Developing a Threat Modeling Mindset

NH Cybersecurity Symposium 2023
March 28, 2023

Robert Hurlbut
Twitter: @RobertHurlbut
LinkedIn: roberthurlbut

Who am I?

Robert Hurlbut

Principal Application Security Architect / Threat Modeling Lead @ Aquia, Inc. (https://aquia.us)

Aquia is a Service-Disabled, Veteran-Owned, Small-Business (SDVOSB)
AWS Partner / AWS Public Sector Partner

Focused on:

- **Software Security: Threat Modeling, Supply-Chain Security, DevSecOps, SaaS Governance, Training / Enablement**
- **Governance, Risk, and Compliance (GRC)**
- **Solution Development**
- **Zero to FedRAMP**

Who am I? (continued)

Co-organizer of Boston Code Camp (20th Anniv) – Free developer conference – returning in-person

https://bostoncodecamp.com/

Co-host of Application Security Podcast

https://www.securityjourney.com/resources/application-security-podcast

On Twitter: @AppSecPodcast

Leader of Amherst Security Group (Meetup)

https://www.meetup.com/AmherstSec

On Twitter: @AmherstSec

Who am I? (continued)

Co-author of "**Threat Modeling Manifesto**" (2020)

https://threatmodelingmanifesto.org/

- Definition
- Values
- Principles
- Anti-Patterns

Co-founder of **Threat Modeling Connect** (Fall, 2022)

https://www.threatmodelingconnect.com/

- Support and insights from other Threat Modelers
- Monthly Community Meetups
- Threat Modeling Hackathons
- Threat Modeling Open Forum
- First Threat Modeling Conference – November, 2023

What is Threat Modeling?

Historically, Threat Modeling originated in 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 (2015) 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 (2015) by Tony UcedaValez and Marco M. Morana)

A Threat Modeling Mindset is …

Strategic vs Reactive

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
- When we look around to cross the street

What is Threat Modeling? (continued)

When we think ahead on:

- What could go wrong (*ask "what if" questions)*
- Weigh risks
- Act accordingly

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

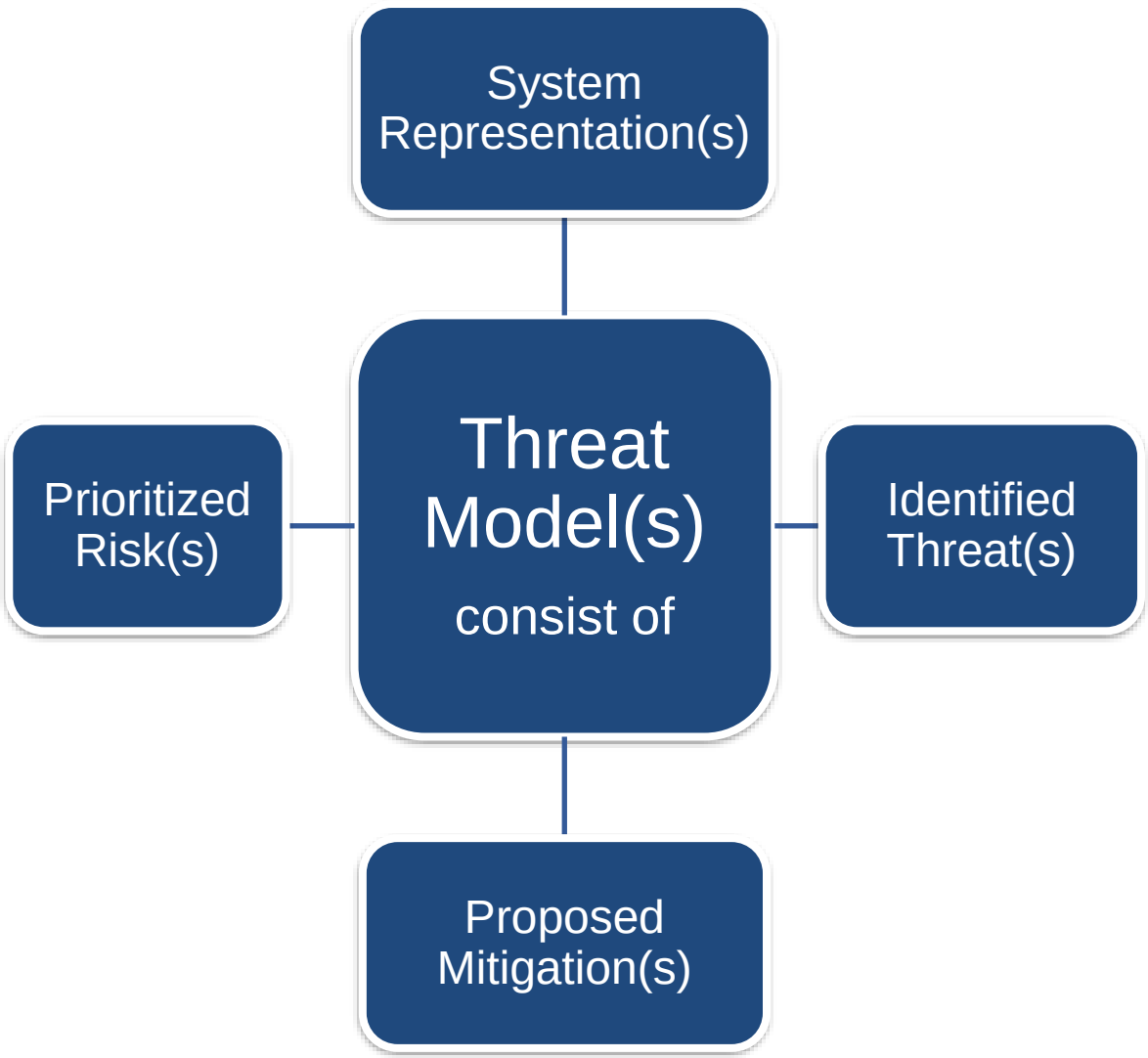
What is Threat Modeling? (continued)

Threat Modeling

Analyzing representations of a system to highlight concerns about security and privacy characteristics*

* **Threat Modeling Manifesto**, 2020 – https://threatmodelingmanifesto.org/

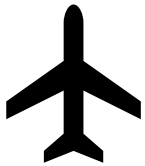
What is Threat Modeling? (continued)



Threat models all around us …

System / situation:

Catching a flight



What could go wrong?

