Evaluating the Security Landscape with Threat Modeling

Who Am I

- Shail Patel (bind_tcp)
- Security Researcher, AppSec Engineer @FormAssembly, Ex-@NREL
- 2 years in information security now
- Occasional Bug Bounty and CTFs

Motivation

- Why would an adversary target my organization?
- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?

Vulnerability Vs Threat Vs Risk

"Close the Open Door (Vulnerability) to keep out the Bear (Threat). Otherwise we are Screwed (Risk)"

-Luca Bongiorni

Common Methods For Finding Security Flaws

- Penetration Testing/Vulnerability Assessments
- SAST/DAST/Fuzzing
- Incident Response
- Scheduled audits and bug reports

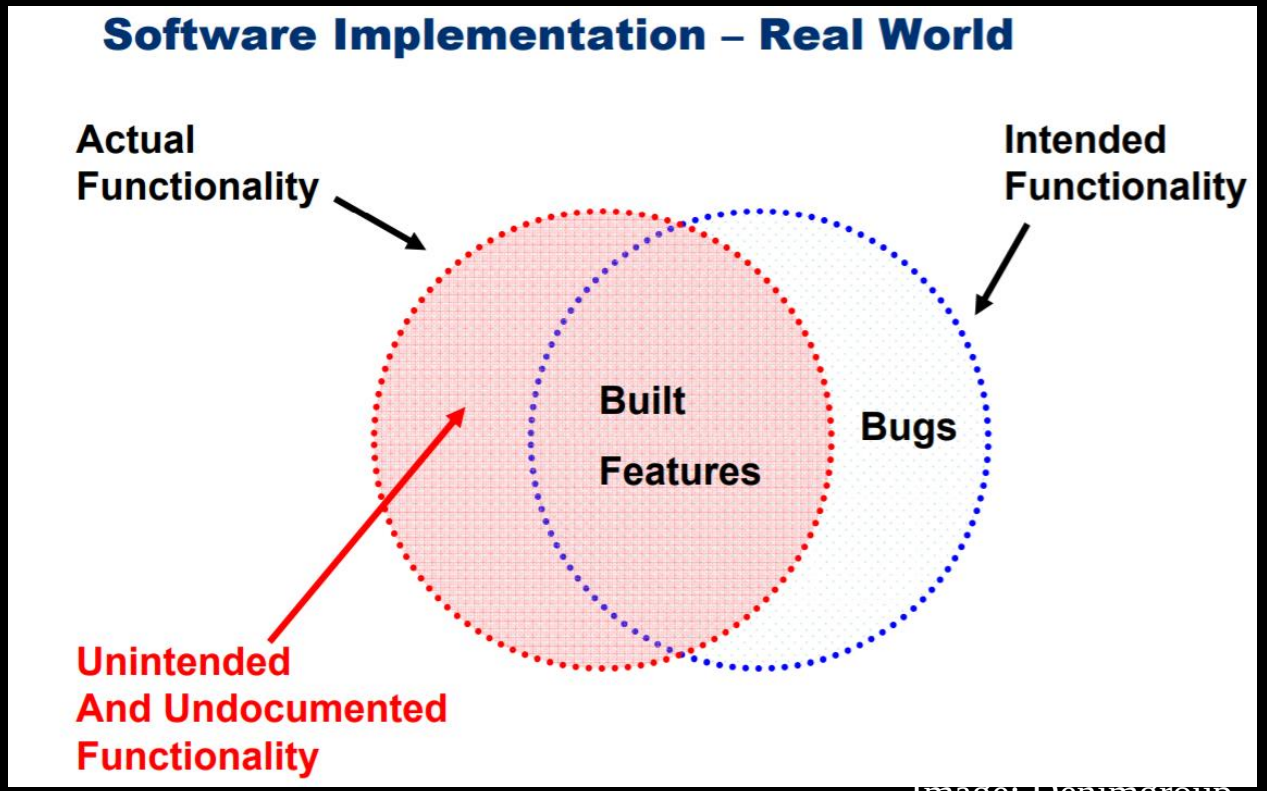
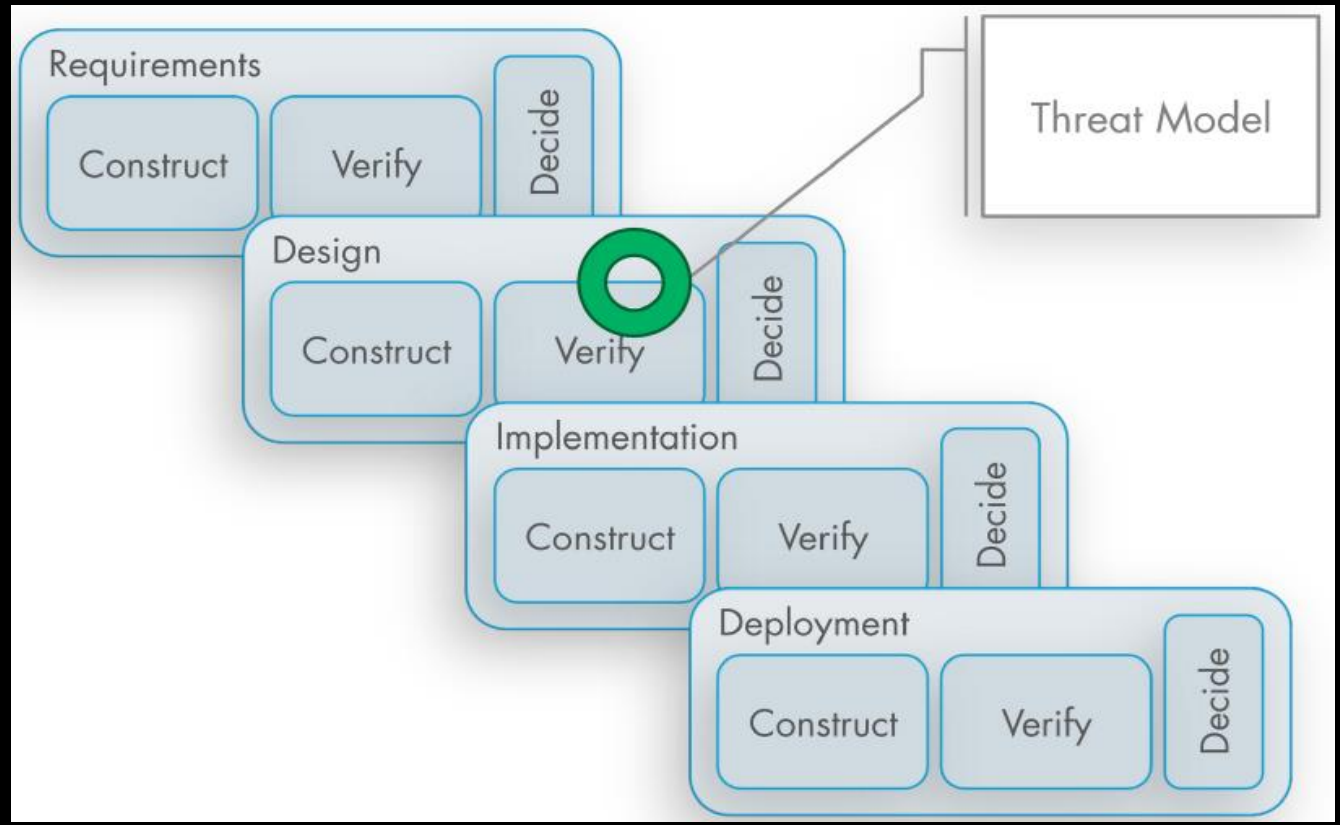


Image: Denimgroup

Why do we care for Threat Modeling?

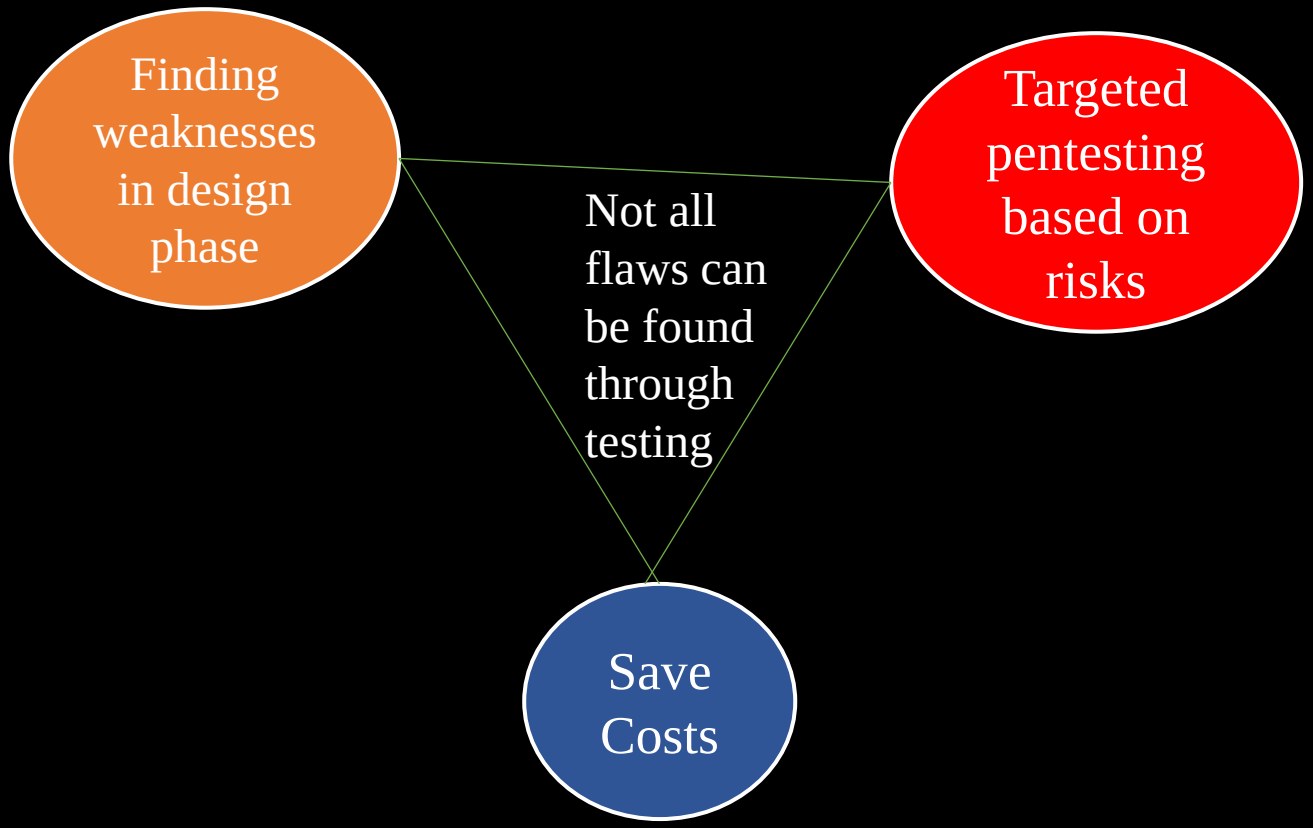
- Improve secure design
- Threat identification and compliance requirements, risk evaluation
- Document threats and mitigation
- Improving efficiency
- Avoid writing buggy code



What is Threat Modeling?

