Developing a Threat Modeling Mindset

Boston Code Camp 38
March 29, 2025

Robert Hurlbut
RobertHurlbut.com

#boscc
Boston
Code Camp

Boston Code Camp 38 *Thanks to our Sponsors!*

Microsoft

Platinum

MILL5

PULSAR SECURITY

Gold

slalom

Progress Telerik

Silver

Duende.

Bronze

In-Kind Donations

CALL FOR PAPERS POWERED BY sessionize

#boscc
Boston
Code Camp

Who am I?

X (*Twitter*): @RobertHurlbut
BlueSky: roberthurlbut.bsky.social
LinkedIn: roberthurlbut
Discord: robert.ct (robertct)

Robert Hurlbut

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

- **Microsoft MVP – Dev Sec / Dev Tech**
- **(ISC2) CSSLP**
- **Boston Code Camp – Co-Organizer**
- **Boston .NET Architecture Group – Founder / Leader**
- **Amherst Security Group – Leader**
- **Application Security Podcast – Co-Host**
- **"Threat Modeling Manifesto" – Co-Author**
- **"Threat Modeling Capabilities" – Co-Author**
- **Threat Modeling Connect – Co-Founding Member**
- **Expert Witness (Threat Modeling, Cybersecurity)**
- **Ph.D. Student – Space Cybersecurity**

Threat Modeling can be traced back to military strategy in the mid-20th century*

- Who is the enemy?
- What are their motives?
- What are their methods?
- Let's plan our strategy/defense

* "A Short History of Threat Modeling", Jason Nelson, February 2025.
See https://www.necessarysecurityllc.com/post/a-short-history-of-threat-modeling

A Threat Modeling Mindset?

#boscc
Boston
Code Camp

*"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?

#boscc
Boston
Code Camp

*"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 …

#boscc
Boston
Code Camp

Strategic vs Reactive
("thinking ahead" vs.
"hope we are safe")

What is Threat Modeling?

#boscc
Boston
Code Camp

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)

#boscc
Boston
Code Camp

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)