Miss the flight

Miss boarding

Delays

Cancelled

Mitigations?

Set alarm

Leave early

Bring a book

Reschedule

Anything else to help?

Ticket ready

Prepare luggage

A Threat Modeling Mindset is …

Strategic

Asking: "what if",
"what could go wrong"

A Threat Modeling Mindset?

*"Threat modeling is the use of abstractions to aid in thinking about risks. […] Threat modeling is the key to a focused defense. Without threat models, you can never stop playing whack-a-mole."**

(* Threat Modeling: Designing for Security (2014) by Adam Shostack)

A Threat Modeling Mindset?

*"Threat modeling is the use of abstractions to aid in thinking about risks. […] Threat modeling is the key to a focused defense. Without threat models, you can never stop playing whack-a-mole."**

(* Threat Modeling: Designing for Security (2014) by Adam Shostack)

A Threat Modeling Mindset is …

Strategic

Asking: "what if", "what could go wrong"

"focused defense"

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	Opening in system helps Threat Agent realize Threat
Control	Mitigation / Countermeasure used to counter or minimize the Threat
Attack	Motivated and sufficiently skilled Threat Agent takes advantage of Vulnerability
Risk	Potential for loss, damage, destruction of Asset from Threat using Vulnerability

Approaches to Threat Modeling

Asset-centric

Software-centric

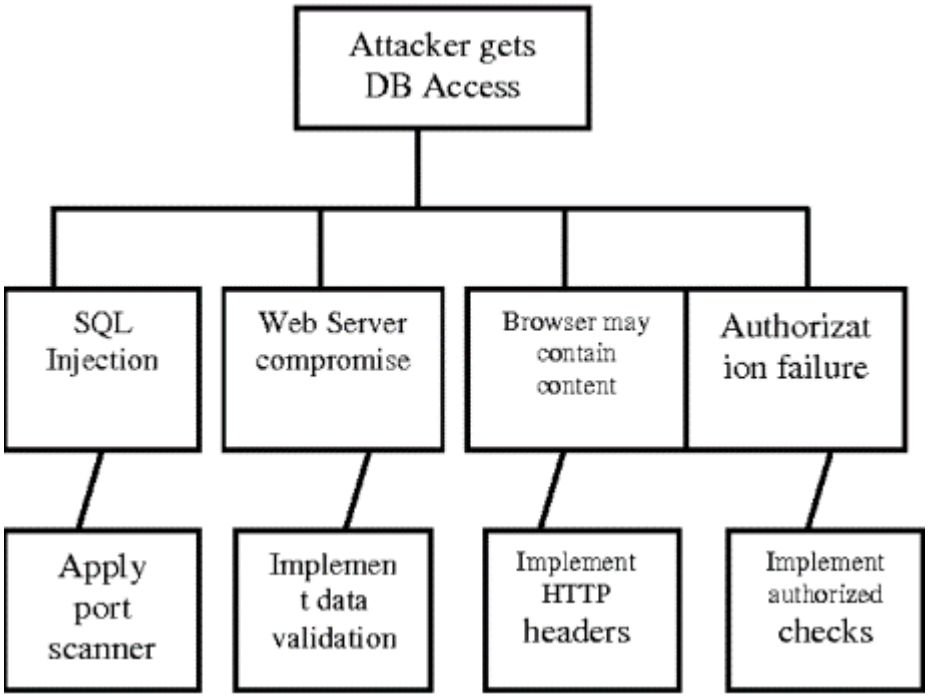
Attacker-centric

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

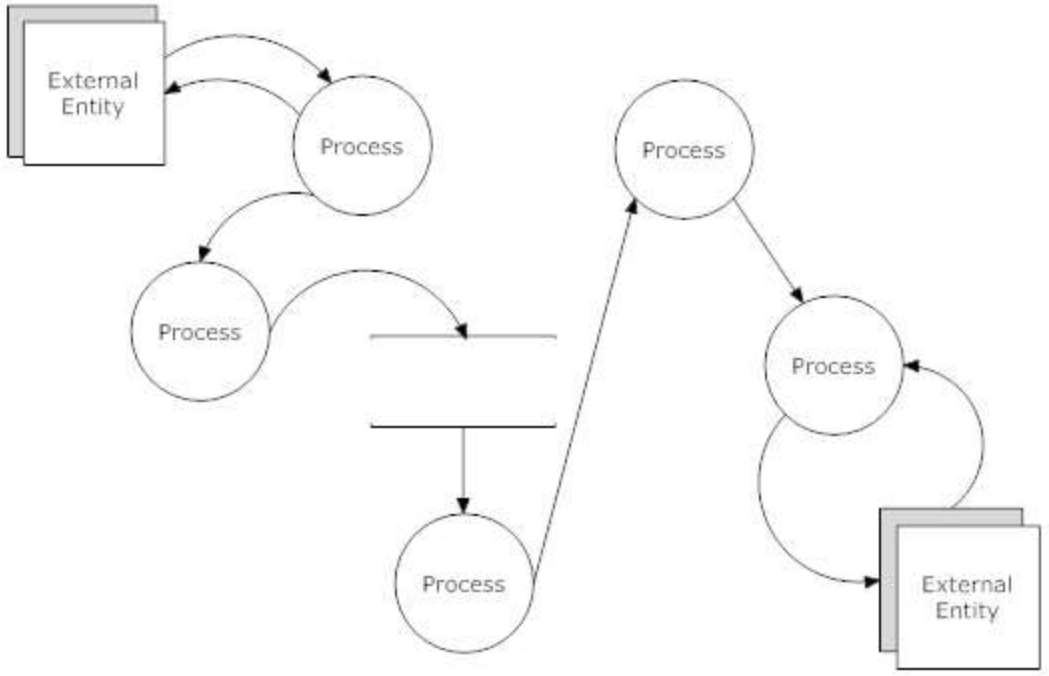


Approaches to Threat Modeling – Software-centric

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

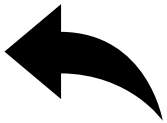
Physical features / entry points (front and back door)

Attacker-centric

Who might break in, current security system

Approaches to Threat Modeling

Asset-centric

Software-centric 

Today – we'll mainly focus on Software-centric

Attacker-centric

Threat Modeling: Getting Started

When do you do Threat Modeling?

