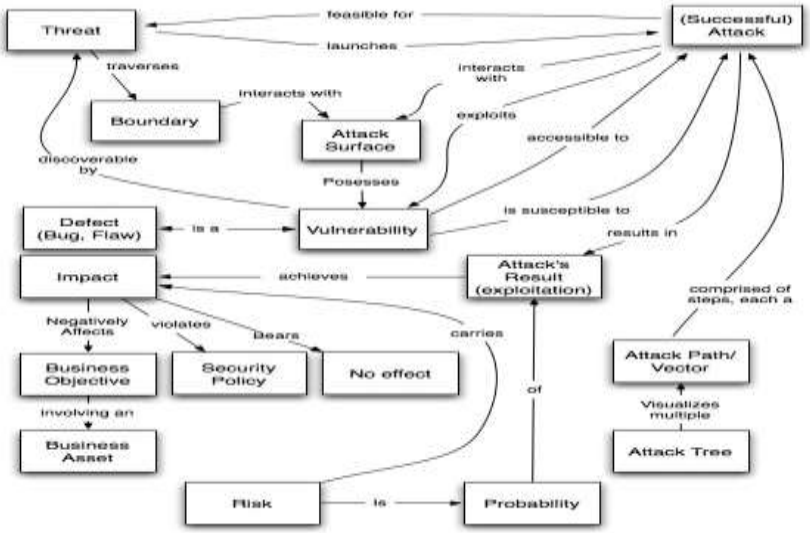
- Which one do you fix first?

Threat Modeling Definitions

Asset	Something of value we want to protect
Threat Agent	Someone or process who could do harm
Threat	Exploits vulnerabilities (intentional or accidental) to obtain, damage, or destroy an asset
Vulnerability	Flaw in system helps threat agent realize threat
Risk	Potential for loss, damage, destruction of asset from threat using vulnerability
Attack	Motivated and sufficiently skilled threat agent takes advantage of vulnerability

23

Threat Modeling Vocabulary*



* https://www.cigital.com/blog/threat-modeling-vocabulary/ (John Steven, Synopsys)

When? Make threat modeling first priority

In SDLC – Requirements and Design phase(s):
Requirements > Design > Development > Test > Deployment

Threat modeling -> new requirements

Incremental threat modeling -> Agile / DevOps (User Stories, Attacker Stories)

Teach threat modeling to your teams

Training

Help / Model

Encourage

Follow Up

Threat Modeling: Getting Started

Typical Threat Modeling Session

Domain Knowledge
Team
Business / Technical Goals
Focused

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

Simple Tools

Whiteboard

Visio (or equivalent) – diagraming

Word (or equivalent) / Excel (or equivalent) - documenting threats / mitigations

Threat Model Sample Worksheet

	A	B	C	D	E	F	G
1	Threat Model Worksheet						
2							
3	ID	Risk Level (H, M, L)	Threat	Description / Impact	Countermeasures	Components Affected	Follow Up Plan
4							
5							

Other Tools

Tool	Cost	Platforms
MS Threat Modeling Tool (2016/2018)	Free	Windows OS Install only
ThreatModeler	Paid	Web Based
IriusRisk	Paid	Web Based
OWASP Threat Dragon	Free	Web Based / Windows, Mac, Linux installs
Draw.IO	Free	Web Based / Windows, Mac, Linux installs

IEEE Computer Society's Center for Secure Design (2015)