#boscc
Boston
Code Camp

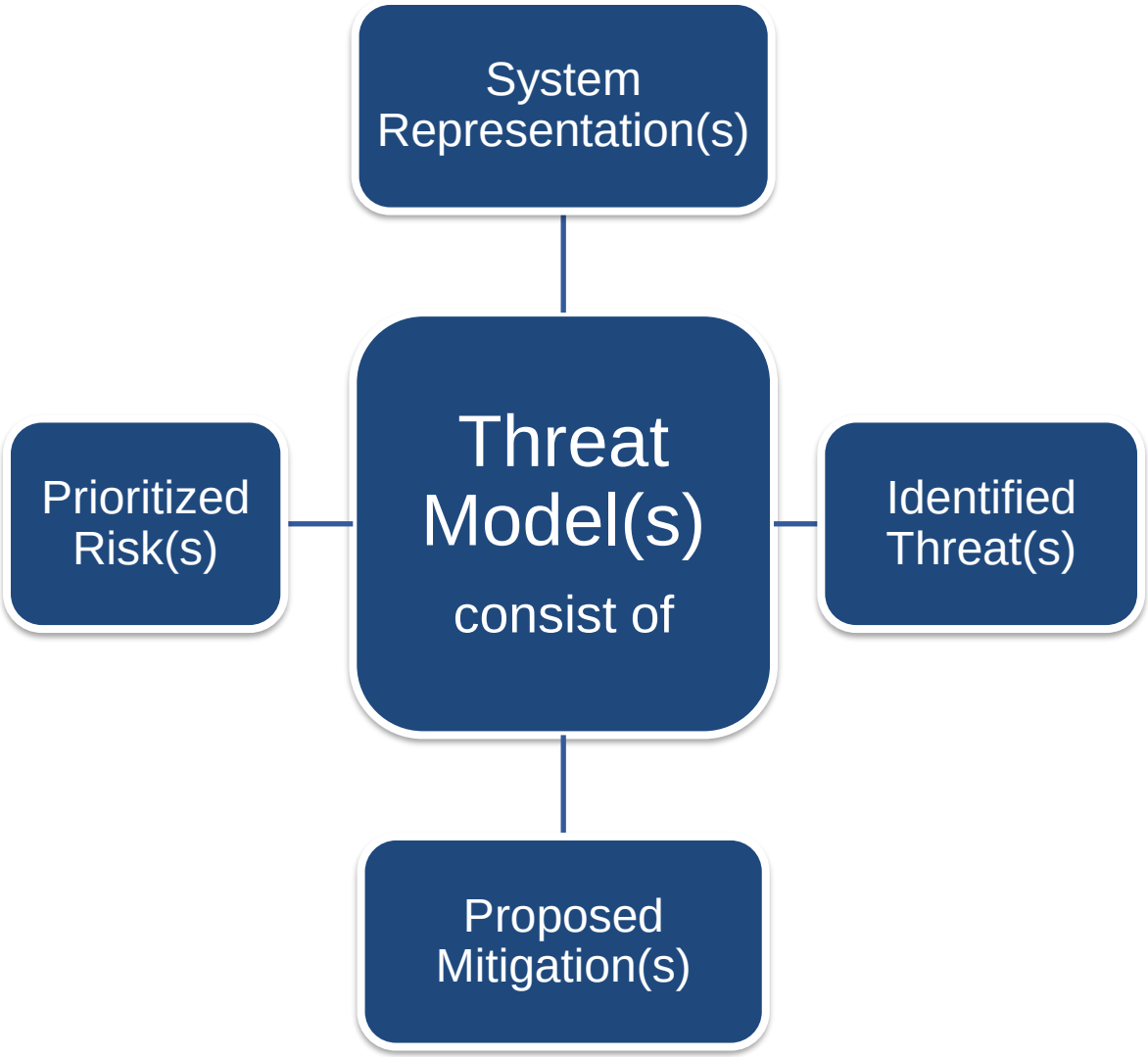
Threat Modeling

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)

#boscc Boston Code Camp

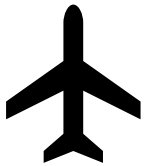


Threat models all around us …

#boscc Boston Code Camp

System / situation:

Catching a flight



What could go wrong?

Miss the flight

Miss boarding

Delays

Cancelled

Mitigations?

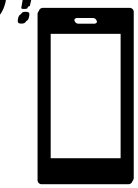
Set alarm

Leave early

Bring a book

Reschedule

Anything else to help?



Ticket ready

Prepare luggage

#boscc
Boston
Code Camp

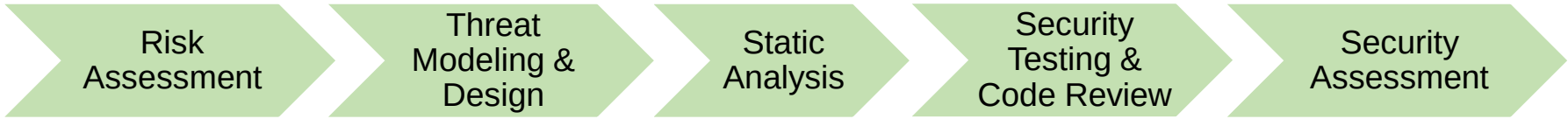
Threat Modeling: Getting Started

When do you do Threat Modeling?

#boscc Boston Code Camp

SDLC* Process

Secure SDLC* Process

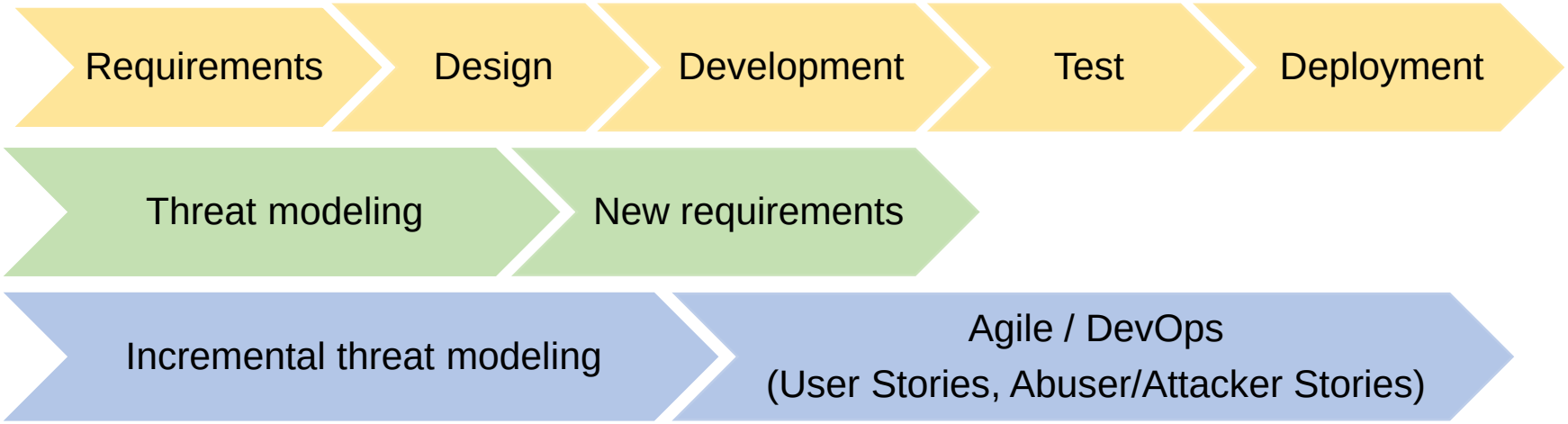


* SDLC = Software Development Life Cycle

When do you do Threat Modeling? (continued)