Penetration Testing
Vulnerability Assessments
DAST/SAST Tools
Other Automated Tools

When do you do Threat Modeling? (continued)

When do you do Threat Modeling? (continued)

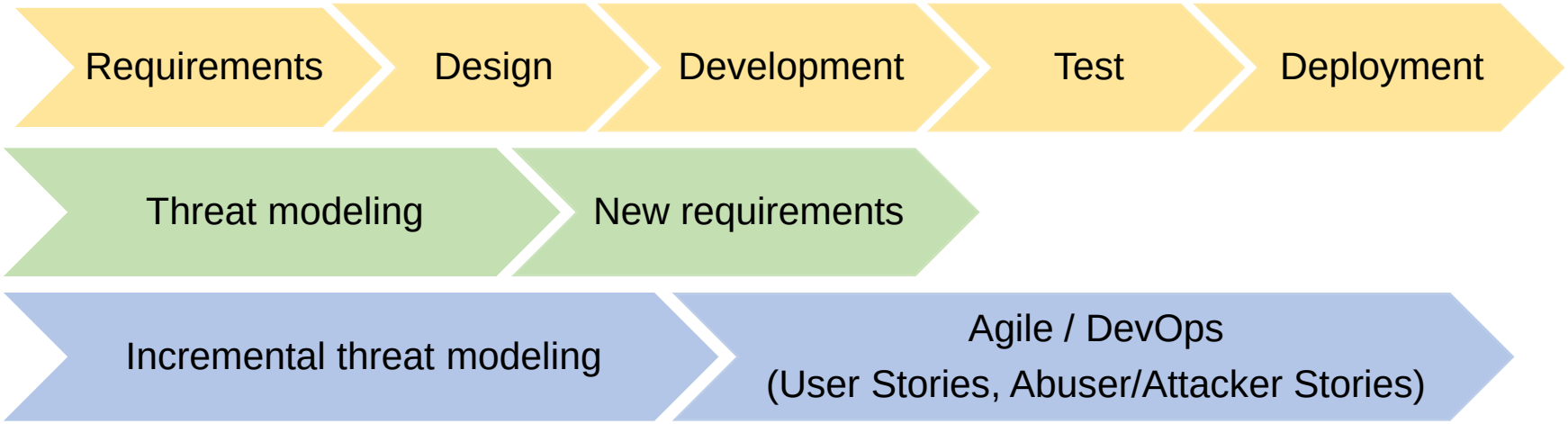
SDLC* Process

Secure SDLC* Process

* SDLC = Software Development Life Cycle

When do you do Threat Modeling? (continued)

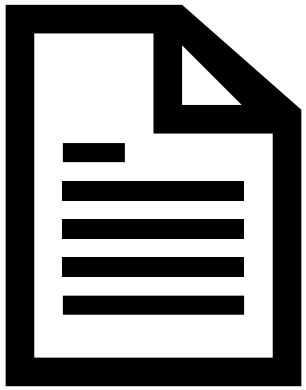
In SDLC* – Requirements and Design phase(s):



* SDLC = Software Development Life Cycle

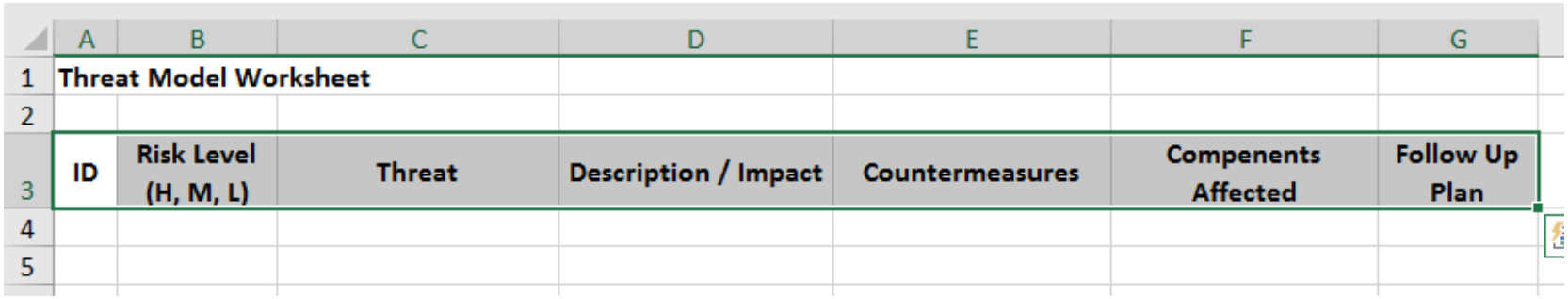
Getting Started - Simple Tools

Diagramming
(Whiteboard -
Real or Virtual)



Documenting
(Word / Excel)
(Confluence / Jira)

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**	**Compenents Affected**	**Follow Up Plan**
4							
5							

Threat Modeling Process

Threat Modeling Process

At the highest levels, when we threat model, we ask four key questions*:

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

* **Threat Modeling Manifesto**, 2020 – https://threatmodelingmanifesto.org/

Threat Modeling Process

1. *What are we working on?*
   Understand / diagram your system

2. *What could go wrong?*
   Identify threats through answers to questions

3. *What are we going to do about it?*
   Determine mitigations and risks

4. *Did we do a good enough job?*
   Review and follow through

Threat Modeling Process

1. *What are we working on?*
   Understand / diagram your system

2. *What could go wrong?*
   Identify threats through answers to questions

3. *What are we going to do about it?*
   Determine mitigations and risks

4. *Did we do a good enough job?*
   Review and follow through

Threat Modeling Process

1. *What are we working on?*
   Understand / diagram your system

2. *What could go wrong?*
   Identify threats through answers to questions

3. *What are we going to do about it?*
   Determine mitigations and risks

4. *Did we do a good enough job?*
   Review and follow through

1. Understand / diagram your system

Gather Team
Domain Knowledge
Business / Technical Goals
Focused Sessions

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

Be sure to document what you learn!