http://www.computer.org/cms/CYBSI/docs/Top-10-Flaws.pdf

Avoiding the Top 10 Software Security Design Flaws:
Bugs vs Flaws

Bug – an implementation-level software problem

Flaw – deeper level problem - result of mistake or oversight at design level

In Threat Modeling, we try to identify design flaws to improve secure design

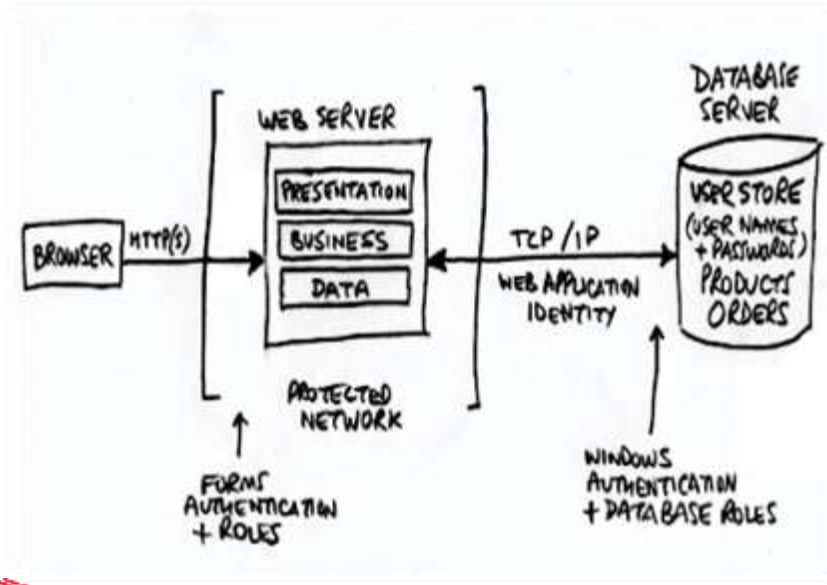
Threat Modeling Process

Threat Modeling Process

1. Diagram / understand your system and data flows
2. Identify threats through answers to questions
3. Determine mitigations and risks
4. Follow through

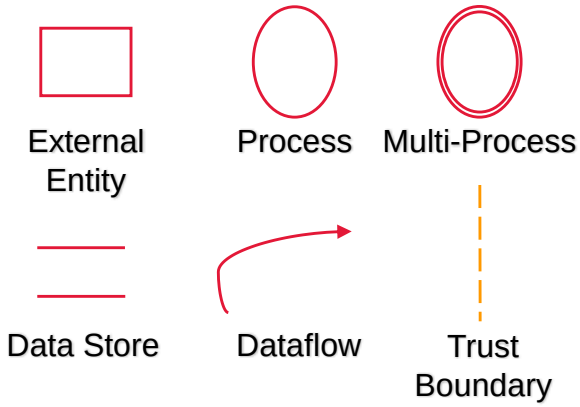
Threat Modeling Process:
Diagram / understand

Draw a picture



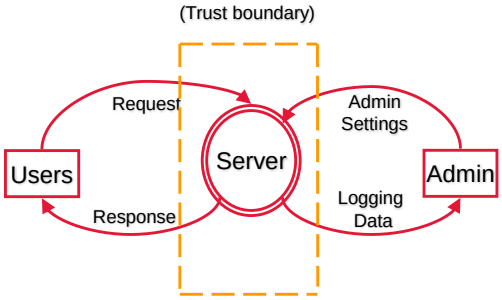
Understand the system

DFD – Data Flow Diagrams (MS SDL)