- Thinking about what bad can happen and what can you do about it
- Finding logical flaws and reveal problems in software development practices
- Deliver better product, prioritize your preventive security measures, and focus your testing on most risky parts of the system
- Free-for-all: devs, testers, architects, project managers and product owners
- To remain useful, the model must be kept up-to-date

Benefits of threat modeling?



What's WITHIN a threat model?

- Each and every nook and cranny of systems involved
- Potential threats and assumptions
- Decision model for addressing each threat
- Validation approach

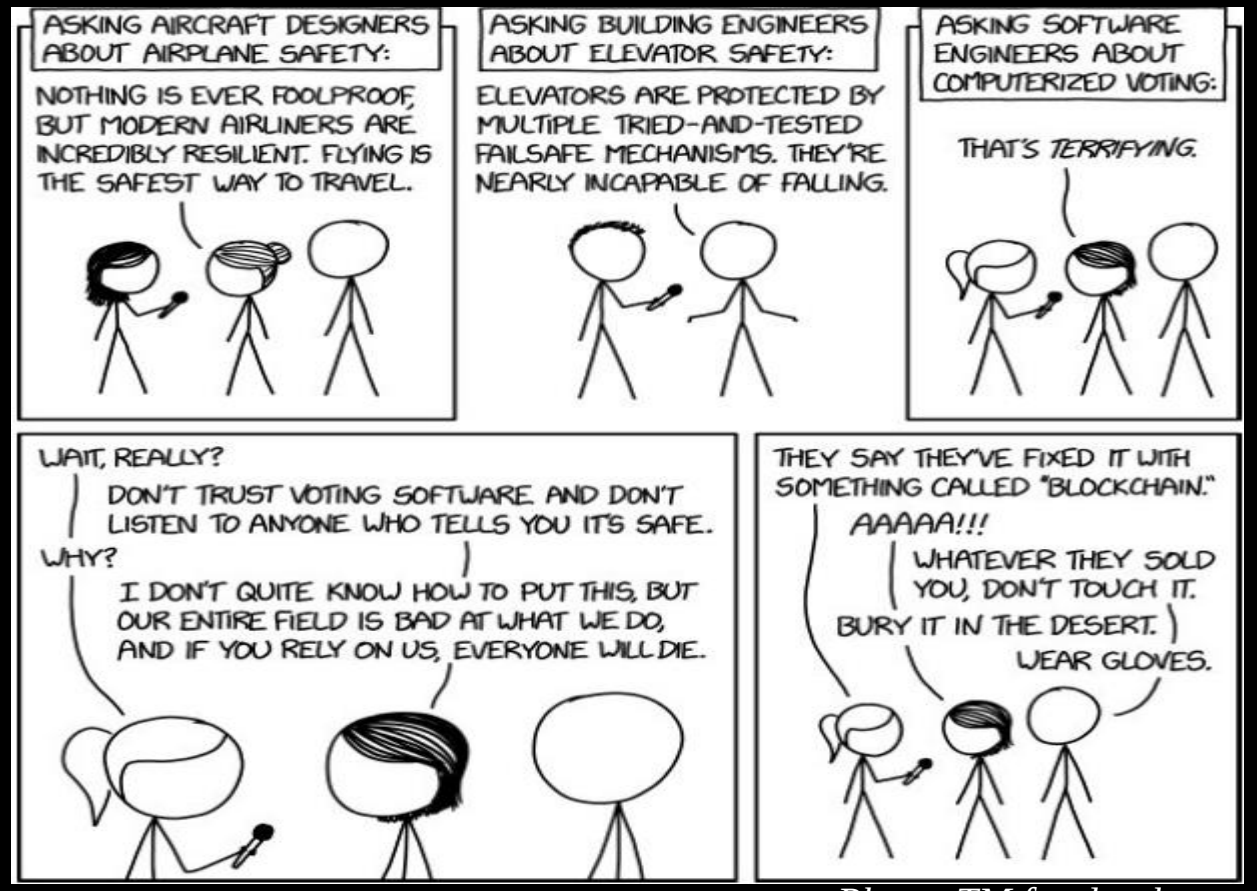


Photo: TM for developers

Additional Things to consider

- Every stakeholder should take part in threat modeling
- Start modeling early as possible
- Can be applied everywhere: E.g. IT as well as ICS/OT security
- Update your model in every cycle

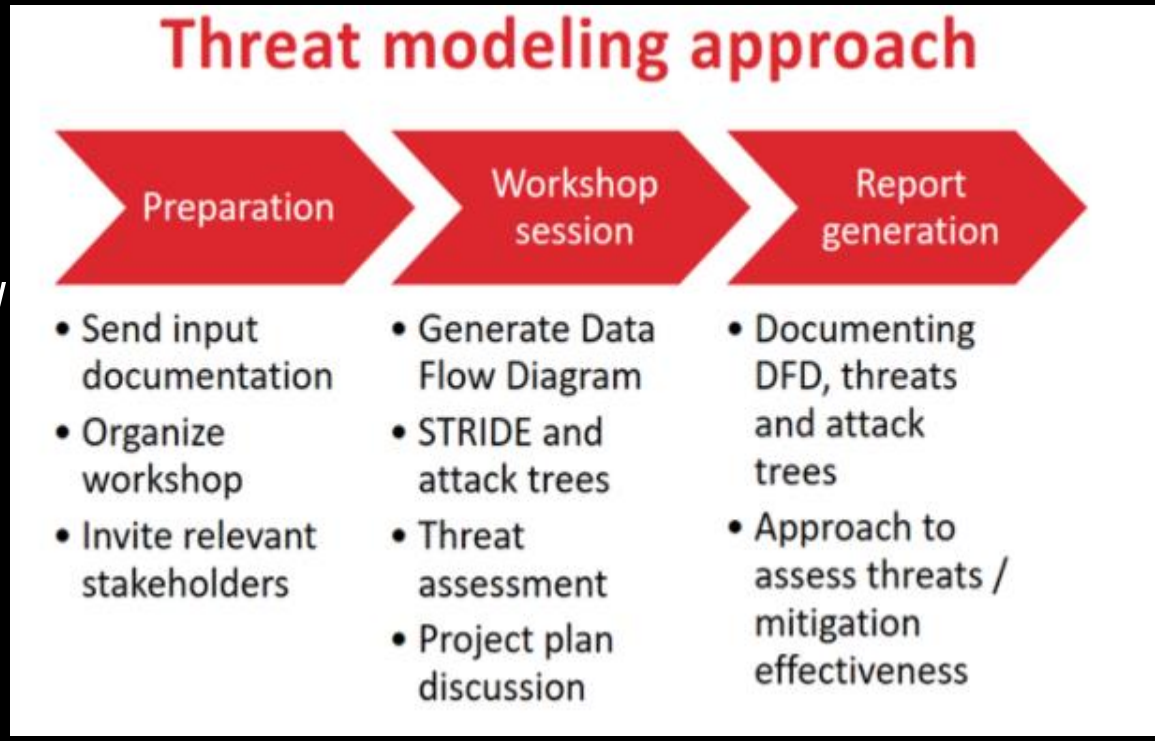
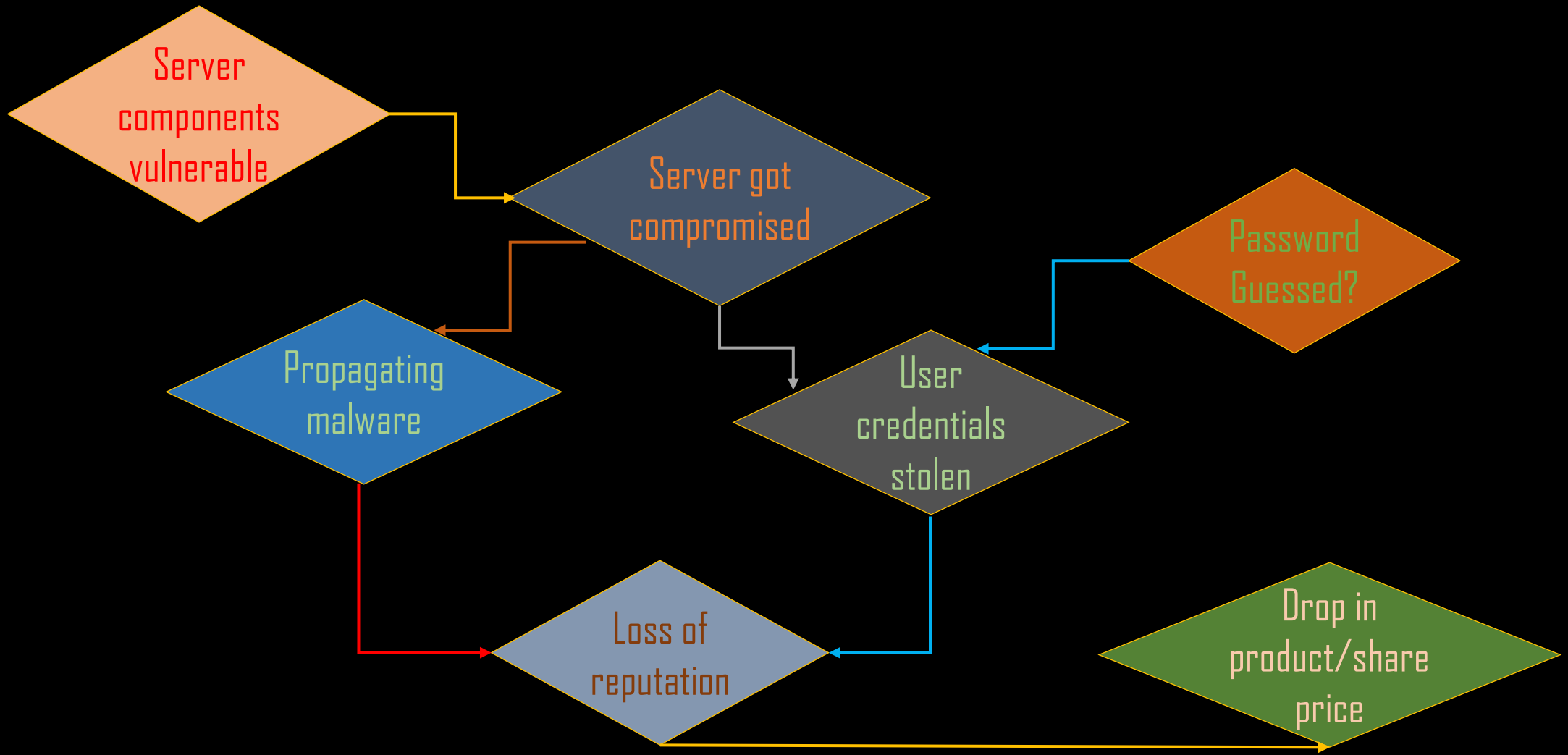