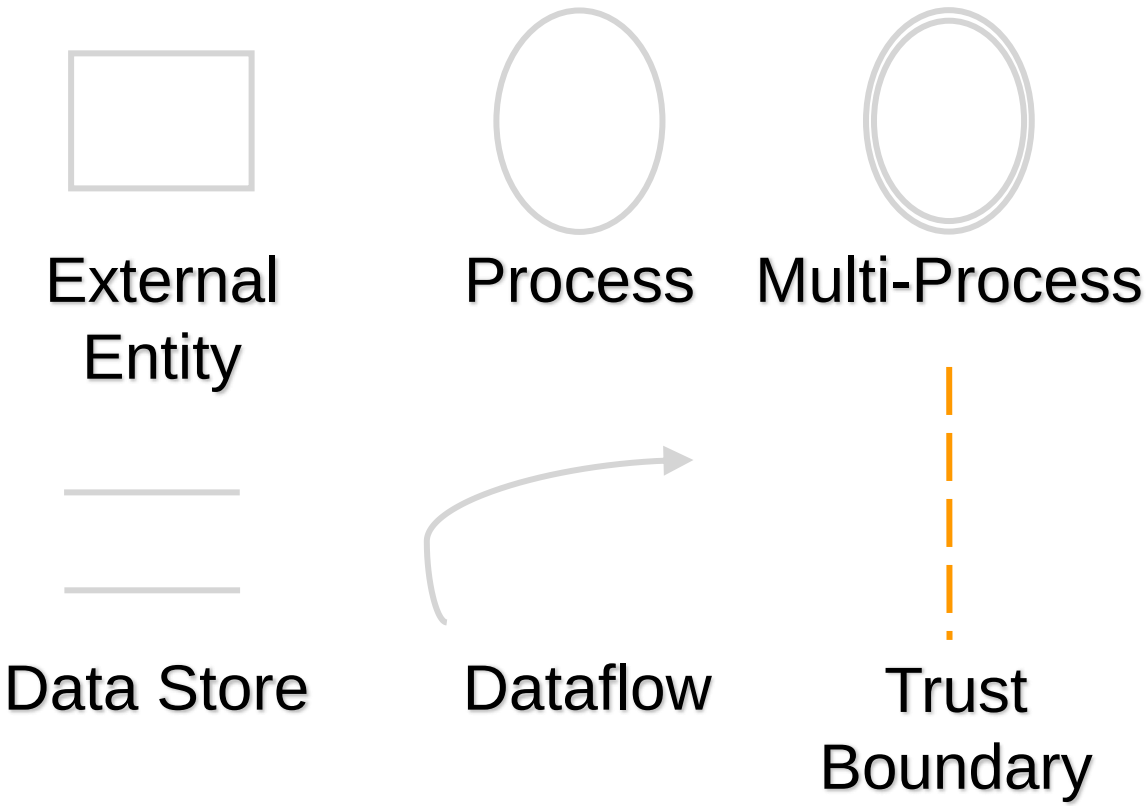
1. Understand / diagram your system

You can use an Architecture or Network diagram

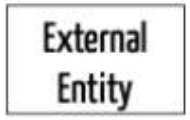
In many cases, a Data Flow Diagram (DFD) is very useful for Threat Modeling

1. Understand / diagram your system

DFD – Data Flow Diagrams (MS SDL)



Draw a Data Flow Diagram (DFD)

Notation element	Reference	Examples
	External entity	People (e.g., users), systems (e.g., other devices), cloud services, browsers
	Process	DDL, exe(D)COM, web service, virtual machine, threat
	Data store	File, database, registry, cache, cookie
	Data flow	http request or response, remote procedure call, UDP communication
	Trust boundary (inside you trust the processes and data stores, outside you don't)	Device boundary, process boundary

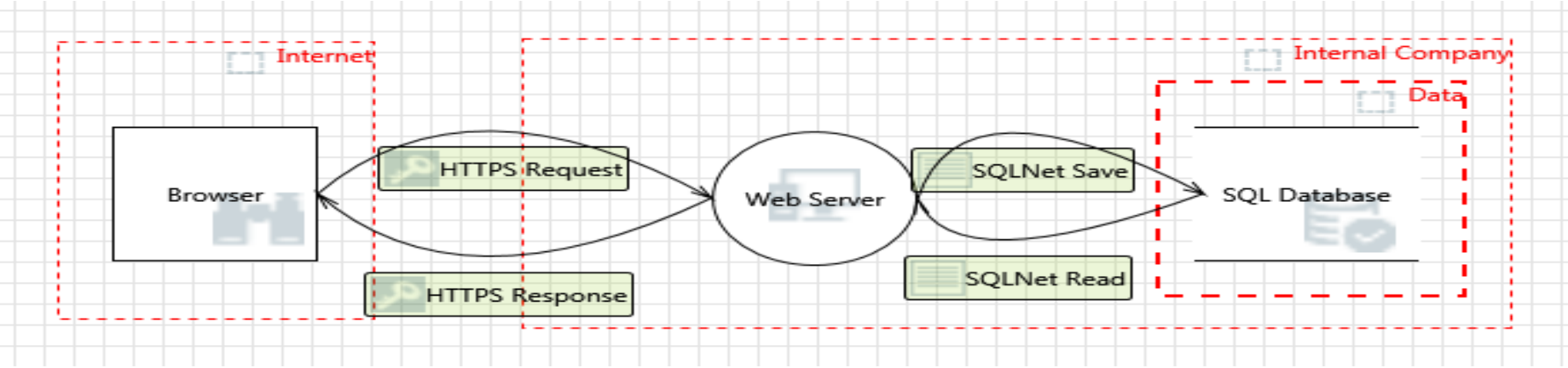
You can use drawing tool of choice – however, try to stay with the basic shapes and meanings for consistency