#boscc Boston Code Camp

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

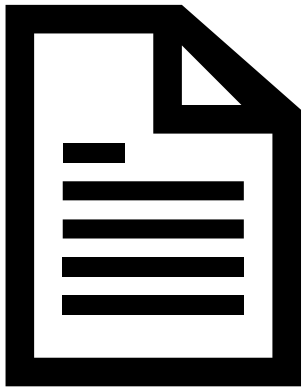


* SDLC = Software Development Life Cycle

Getting Started - Simple Tools

#boscc
Boston
Code Camp

Diagramming
(Whiteboard -
Real or Virtual)



Documenting
(Word / Excel)
(Confluence / Jira)

Threat Model Sample Worksheet

#boscc
Boston
Code Camp

	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							

#boscc
Boston
Code Camp

Threat Modeling Process

A Threat Modeling Mindset is …

#boscc
Boston
Code Camp

Strategic

Threat Modeling Process

#boscc Boston Code Camp

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

#boscc Boston Code Camp

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

#boscc Boston Code Camp

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

#boscc
Boston
Code Camp

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

#boscc
Boston
Code Camp

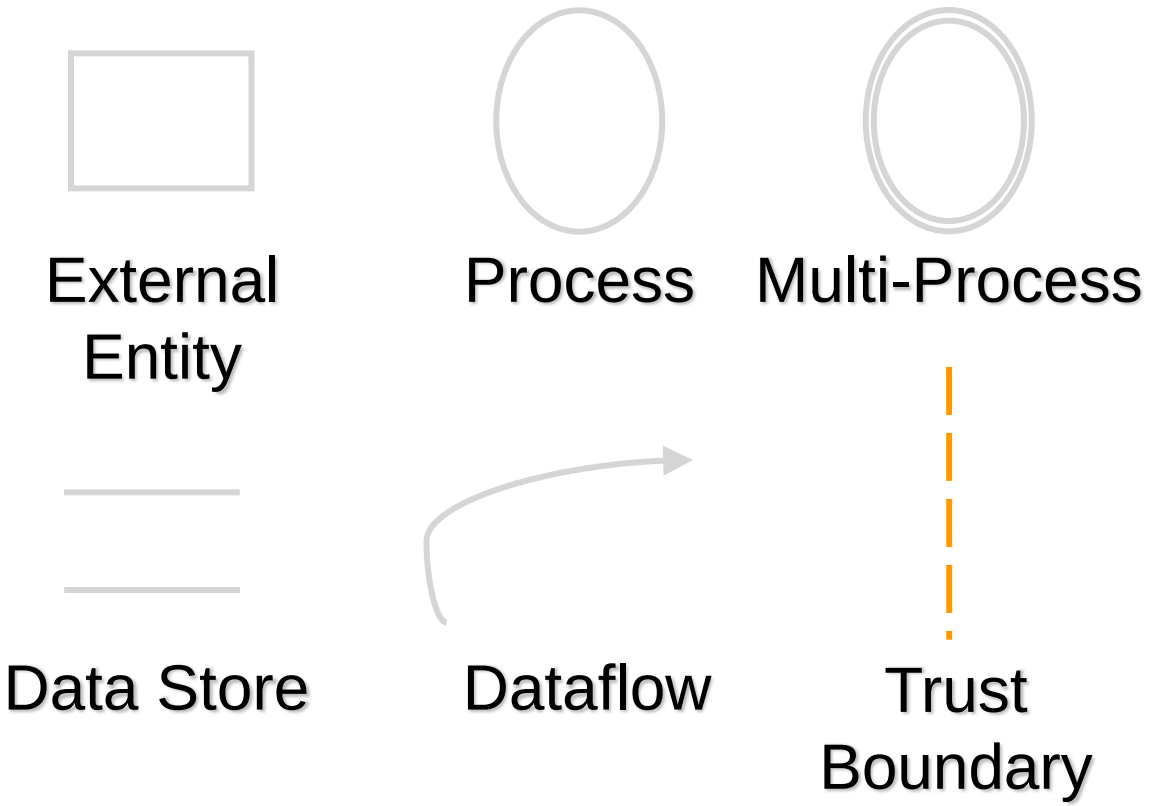
You can use an Architecture or Network diagram

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

1. Understand / diagram your system

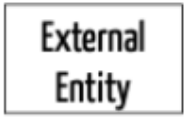
#boscc Boston Code Camp

DFD – Data Flow Diagrams (MS SDL)