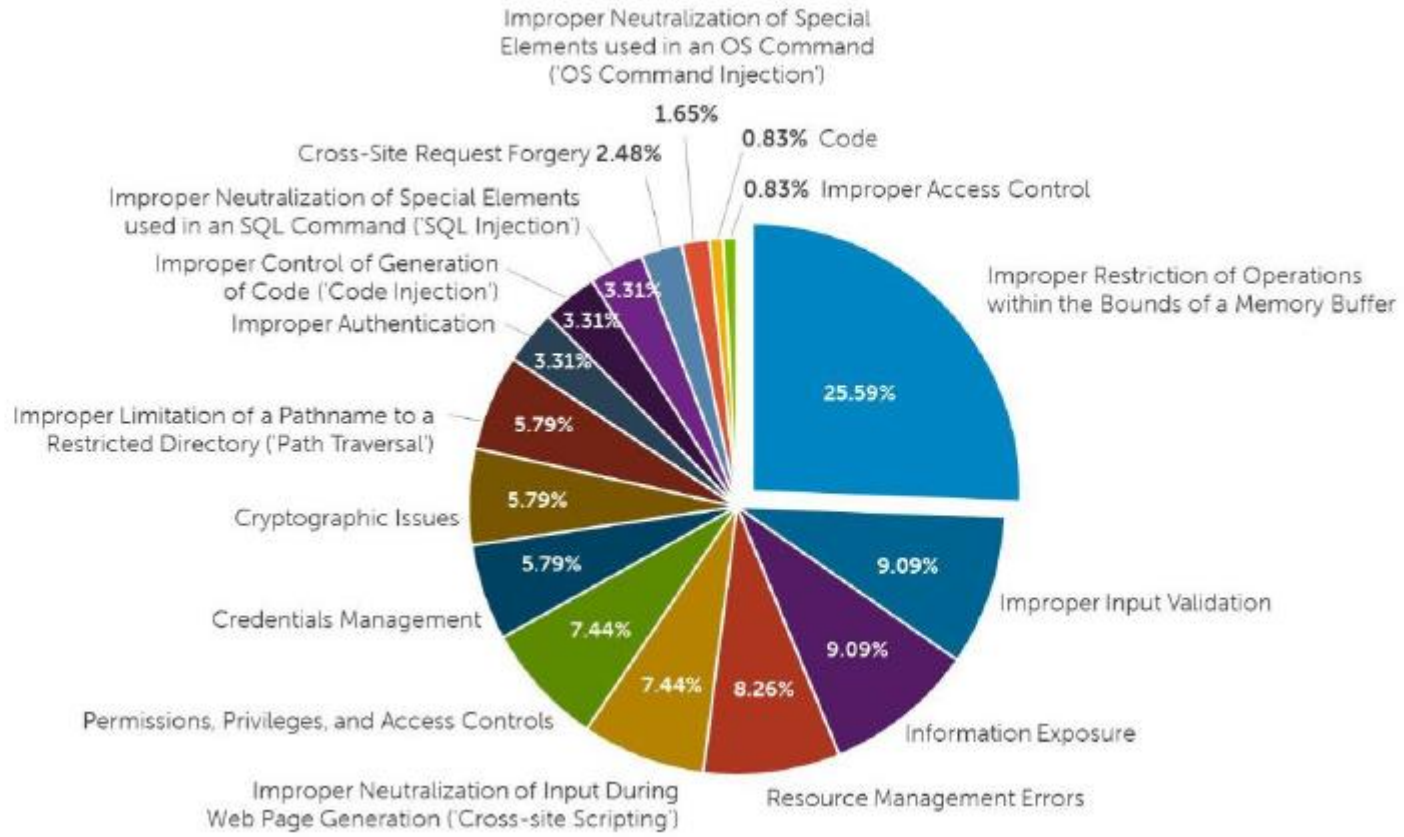
Image: secura.com

A typical threat scenario



Coping with Vulnerabilities

Many of them are application-based attacks



* Dell Security Annual Report 2015

Beware! They are right between you and me.

Think like an attacker first

- What does an adversary want?
- What are they aware of?
- What can they do?
- What threats are relevant to our business?