1. Understand / diagram your system

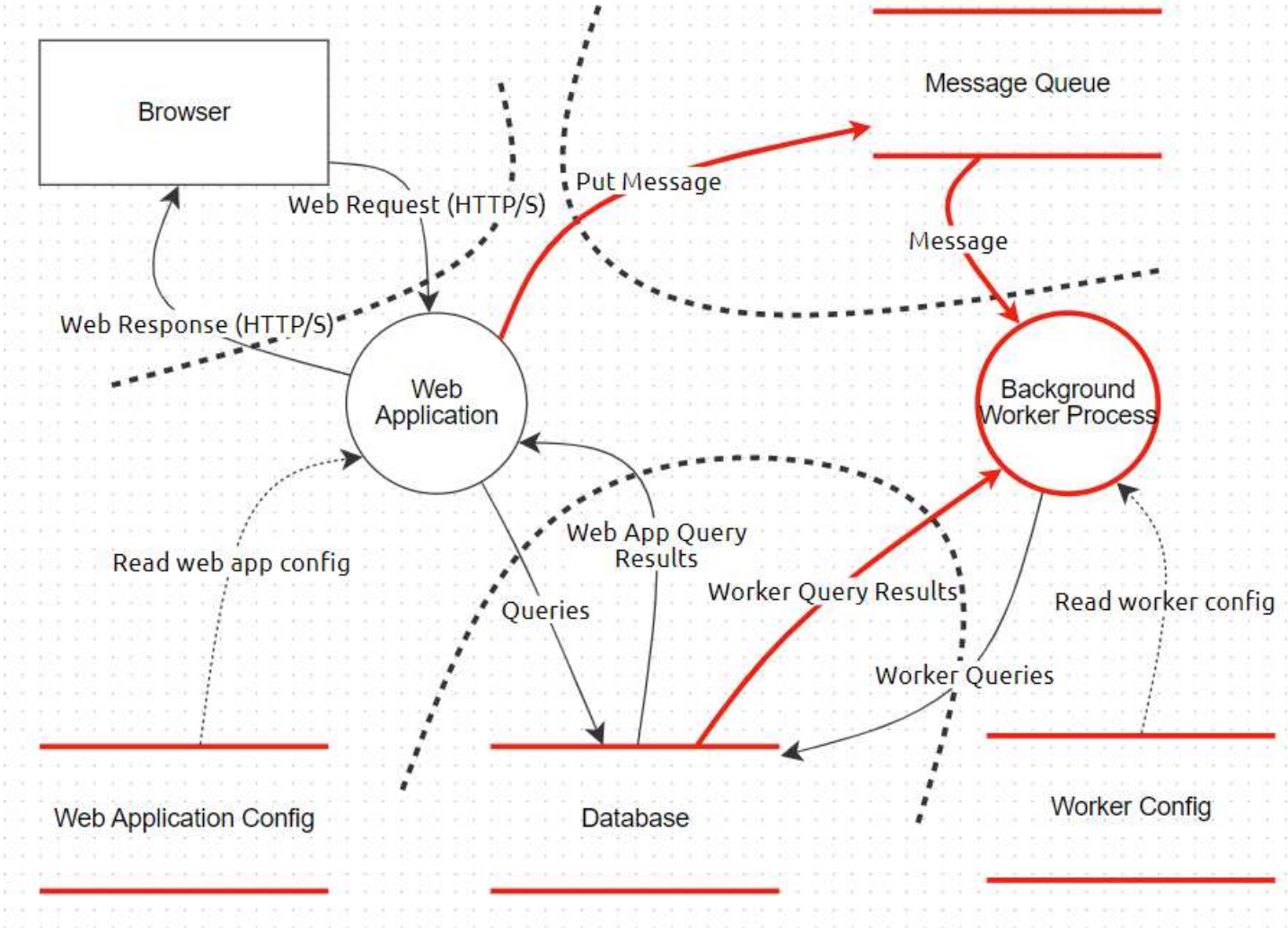
How do the External Entities, Processes, and Data Stores connect? Connect the information points with the Data Flow arrows.

Where are the Trust Boundaries?
For example:

- Browser (external entity) sends / receives data (data flow) with a web server / app (process) which saves / reads data (data flow) using a SQL Database (data store)
- Trust Boundaries indicate where trust changes — Authenticate / Authorize / Validate



Example Data Flow Diagram (DFD)



(Sample DFD created with OWASP Threat Dragon 2.0)

Threat Modeling Process

1. *What are we working on?*
   Understand / diagram your system

2. *What could go wrong?*
   Identify threats through answers to questions

3. *What are we going to do about it?*
   Determine mitigations and risks

4. *Did we do a good enough job?*
   Review and follow through

2. Identify Threats – “What can go wrong?”

Conspicuously overloaded truck stopped by State Police - Springfield, MA

“Please remember, when traveling with a load in a vehicle, take a look at it and before taking to the roads, ask yourself, ‘**What could go wrong?**’ “ (Boston Globe, June 21, 2018)

2. Identify threats – Mental Model

If a “threat actor” can acquire an “asset”
by abusing / bypassing a “control”,
you have a “threat”.

“A simple mental model for Threat Modeling” (3/13/2023) by Aditya Patel
https://www.secwale.com/p/threatmodeling

2. Identify Threats - STRIDE

Threat	Examples	Control we want
Spoofing	Pretending to be someone else	Identity Assurance
Tampering	Modifying data that should not be modifiable	Integrity
Repudiation (lack of proof)	Claiming someone didn't do something	Non-repudiation (proof – Auditability)
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

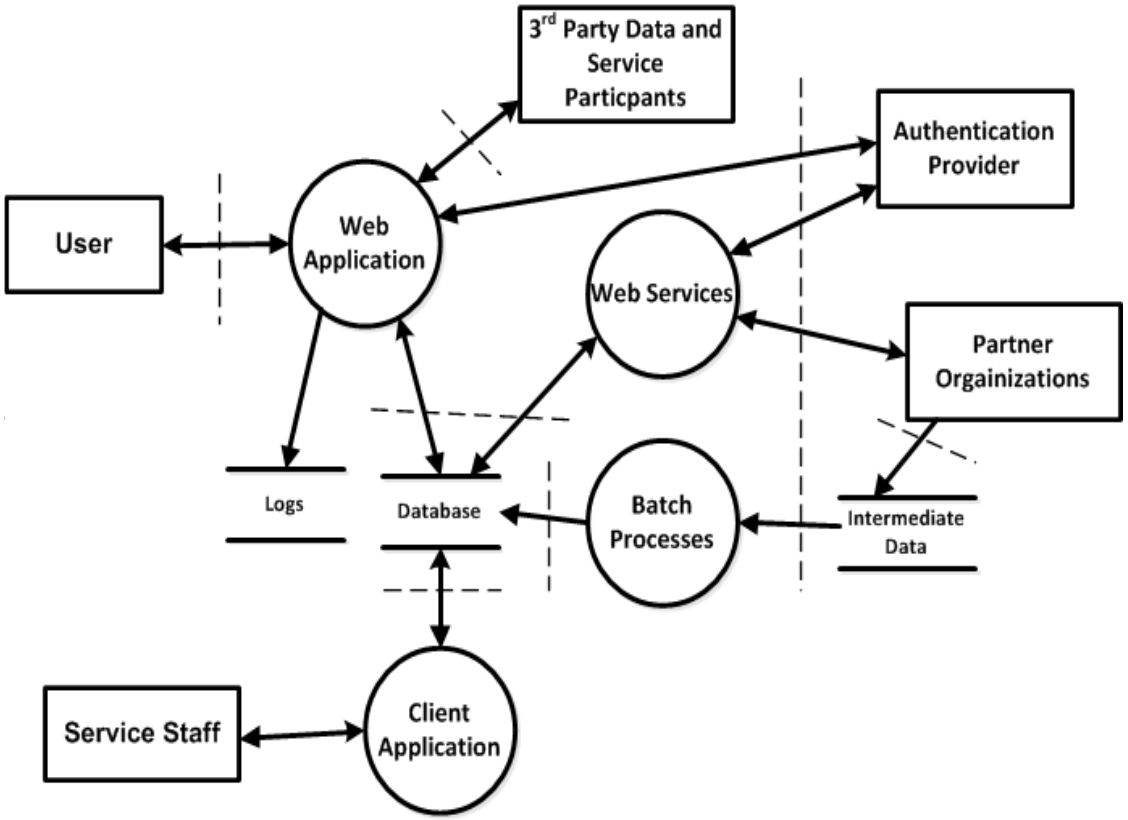
2. Identify Threats – Applying STRIDE to a DFD