Draw a Data Flow Diagram (DFD)

#boscc Boston Code Camp

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

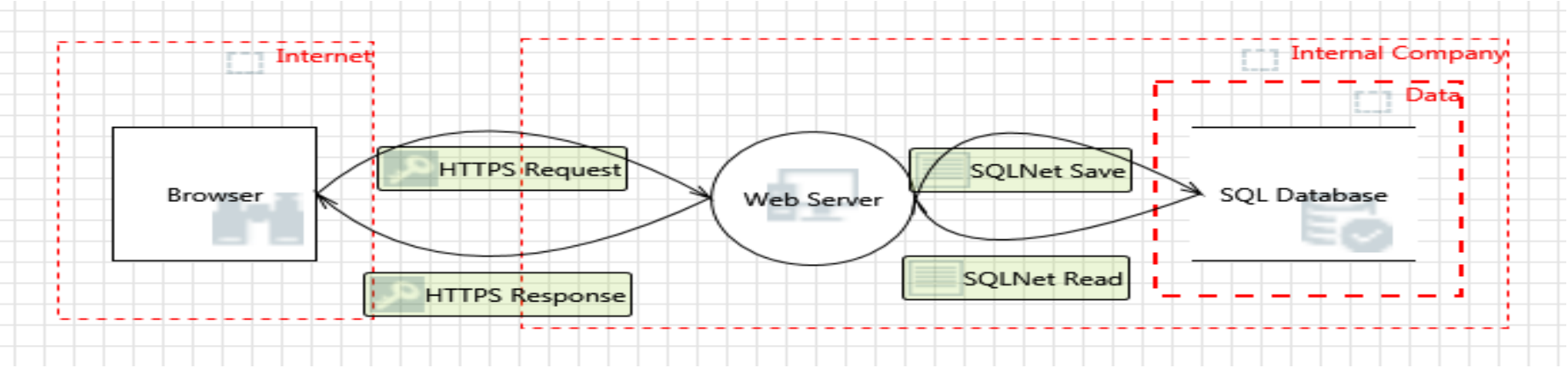
1. Understand / diagram your system

#boscc Boston Code Camp

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

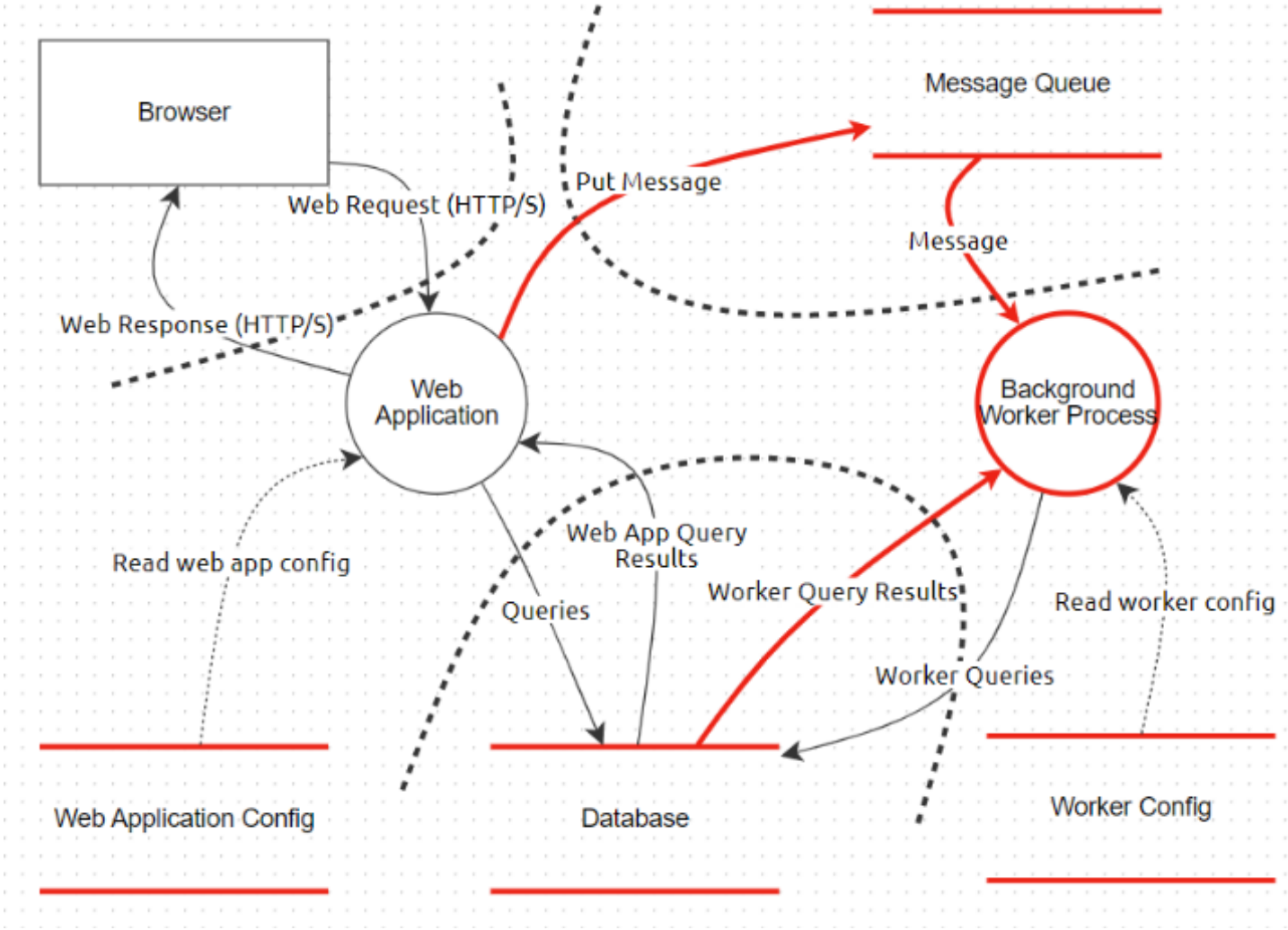
Where are the Trust Boundaries?
For example:

- 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)

#boscc Boston Code Camp



(Sample DFD created with OWASP Threat Dragon 2.0)

Threat Modeling Process

#boscc Boston Code Camp

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

A Threat Modeling Mindset is …

#boscc

Strategic

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

2. Identify threats – Mental Model

#boscc
Boston
Code Camp

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

#boscc Boston

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

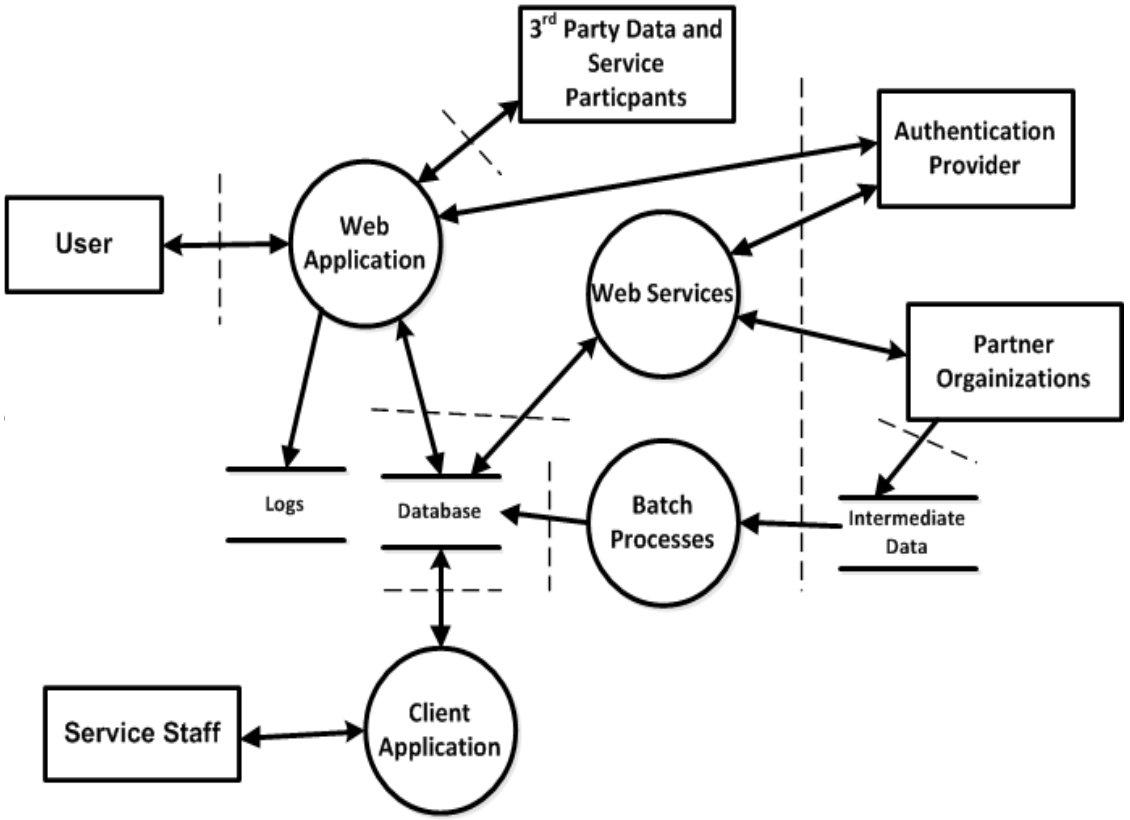
#boscc Boston Code Camp

Options:

Each part of STRIDE applies to specific elements or interactions

and/or

You can look at STRIDE per interaction.