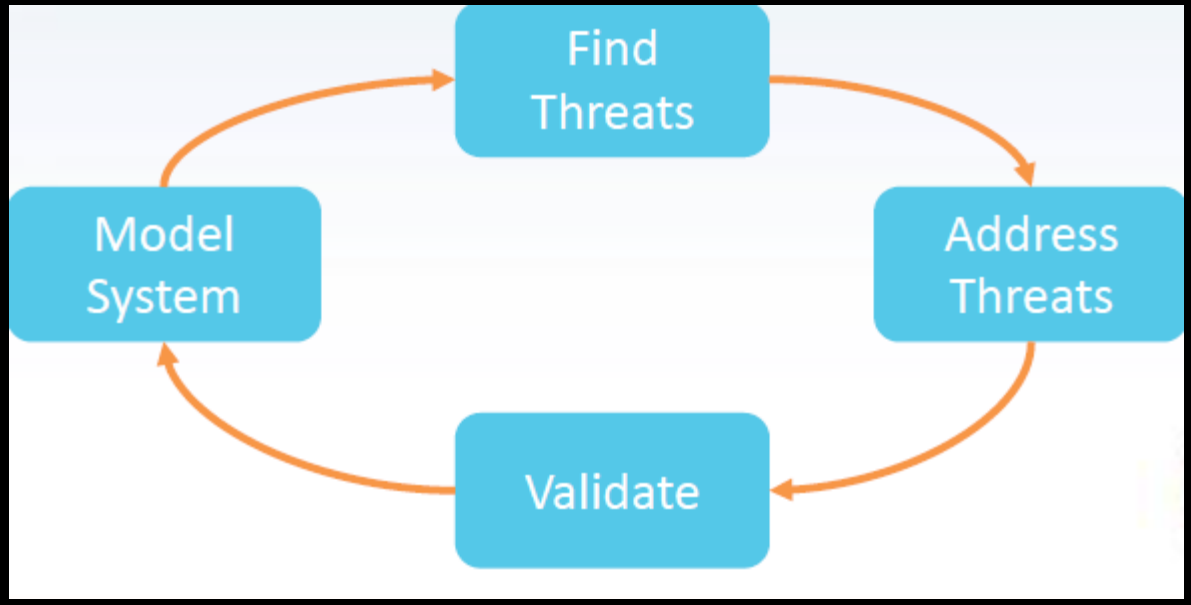


Image: Shostack's questions

“ Building Security in “

“ Security by design “

“ Shifting security left “

Threat Modeling Stages

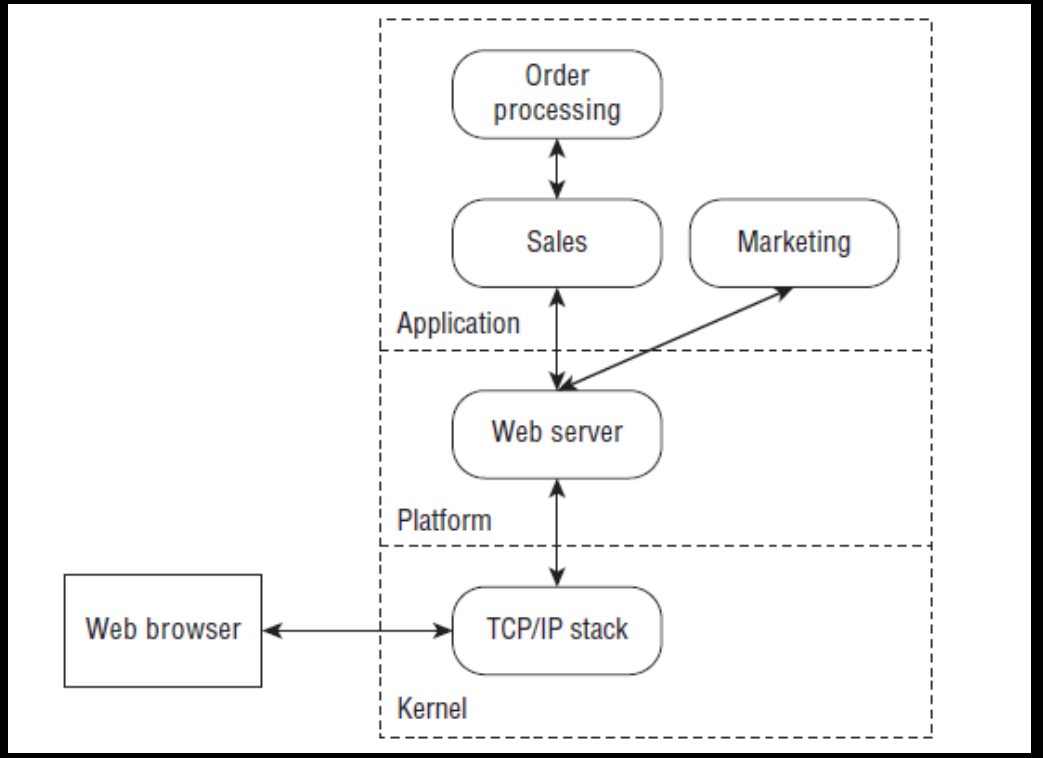
- Identify assets
  - What is most important to (customer, vender)-attenders and bankers (organizers)
  - What does law / regulations require –pci compliance
  - What / who can do damage
- Create an architectural overview
  - Context diagram
  - Decompose the system (e.g. DFD) to illustrate the boundaries of system components)
- Identify and categorize threats
- Rank threats
- Plan for mitigations

All to know about trust boundaries

- Trust boundaries show where trust levels change

- Across where two or more principals interact
  - Principles are UIDs (unix) / SIDs (Windows)
  - Apps on mobile platforms

- Need to be enforced in some way
  - Best to rely on existing facilities – don't "roll your own"
  - Building a database sometimes is not possible



- Any place where data is passed between two processes is typically a trust boundary

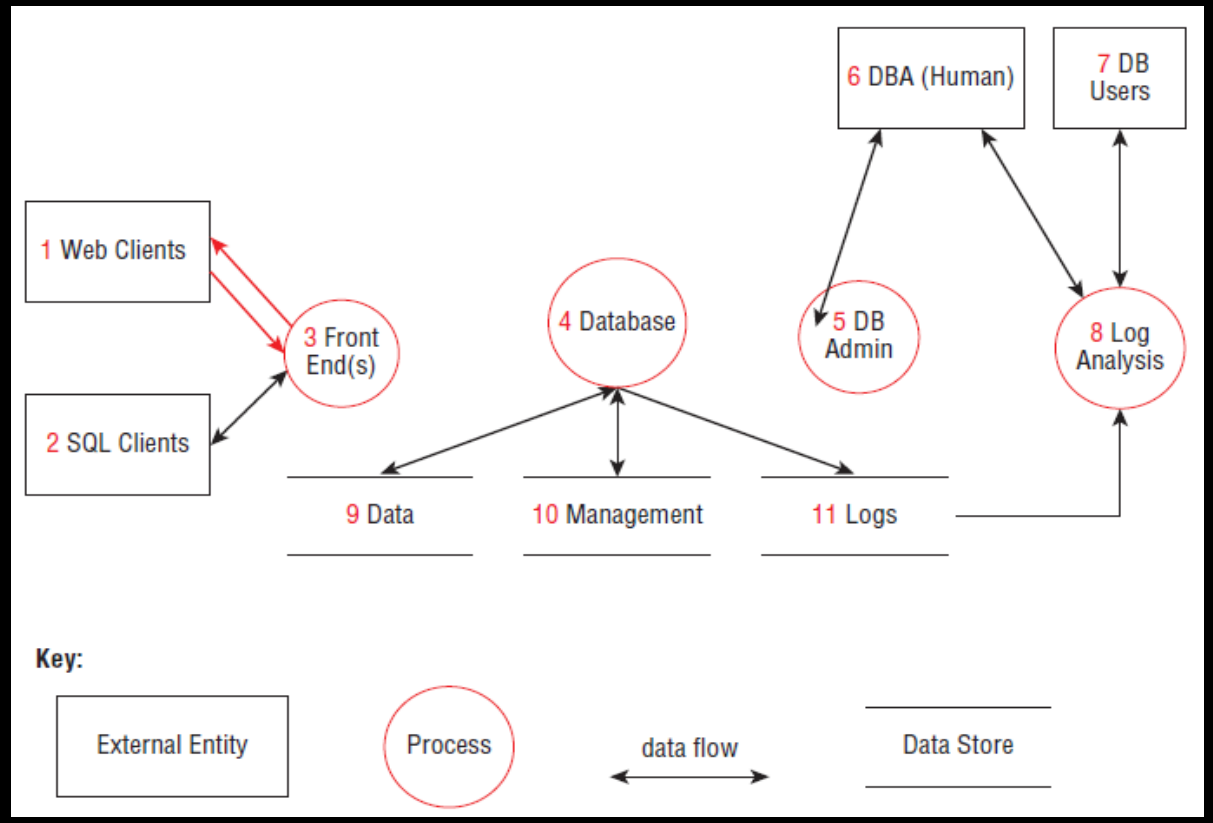
Data Flow Diagrams

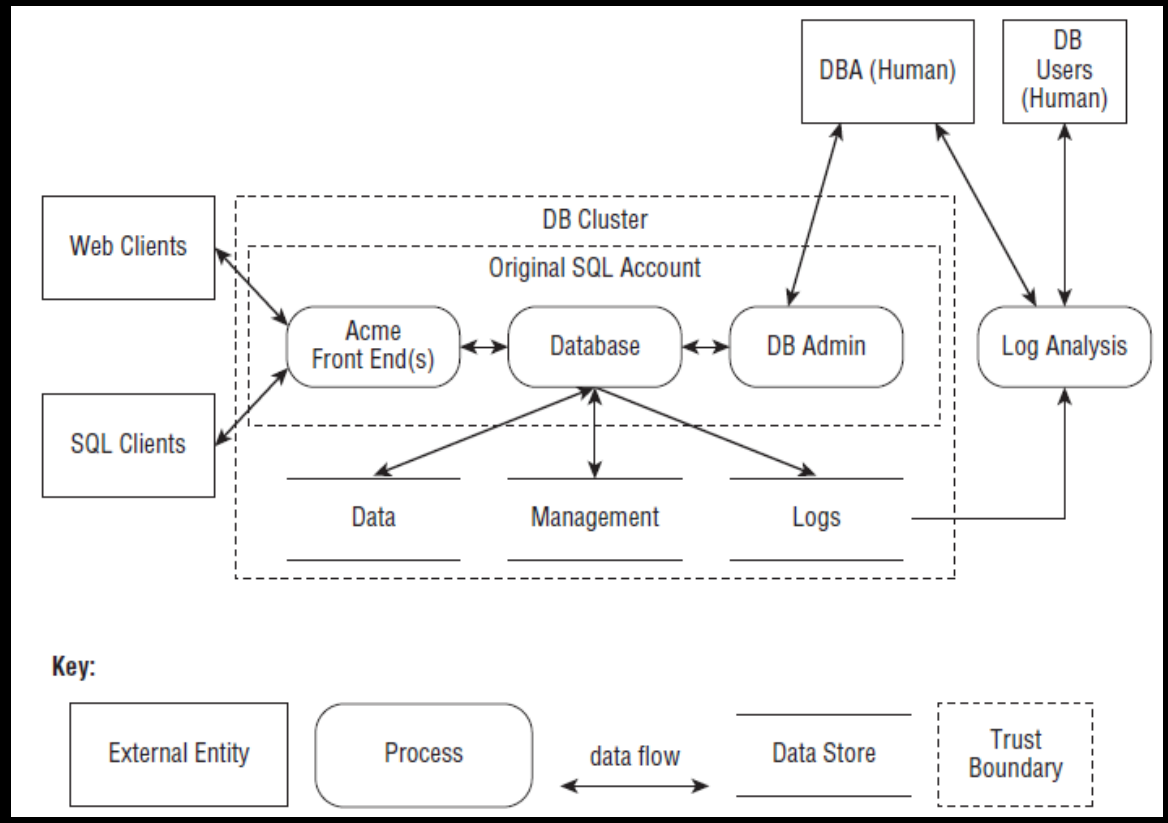
- Data flow models are ideal for threat modeling
- More commonly exist for network / architected systems than software products
- Consists of numbered elements connected by data flows, interacting with external entities

ELEMENT	APPEARANCE	MEANING	EXAMPLES
Process	Rounded rectangle, circle, or concentric circles	Any running code	Code written in C, C#, Python, or PHP
Data flow	Arrow	Communication between processes, or between processes and data stores	Network connections, HTTP, RPC, LPC
Data store	Two parallel lines with a label between them	Things that store data	Files, databases, the Windows Registry, shared memory segments
External entity	Rectangle with sharp corners	People, or code outside your control	Your customer, Microsoft.com