Options:

Each part of STRIDE applies to specific elements or interactions

and/or

You can look at STRIDE per interaction.

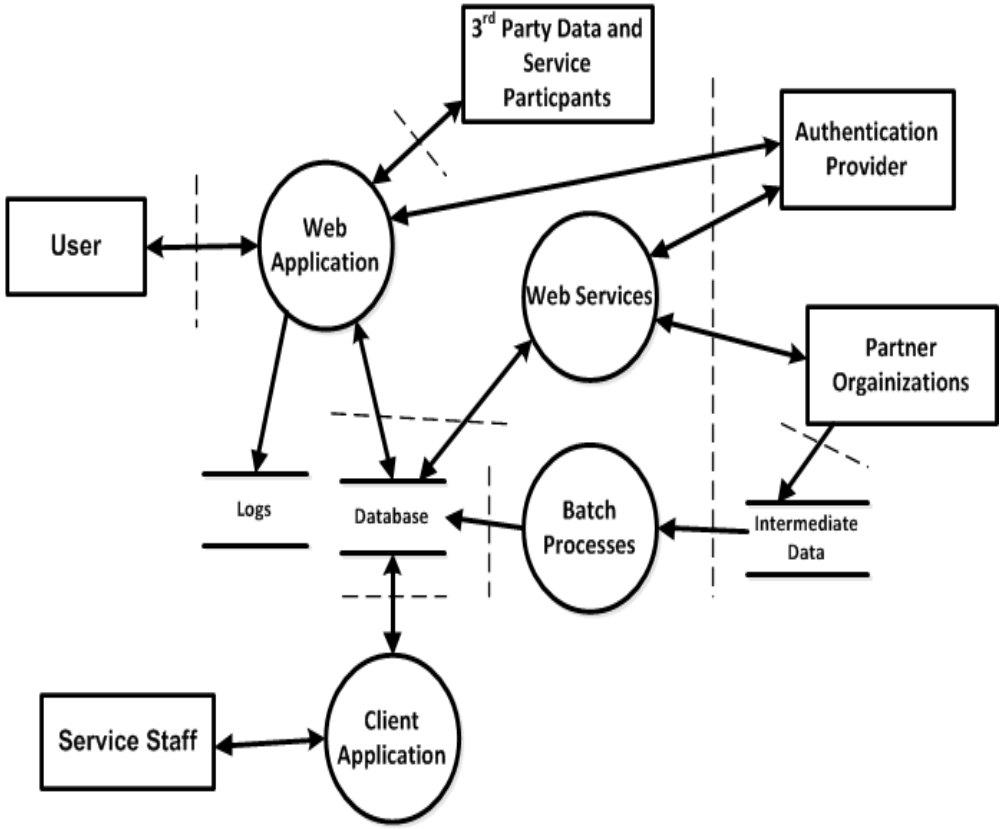


Using STRIDE to Identify Threats

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?

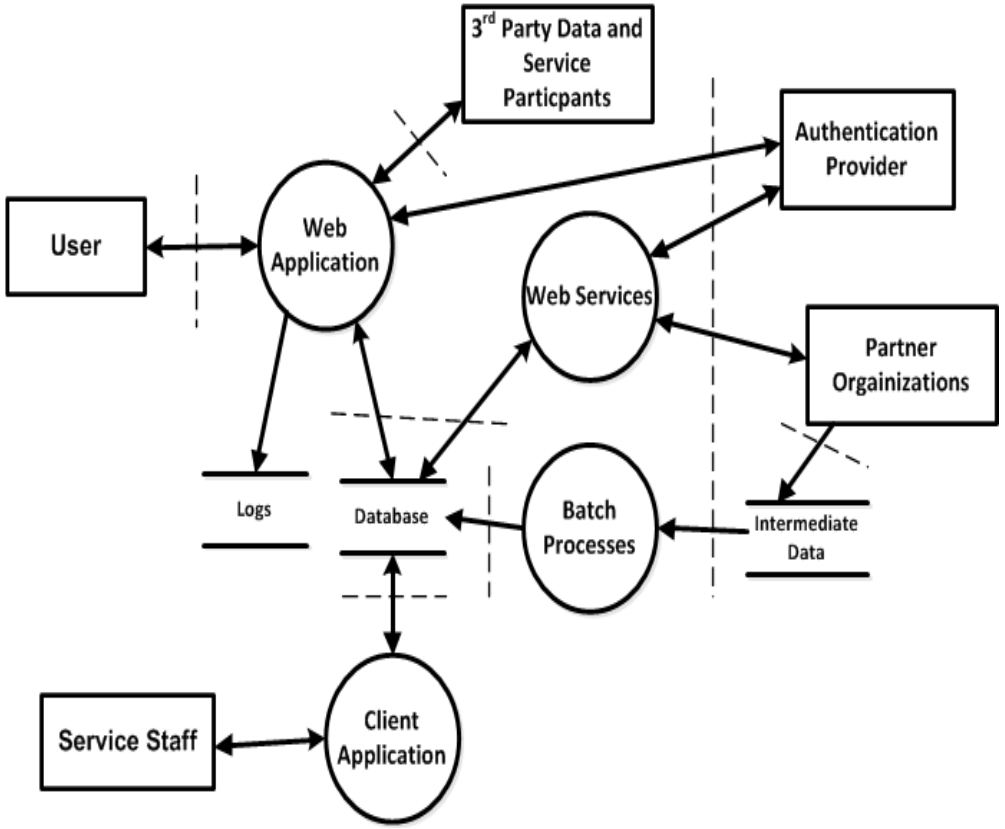


Using STRIDE to Identify Threats

Information Disclosure
Setting and getting credentials could be exposed in transit