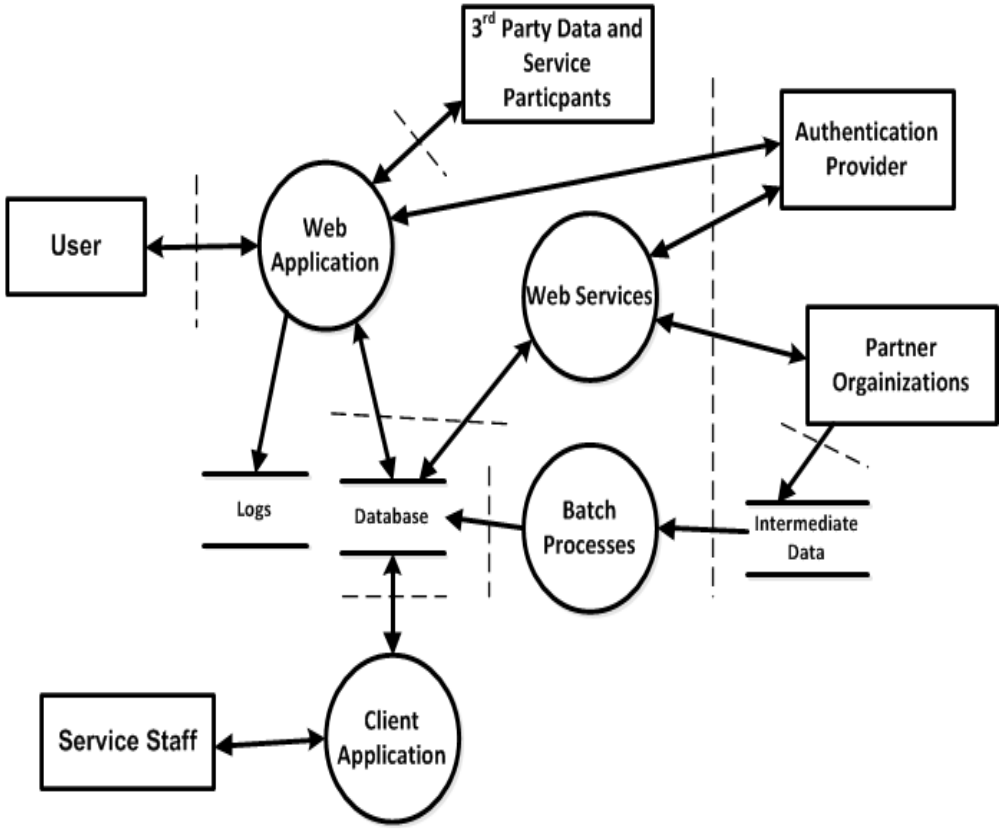
Using STRIDE to Identify Threats

#boscc
Boston
Code Camp

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?