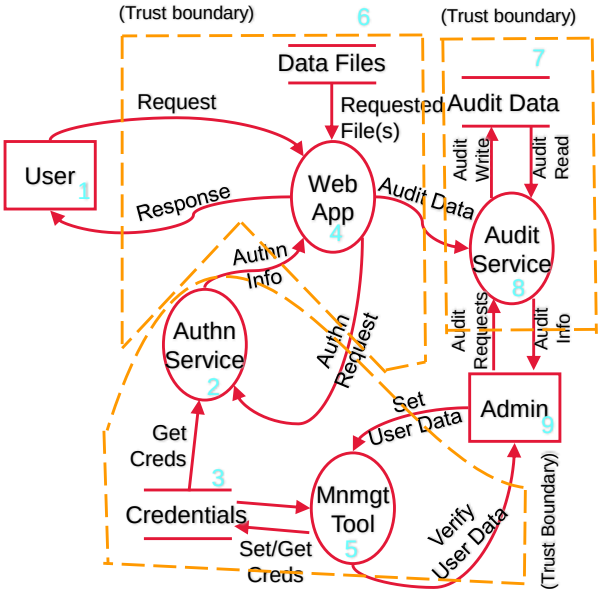


Understand the system

Logical and component architecture
Communication flows
Data moved and stored



Understand the system



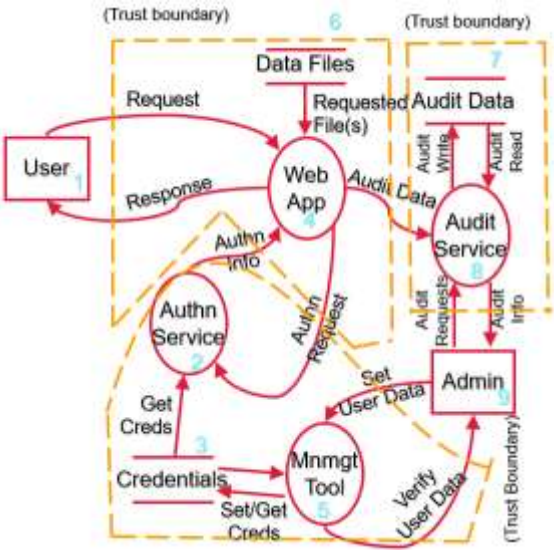
Understand the system

External Entities:
Users, Admin

Processes:
Web App, Authn Svc, Audit Svc, Mnmgt Tool

Data Store(s):
Data Files, Credentials

Data Flows:
Users <-> Web App
Admin <-> Audit Svc



Your threat model now consists of …

1. Diagram / understand your system and data flows

Threat Modeling Lab 1:
Review case study
Build data flow diagram (DFD)

Threat Modeling Process:
Identify threats

Identify threats – Many Ways

STRIDE

Attack Trees

Bruce Schneier - Slide deck

Threat Libraries

CAPEC, ATT&CK, OWASP Top 10, SANS Top 25

Checklists

OWASP ASVS, OWASP Proactive Controls

Card Games

OWASP Cornucopia, Elevation of Privilege

Use Cases / Misuse Cases

45

STRIDE Framework – Data Flow

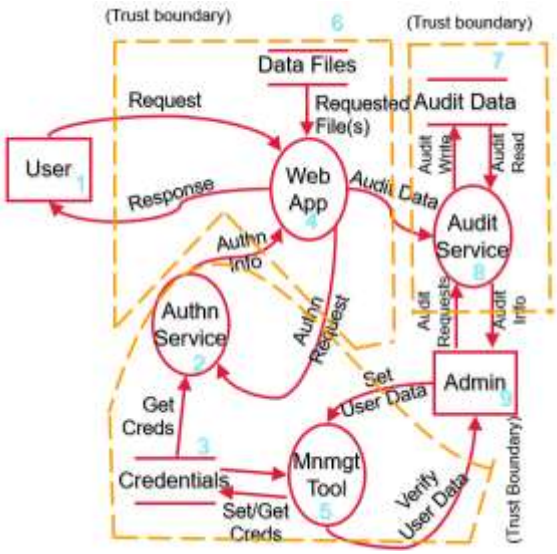
Threat	Examples	Property we want
Spoofing	Pretending to be someone else	Identity Assurance
Tampering	Modifying data that should not be modifiable	Integrity
Repudiation	Claiming someone didn't do something	Non-repudiation
Information Disclosure	Exposing information	Confidentiality
Denial of Service	Preventing a system from providing service	Availability
Elevation of Privilege	Doing things that one isn't suppose to do	Least Privilege

Using STRIDE to Identify Threats

Spoofing
User could be spoofed by an attacker to connect to Web App

Tampering
Requests from User to Web App may be modified

Repudiation
How would we know actions performed by the Web App?