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

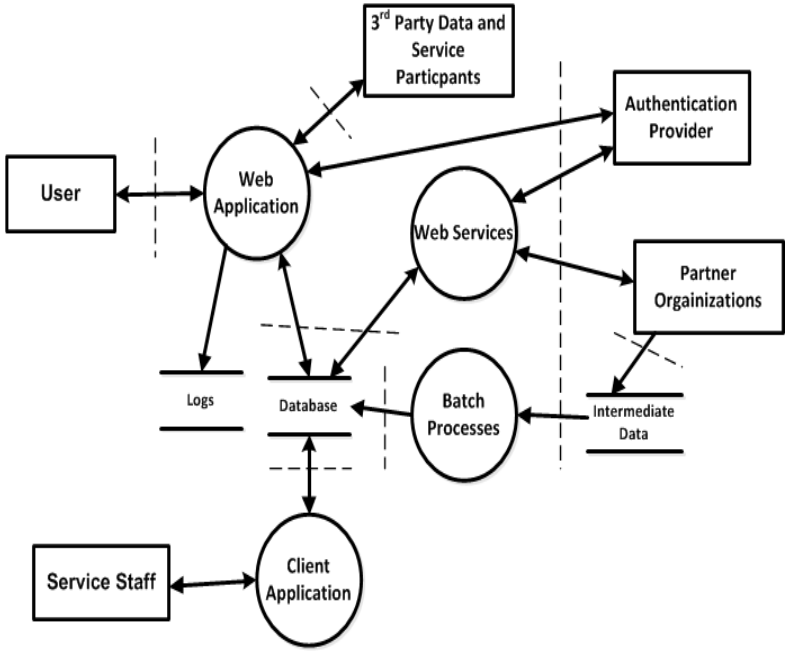
Elevation of Privilege
Does audit data have access control for reading?



2. Identify Threats – Applying STRIDE to a DFD

Threat Model for ACME Web Application

Threat	STRIDE	
Partner Organization communication to Web Services may be compromised	Tampering, Information Disclosure	
Logs for Web Application may be tampered with	Tampering, Repudiation	



2. Identify threats – Many Ways

- STRIDE (software-centric)
- LINDDUN (privacy-focused)
- Attack Trees (asset or attacker-centric)
- PASTA (risk-centric)
- MITRE ATT&CK (intrusion-centric knowledge base)

Other:

- Card Games - OWASP Cornucopia, Elevation of Privilege
- Use Cases / Abuse Cases

Threat Modeling Process

1. *What are we working on?*
   Understand / diagram your system

2. *What could go wrong?*
   Identify threats through answers to questions

3. *What are we going to do about it?*
   Determine mitigations and risks

4. *Did we do a good enough job?*
   Review and follow through

3. 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

3. Determine mitigations and risks

Mitigation Options:

- Leave as-is
- Remove from product
- Remedy with technology countermeasure
- Warn user

Make the mitigations / countermeasures part of your Security acceptance criteria

3. Determine mitigations and risks

What is the risk associated with the vulnerability and threat identified?

Risk is product of two factors:

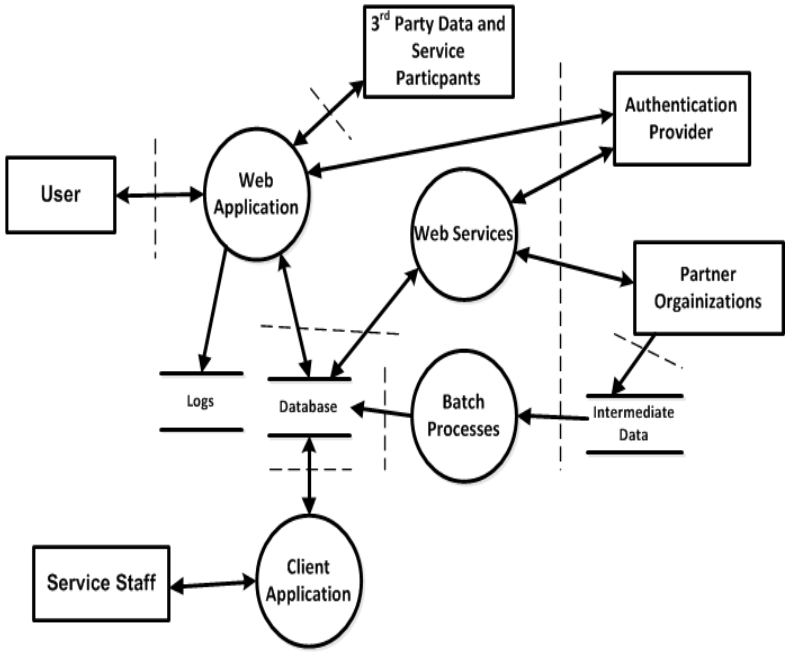
- Ease of exploitation
- Business impact

At a bare minimum, use Risk Rating where overall risk of a threat expressed in High, Medium, or Low

3. Determine mitigations and risks

Threat Model for ACME Web Application:

Threat	STRIDE	Mitigation / Risk
Partner Organization communication to Web Services may be compromised	Tampering, Information Disclosure	Implement encryption (HTTPS TLS 1.2+) and validation of message integrity (High)
Logs for Web Application may be tampered with	Tampering, Repudiation	Apply access control on logs, send logs to centralized server (Medium)



Threat Modeling Process

1. *What are we working on?*
   Understand / diagram your system

2. *What could go wrong?*
   Identify threats through answers to questions

3. *What are we going to do about it?*
   Determine mitigations and risks

4. *Did we do a good enough job?*
   Review and follow through

4. Review and follow through

Document findings and decisions

File bugs or new requirements (as stories)