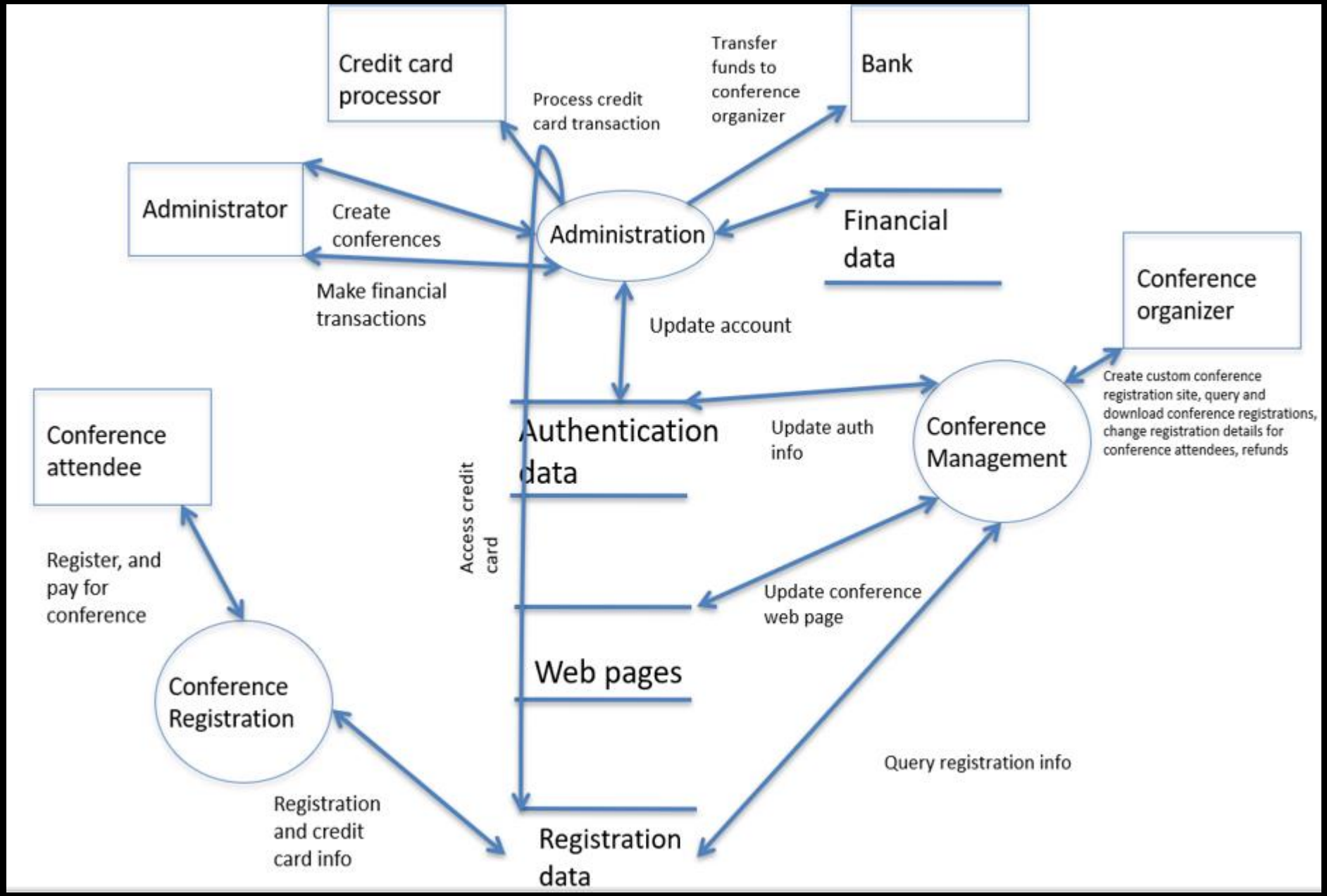
Elements of a DFD

Data Flow Diagrams Continued





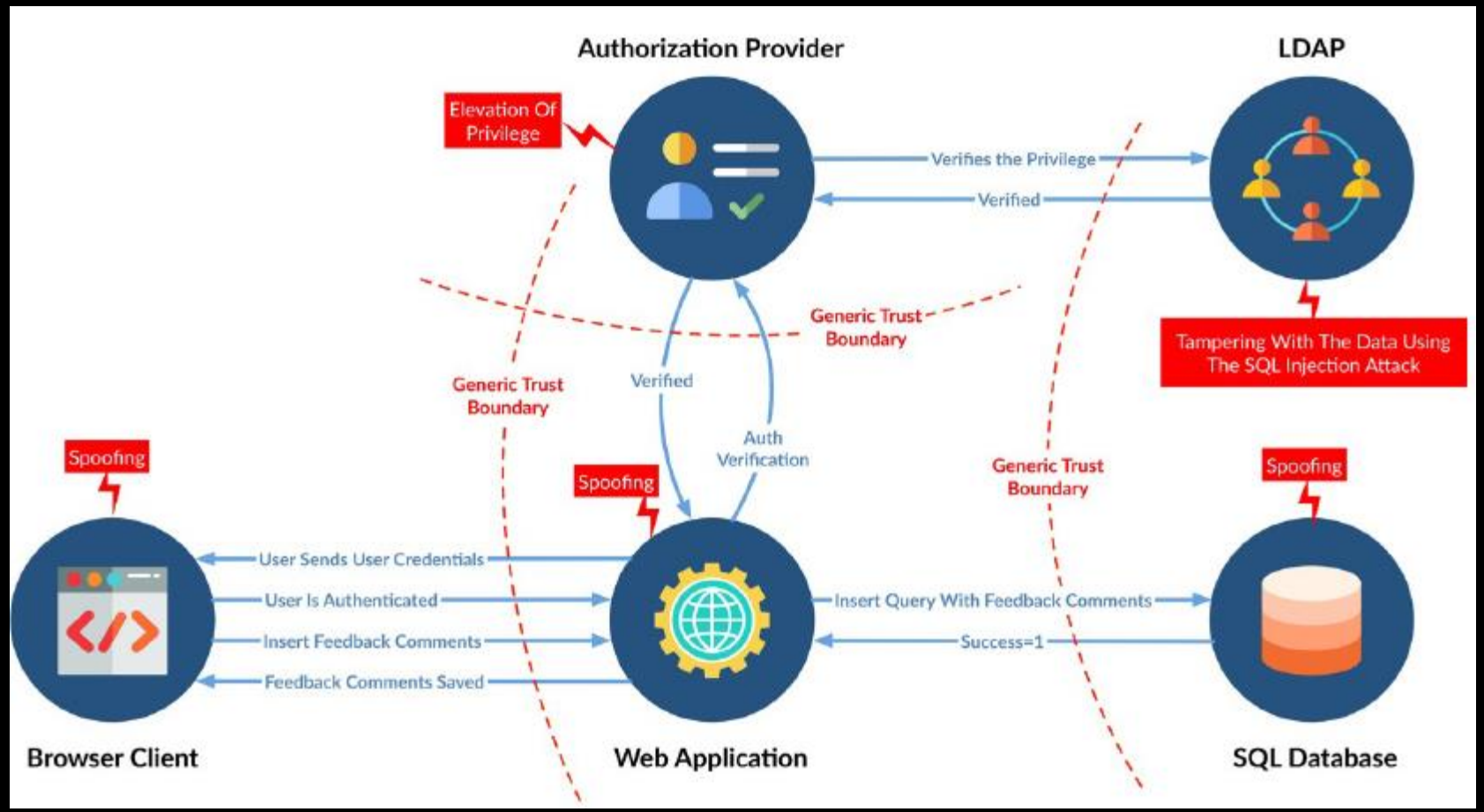
A classic DFD model VS modern DFD implementation



Level-1 DFD for online conference management system

STRIDE* threat categories

Spoofing identity
Tampering with data
Repudiation
Information Disclosure
Denial of service
Elevation of privilege



How to apply STRIDE*

- How can every STRIDE threat affect every other part of the model!

- Consider an adversary could spoof this part of the system?...tamper with?...etc."