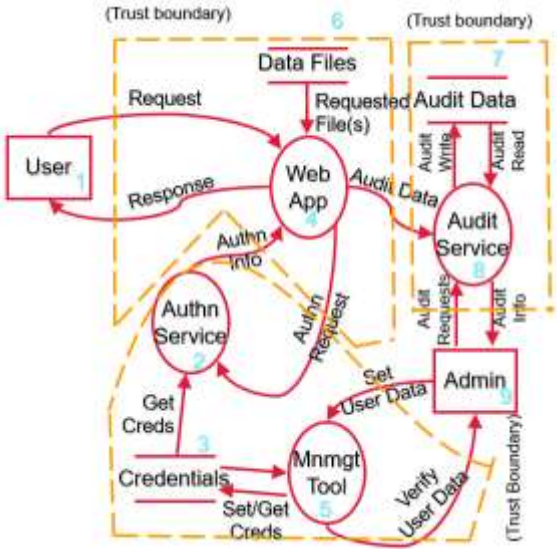


Using STRIDE to Identify Threats

Information Disclosure
Setting and getting credentials could be exposed in transit

Denial of Service
What happens if Authentication Service is not available?

Elevation of Privilege
Does audit data have access control for reading?



Identify Threats – Functional

Input and data validation
Authentication
Authorization
Configuration management
Data Classification
- Public, Proprietary, Confidential

Identify Threats – Functional

Session management
Cryptography
Parameter manipulation
Exception management
Auditing, logging, and monitoring

Identity Threats – Ask Questions

Who's interested in app and data (threat agents)?

What goals (assets)?

What attack methods (how)?

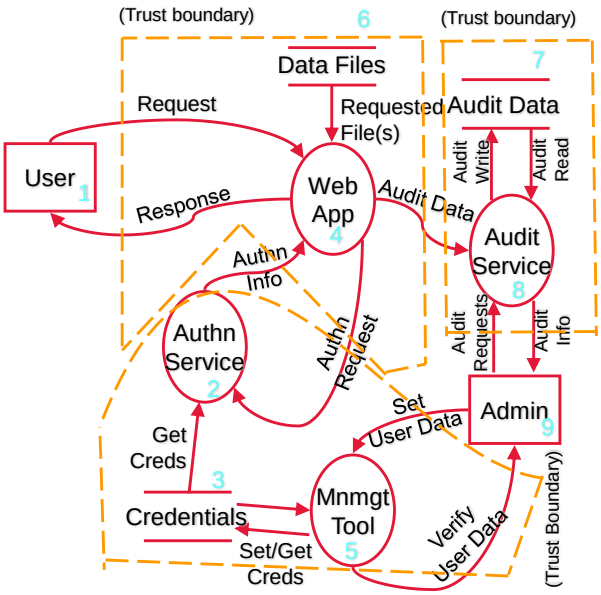
Any attack surfaces (trust boundaries) exposed?

Any input/output (data flows) missing?

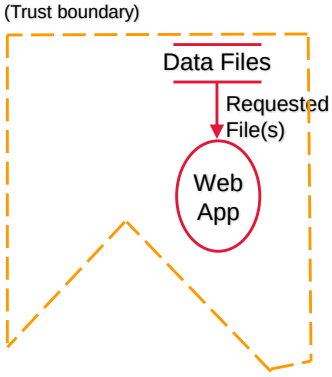
One of the best questions …

Is there anything keeping you up at night worrying about this system?

Scenario – Configuration Management



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 to identify threats:
How does the app use the configuration files?
What validation is applied?
Implied trust?
Can anyone update / change the files?