Verify bugs fixed / new requirements (stories) implemented

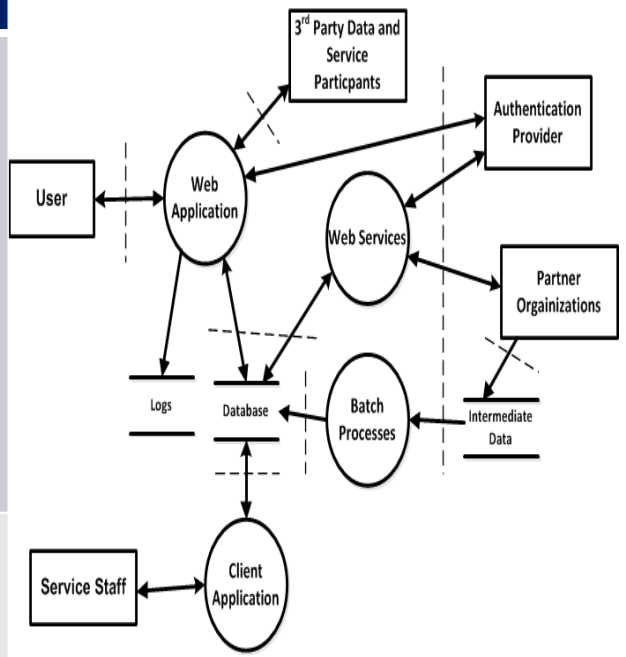
Did we miss anything? Review again

Anything new? Review again

4. Review and follow through

Threat Model for ACME Web Application

Threat	STRIDE	Mitigation / Risk	Review / Action Items
Partner Organization communication to Web Services may be compromised	Tampering, Information Disclosure	Implement encryption (HTTPS TLS 1.2+) and validation of message integrity (High)	Address issue in next Sprint
Logs for Web Application may be tampered with	Tampering, Repudiation	Apply access control on logs, send logs to centralized server (Medium)	Evaluate if will fix in next Sprint or future Sprint



Repeat or iterate as needed

- Consider a baseline threat model of your project if you have never, ever created a threat model before

- Then, update and/or review your threat model as you continue to add new features

A Threat Modeling Mindset is …

Strategic

Asking: "what if", "what could go wrong"

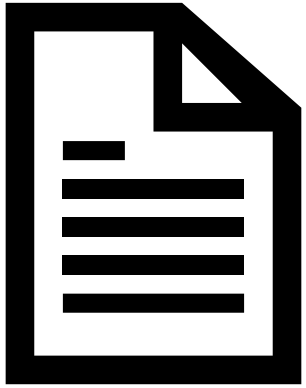
"focused defense"

"review / follow through"

Threat Modeling Process Tools

Threat Modeling Process - Simple Tools

Diagramming
(Whiteboard -
Real or Virtual)



Documenting
(Word / Excel)
(Confluence / Jira)

Threat Modeling Process - Tools

Tool	Cost	Platforms
Microsoft Threat Modeling Tool	Free	Desktop, Windows OS Install only
Threats Manager Studio	Free	Desktop, Windows OS Install only
ThreatModeler	Paid	Web-based, In-house or Cloud, CI/CD integration
IriusRisk	Paid	Web-based, In-house or Cloud, CI/CD integration
SD Elements	Paid	Web-based, In-house or Cloud
OWASP Threat Dragon	Free	Web-based, Windows, Mac, Linux installs
Drawing tools – Draw.IO, Mural, Miro, etc.	Free-*ish*	Web-based, Windows, Mac, Linux installs

What next?

What next?

Learn more about:

- Privacy Threat Modeling
  - LINDDUN (https://www.linddun.org/)
- Attack Trees
  - Bruce Schneier's 1999 article
- Incremental Threat Modeling
  - Agile approaches – Irene Michlin (@IreneMichlin)
- MITRE ATT&CK / D3FEND
  - https://d3fend.mitre.org/
  - https://d3fend.mitre.org/

Key Takeaways

Pursue a Threat Modeling Mindset:

- Be strategic: think of secure design before new features
- Ask “what if” / “what could go wrong” questions
- Focus on where defenses may fail
- Review / follow through (and repeat) as needed

Resources – Threat Modeling Manifesto

"Threat Modeling Manifesto" (2020)

https://threatmodelingmanifesto.org/

- Definition
- Values
- Principles
- Anti-Patterns

Resources – Threat Modeling Connect

Threat Modeling Connect (started Fall, 2022)

https://www.threatmodelingconnect.com/

- Support and insights from other Threat Modelers
- Monthly Community Meetups
- Threat Modeling Hackathons
- Threat Modeling Open Forum
- First Threat Modeling Conference – November, 2023

Resources - Books

Threat Modeling as a Practice:

Threat Modeling: A Practical Guide for Development Teams (2020)
Izar Tarandach and Matthew Coles

Threat Modeling: Designing for Security (2014)
and
Threats: What Every Engineer Should Learn from Star Wars (2023)
Adam Shostack

Securing Systems: Applied Architecture and Threat Models (2015)
Brook S.E. Schoenfield

Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis (2015)
Marco Morana and Tony UcedaVelez

Resources - Books

Applied Threat Modeling:

Hacking Kubernetes: Threat-Driven Analysis and Defense (2021)
Andrew Martin, Michael Hausenblas

Playbook for Threat Modeling Medical Devices (2021)
MITRE: https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf

Resources - Tools

Microsoft Threat Modeling Tool

https://aka.ms/threatmodelingtool

ThreatModeler – Web Based (in-house) Tool

https://threatmodeler.com

IriusRisk Software Risk Manager

https://iriusrisk.com

OWASP Threat Dragon

https://owasp.org/www-project-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

Upcoming Local Events

OWASP Boston Application Security Conference (BASC) 2023
at
Microsoft Offices, Burlington, MA (4/1) – **FREE**

- https://www.basconf.org/
- Topics: Defense-in-depth, Open Source Software, Cloud Native Apps, JavaScript Security, ***Threat Modeling and Agile/DevOps***, OWASP ZAP, Security Vulnerabilities, GraphQL, Mobile App Security

Questions?

Slides:

https://roberthurlbut.com/r/NHCS2023

@RobertHurlbut

Thank you!