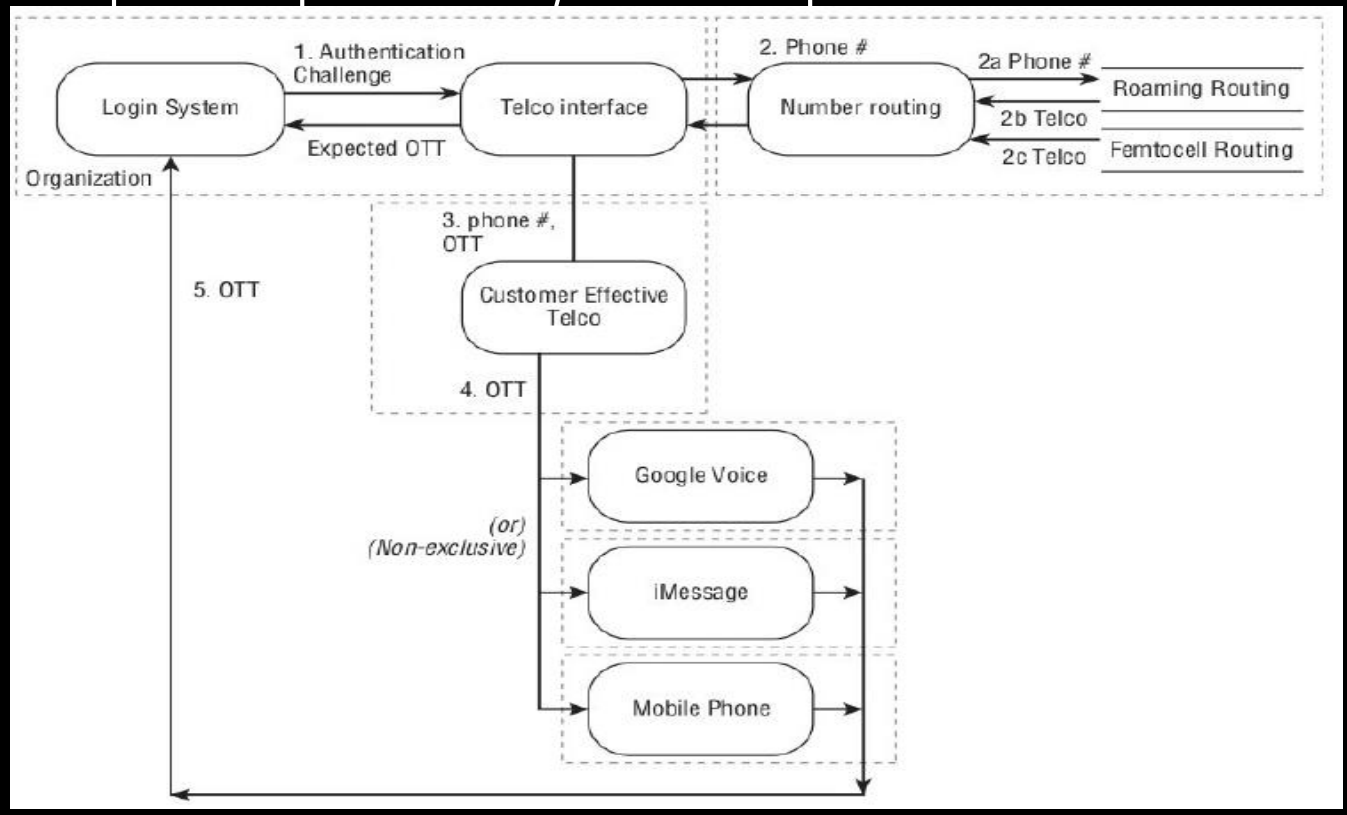
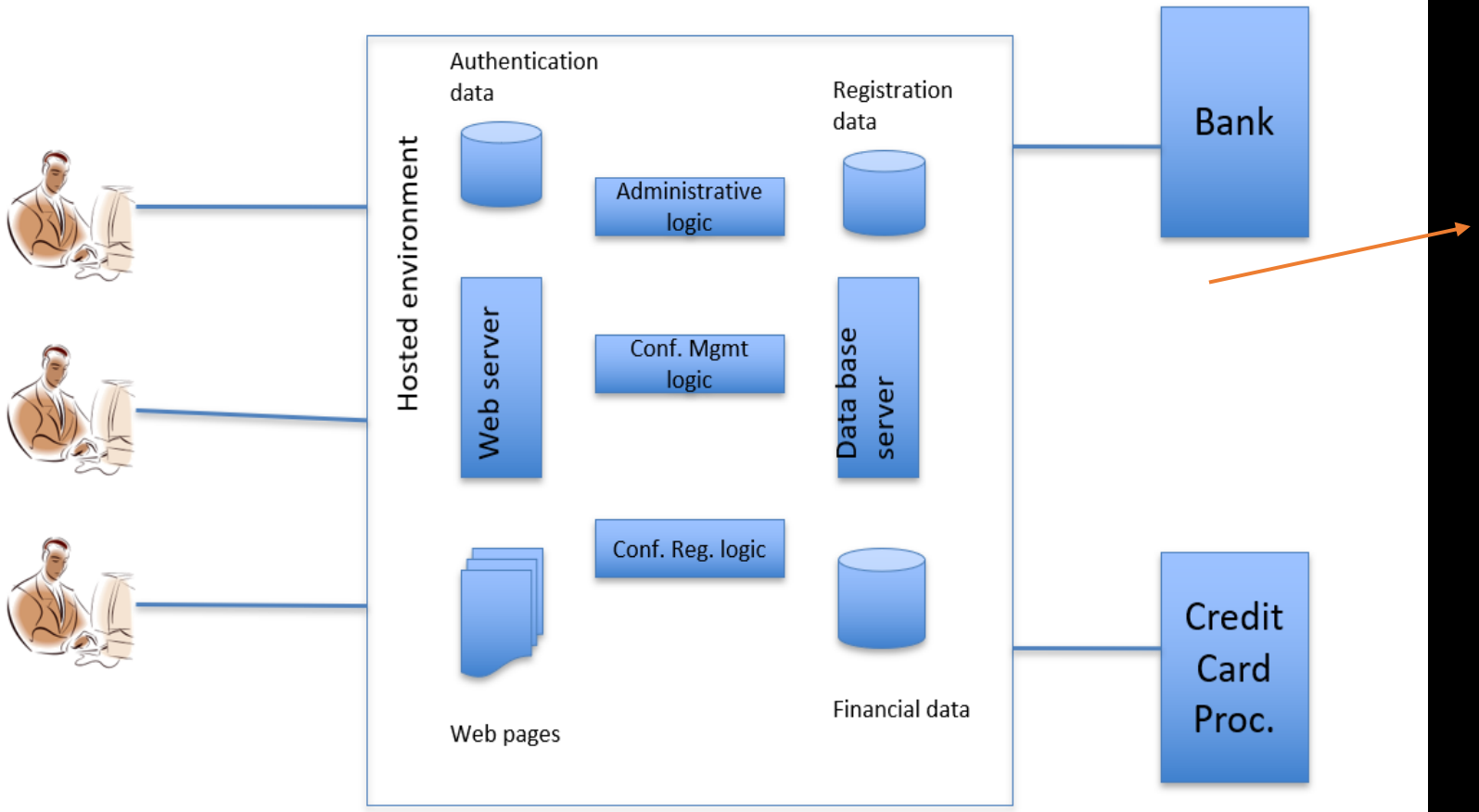


Photo: Adam Shostack

Physical view of our Conference Management System



Developing a threat model for an Online Conference Management System

How to get into the Conference system?