Your threat model now consists of …

1. Diagram / understand your system and data flows
2. Identify threats through answers to questions

Threat Modeling Lab 2: Identify threats

Threat Modeling Process: Determine mitigations and risks

Determine mitigations and risks – Controls mapped to STRIDE

STRIDE	Example controls
Identity Assurance (Spoofing)	• Authentication based on key exchange • Decide on single-factor, two-factor, or multi-factor authentication • Offload authentication to another provider • Restrict authentication to certain IP ranges or locations
Integrity (Tampering)	• Data protected from tampering with cryptographic integrity mechanisms • Only enumerated authorized users may modify data
Non-Repudiation (Repudiation)	• Maintain logs • Digital signature
Confidentiality (Information Disclosure)	• Data in files / database will only be available to authorized users • Name / existence of database will only be exposed to authorized users • Content and existence of communication between Alice and Bob will only be exposed to these authorized users
Availability (Denial of Service)	• Rate limiting or throttling access to a service • Real-time monitoring of log files and other resources to note sudden changes
Least Privilege (Elevation of Privilege)	• System has a central authorization engine • Authorization controls stored with item being controlled using ACLs • System limits who can write data to higher integrity level • System uses roles / accounts or permissions to manage access

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 and threat identified?

Determine mitigations and risks

Risk Management

FAIR (Factor Analysis of Information Risk) – Jack Freund, 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
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

Risk Rating	Description
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

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

Scenario – Configuration Management

System: Web application uses configuration files
Security principles:
Be reluctant to trust, Assume secrets not safe
Questions to identify threats:
How does the app use the configuration files?
What validation is applied?
Implied trust?
Can anyone change / update the files?
Possible controls / mitigations:
Set permissions on configuration files.
Validate all data input from files.
Use fuzz testing to insure input validation.

Scenario – Configuration Management

System: Web application uses configuration files
Security principles:
- Be reluctant to trust, Assume secrets not safe

Questions to identify threats:
- How does the app use the configuration files?
- What validation is applied?
- Implied trust?
- Can anyone change / update the files?

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

Risk Rating:

- **On Prem (Medium/Low) vs. Cloud (High)**

Your threat model now consists of …

1. Diagram / understand your system and data flows
2. Identify threats through answers to questions
3. Determine mitigations and risks

Threat Modeling Lab 3: Determine mitigations

Threat Modeling Process: Follow through

Follow through

Document findings and decisions

File bugs or new requirements

Verify bugs fixed / new requirements implemented

Did we miss anything? Review again

Anything new? Review again

Your threat model now consists of …

1. Diagram / understand your system and data flows
2. Identify threats through answers to questions
3. Determine mitigations and risks
4. Follow through

A living threat model!

What next?

What next?

Look at tools that can help take you further (DFDs):

- MS Threat Modeling Tool 2018
- OWASP Threat Dragon
- Draw.IO – see Michael Enriksen's article: https://michenricksen.com/blog/drawio-for-threat-modeling

What next, continued?

Learn more about:

- Attack Trees
  - Bruce Schneier's 1999 article
- Incremental Threat Modeling
  - Agile approaches – Irene Michlin (@IreneMichlin)
- Lateral Movement
  - "The Industrial Revolution for Lateral Movement" BlackHat 2017

75

What next, continued?

Learn more about:

- List vs Graph Thinking, Recursive Threat Modeling
  - John Lambert (@JohnLaTwC) at Microsoft

What next, continued?

Learn more about:

- Threat Modeling as Code
  - ThreatPlaybook (@abhaybhargav)
  - ThreatSpec (@ThreatSpec, @zeroXten)

77

Conclusion

Get started with Threat Modeling today:

Start with secure design as goal

Ask the “what if” questions

Understand bigger picture

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

Microsoft Threat Modeling Tool 2018

https://aka.ms/threatmodelingtool

ThreatModeler – Web Based (in-house) Tool

http://myappsecurity.com

IriusRisk Software Risk Manager

https://iriusrisk.continuumsecurity.net

OWASP Threat Dragon

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

Resources - Tools

Attack Trees – Bruce Schneier on Security
https://www.schneier.com/attacktrees.pdf

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

OWASP Application Security Verification Standard (ASVS)
https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

OWASP Top 10 Proactive Controls 2018
https://www.owasp.org/index.php/OWASP_Proactive_Controls

81

Questions?

Slides:
https://roberthurlbut.com/r/CM19TMW

@RobertHurlbut

Thank you!