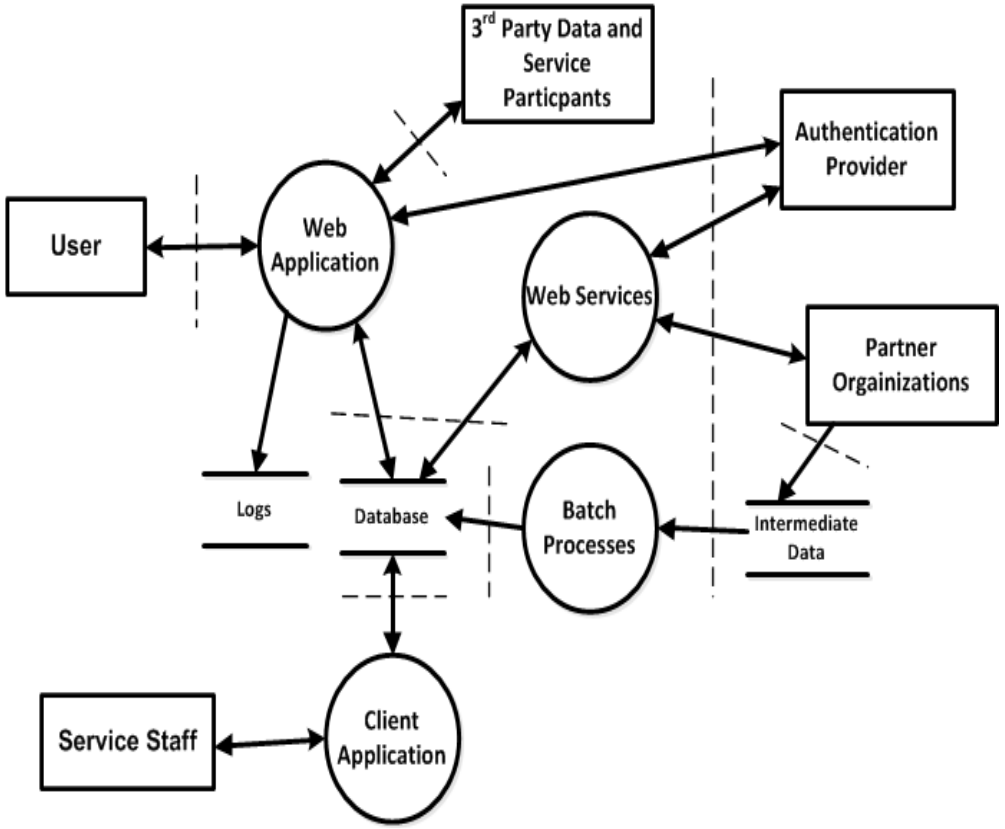
Using STRIDE to Identify Threats

#boscc
Boston
Code Camp

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?

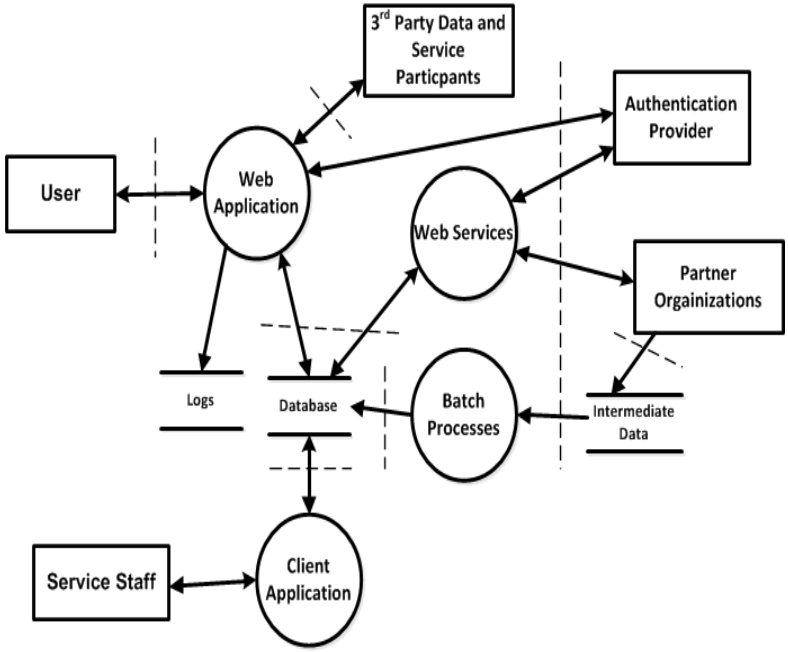


2. Identify Threats – Applying STRIDE to a DFD

#boscc Boston Code Camp

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

#boscc
Boston
Code Camp

- 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

#boscc Boston Code Camp

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

A Threat Modeling Mindset?

#boscc
Boston
Code Camp

*"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?

#boscc
Boston
Code Camp

*"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 …

#boscc

Strategic

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

"focused defense"

3. Determine mitigations and risks
Controls mapped to STRIDE

#boscc Boston Code Camp

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

#boscc Boston Code Camp

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

#boscc Boston Code Camp

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

Risk is product of two factors:

- Ease of exploitation
- Business impact

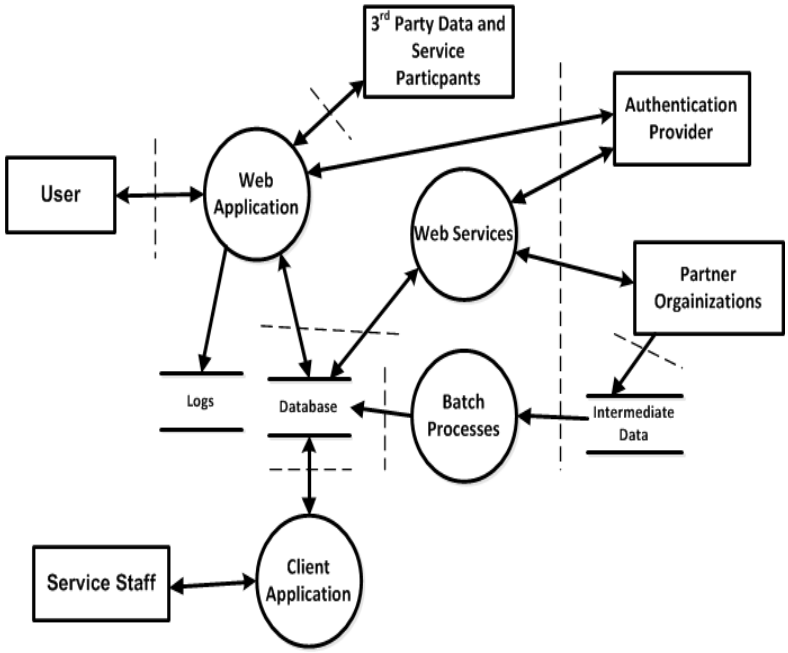
At a bare minimum, use Risk Rating where overall risk of a threat expressed in High, Medium, or Low