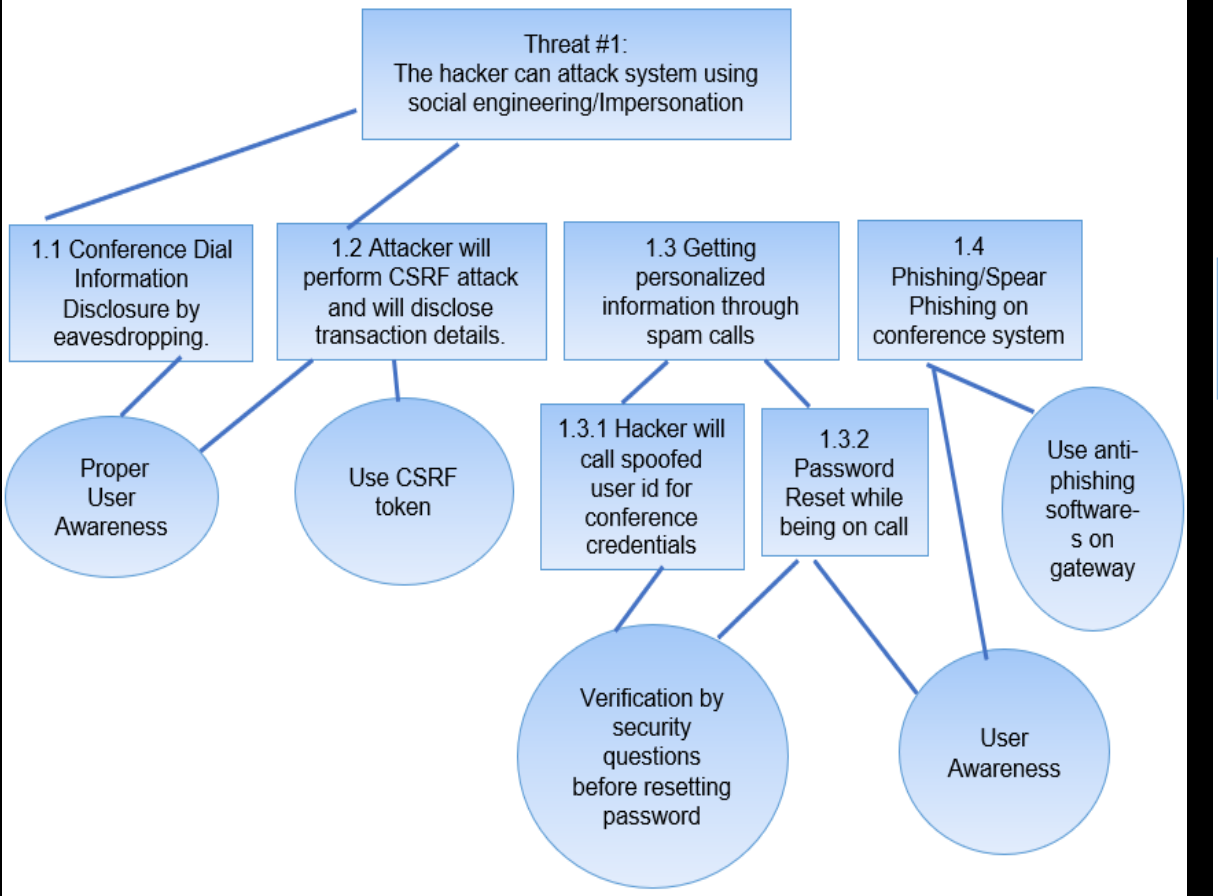
Various entry - endpoints

Boundaries

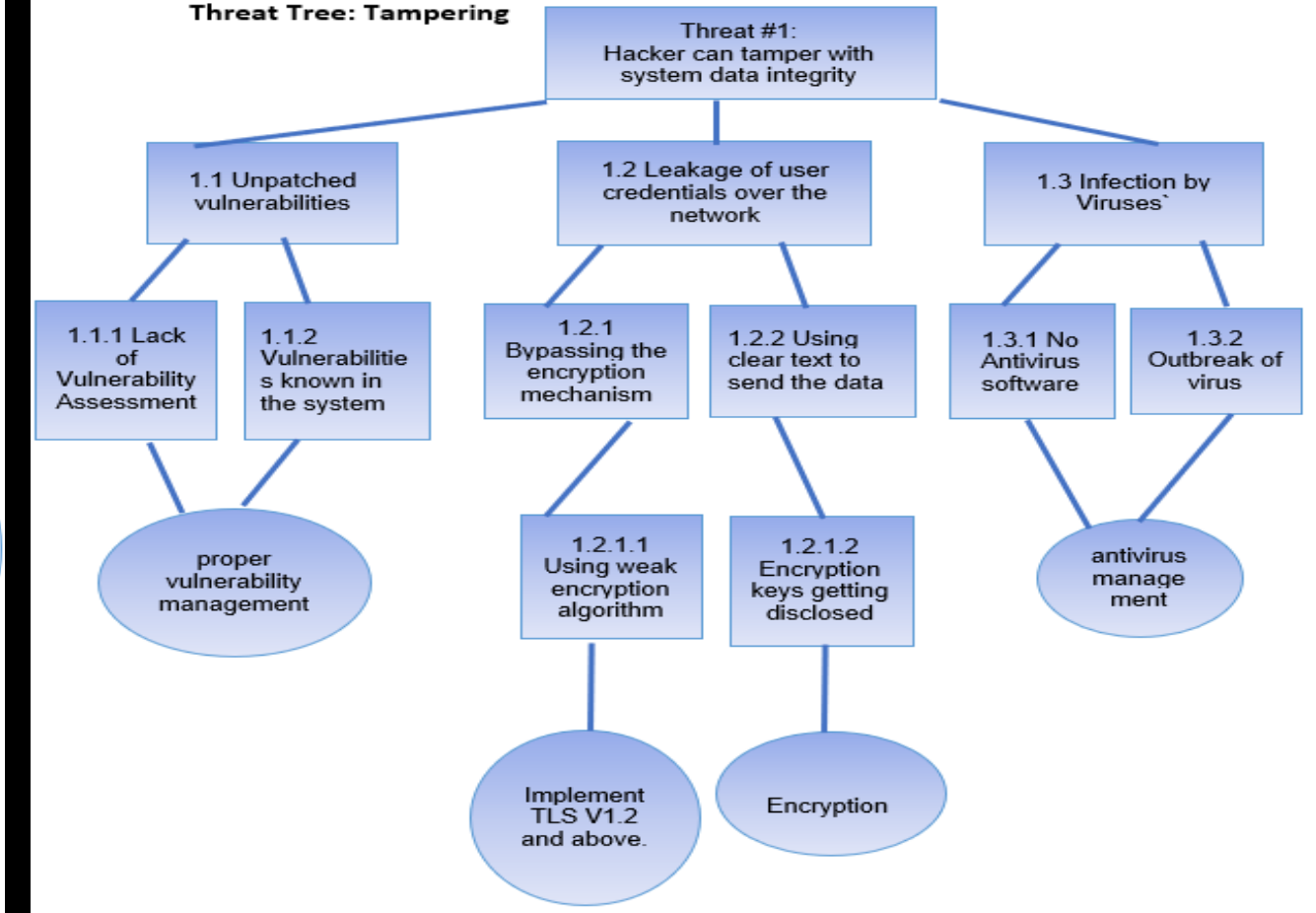
Entry Points

Name	Description	Trust Levels
HTTPS Port	The online conference website will be accessible via SSL. All pages within the conference system website are layered on this entry point.	(1) Anonymous Web User (2) User with Valid Login Credentials (3) User with Invalid Login Credentials (4) Admin
Online Conference Main Page	The splash page for the Online Conference website is the entry point for all users.	(1) Anonymous Web User (2) User with Valid Login Credentials (3) User with Invalid Login Credentials (4) Admin
Login Page	Conference attendees, conference organizers and admin must log in to the conference system website before they can carry out any of the use cases.	(1) Anonymous Web User (2) User with Login Credentials (3) User with Invalid Login Credentials (4) Admin
Login Function	The login function accepts user supplied credentials and compares them with those in the database.	(1) User with Valid Login Credentials (2) User with Invalid Login Credentials (3) Admin
Search Entry Page	The page used to enter a search query.	(2) User with Valid Login Credentials (4) Admin