3. Determine mitigations and risks

#boscc Boston Code Camp

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

#boscc Boston Code Camp

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

A Threat Modeling Mindset is …

#boscc

Strategic

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

"focused defense"

"review / follow through"

4. Review and follow through

#boscc
Boston
Code Camp

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

Repeat or iterate as needed

#boscc Boston Code Camp

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

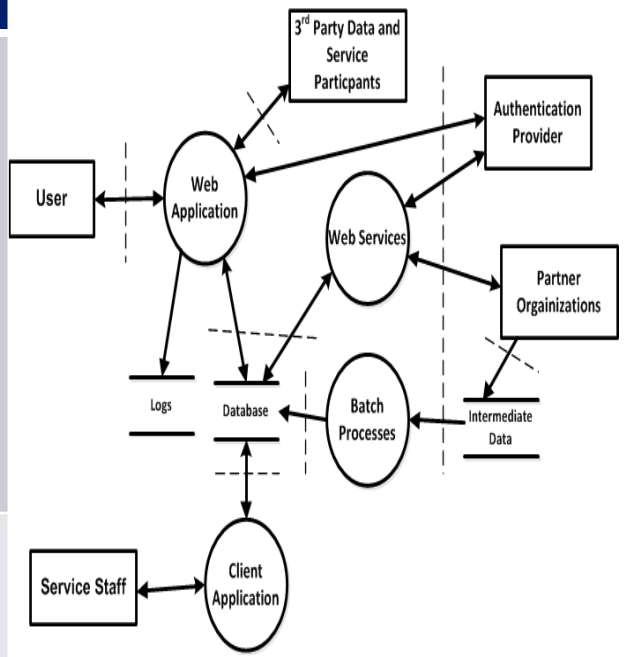
- Then, update and/or review your threat model as you continue to add new features

4. Review and follow through

#boscc Boston Code Camp

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



#boscc Boston Code Camp

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

#boscc Boston Code Camp

"Threat Modeling Manifesto" (2020)

https://threatmodelingmanifesto.org/

- Definition
- Values
- Principles
- Anti-Patterns

Resources – Threat Modeling Connect

#boscc Boston Code Camp

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
- Threat Modeling Conferences

Resources - Books

#boscc Boston Code Camp

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

#boscc Boston Code Camp

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

#boscc Boston

Tool	Cost	Platforms	Links
Microsoft Threat Modeling Tool	Free	Desktop, Windows OS Install only	*https://aka.ms/threatmodelingtool*
Threats Manager Studio	Free	Desktop, Windows OS Install only	https://threatsmanager.com/ (ending December 2025)
ThreatModeler	Paid	Web-based, In-house or Cloud, CI/CD integration	*https://threatmodeler.com*
IriusRisk	Paid	Web-based, In-house or Cloud, CI/CD integration	*https://iriusrisk.com*
SD Elements	Paid	Web-based, In-house or Cloud	https://www.securitycompass.com/sdelements/
Devici	Paid	Web-based	https://devici.com/
OWASP Threat Dragon	Free	Web-based, Windows, Mac, Linux installs	https://www.threatdragon.com/
Drawing tools – Draw.IO, Mural, Miro, etc.	Free-*ish*	Web-based, Windows, Mac, Linux installs	Various

Resources – More Tools

#boscc Boston Code Camp

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
https://top10proactive.owasp.org/

Upcoming Local Events

#boscc
Boston
Code Camp

OWASP Boston Application Security Conference (BASC) 2025 at
Microsoft Offices, Burlington, MA (4/5) – $30 per ticket*
* - Students are free (will be refunded the $30)

https://www.basconf.org/

- Topics: AI, Zero Trust, Red Teaming, Threat Modeling, API Fuzzing, Mobile Security, and more!

Questions?

#boscc
Boston
Code Camp

Slides:

https://roberthurlbut.com/r/BCC38

RobertHurlbut.com

@RobertHurlbut

#boscc
Boston
Code Camp

Thank you!