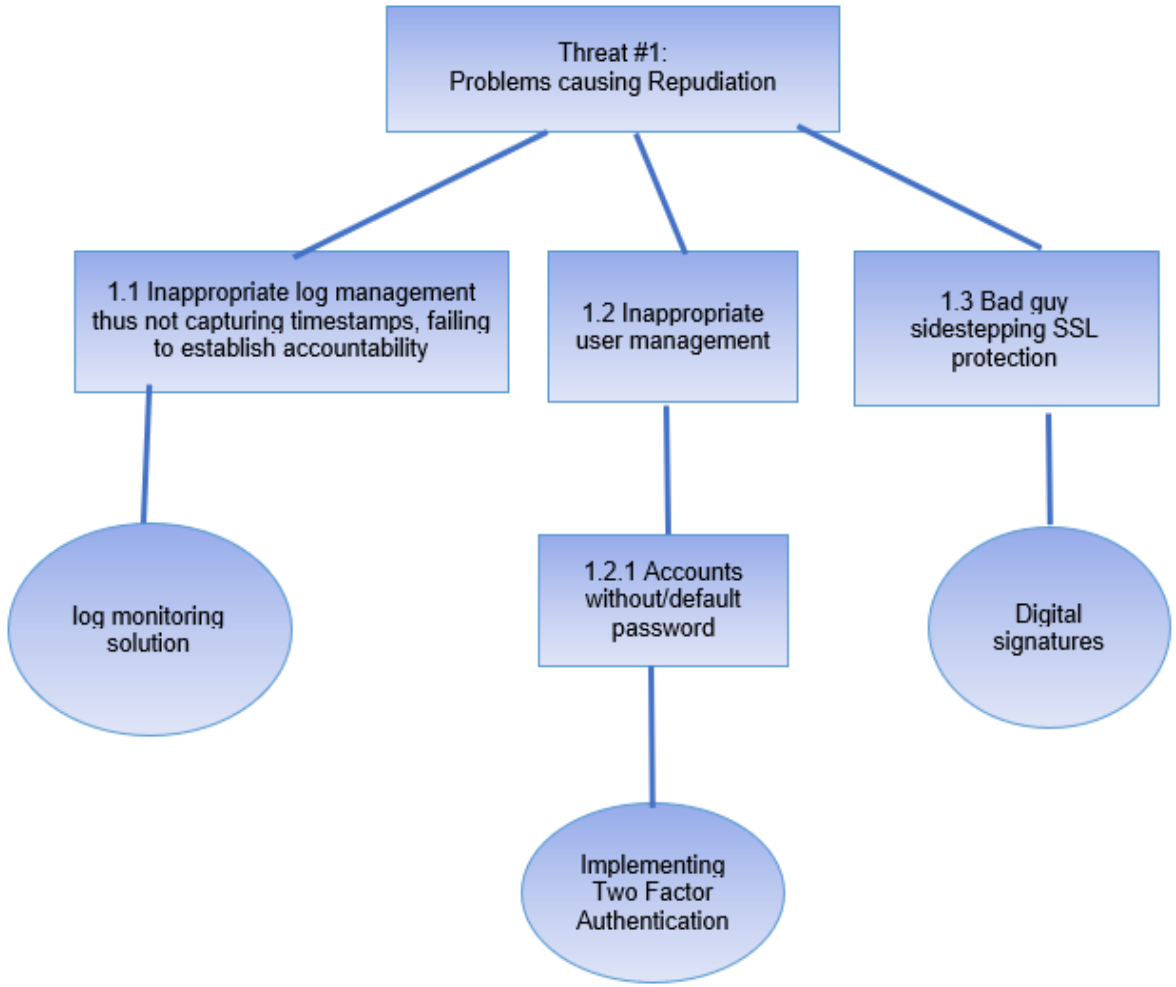
Threat Tree: Spoofing



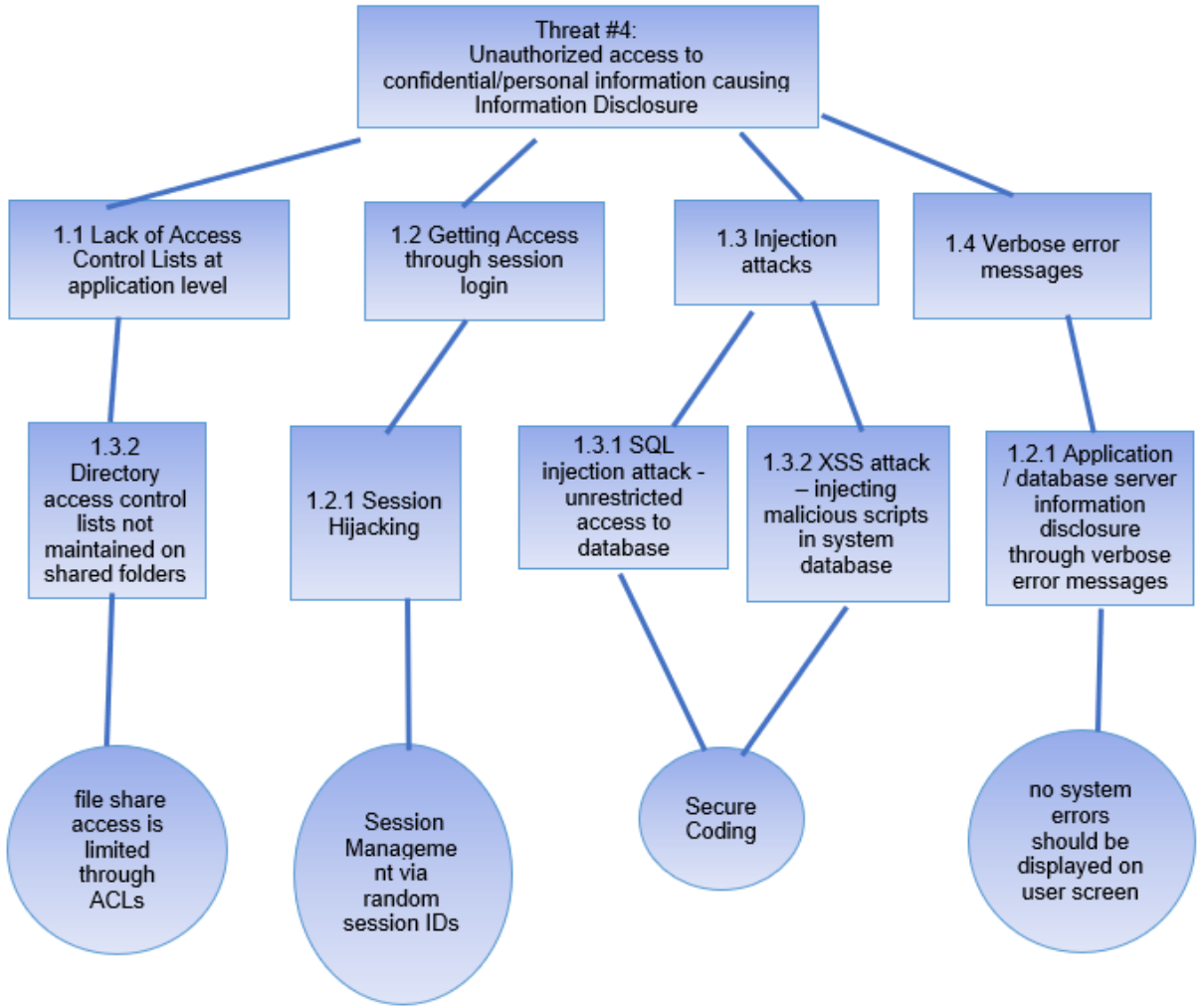
Threat Tree: Tampering



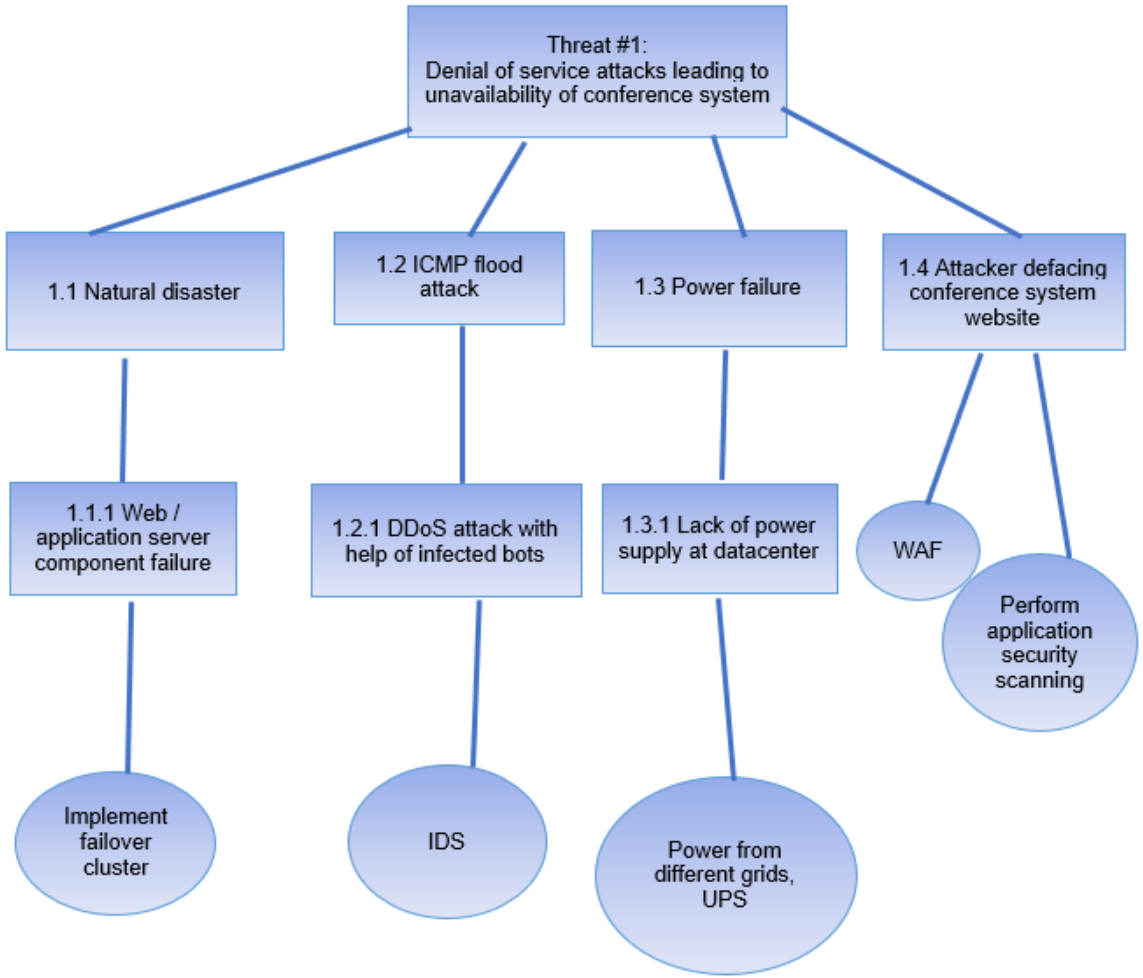
Threat Modelling: Repudiation



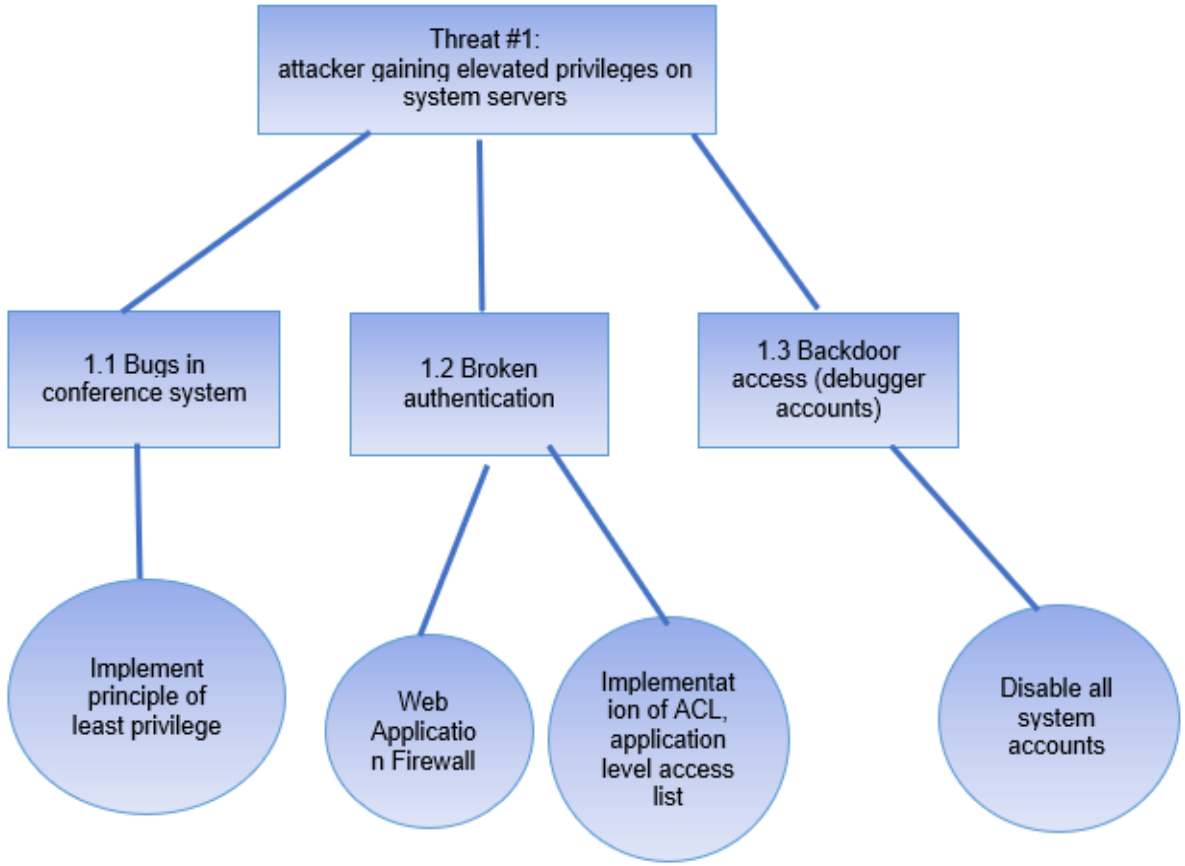
Threat Tree: Information Disclosure



Threat Tree: Denial of Service

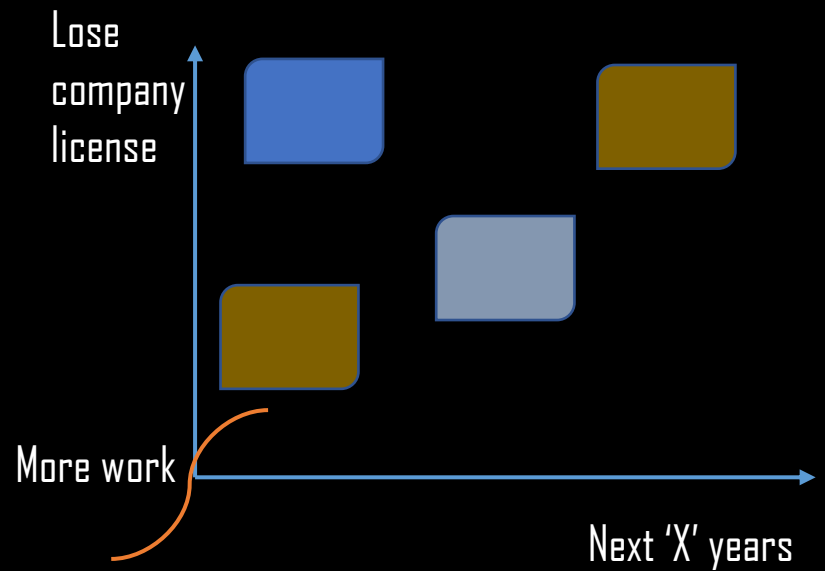


Threat Tree: Elevation of Privileges



What to do with the identified?

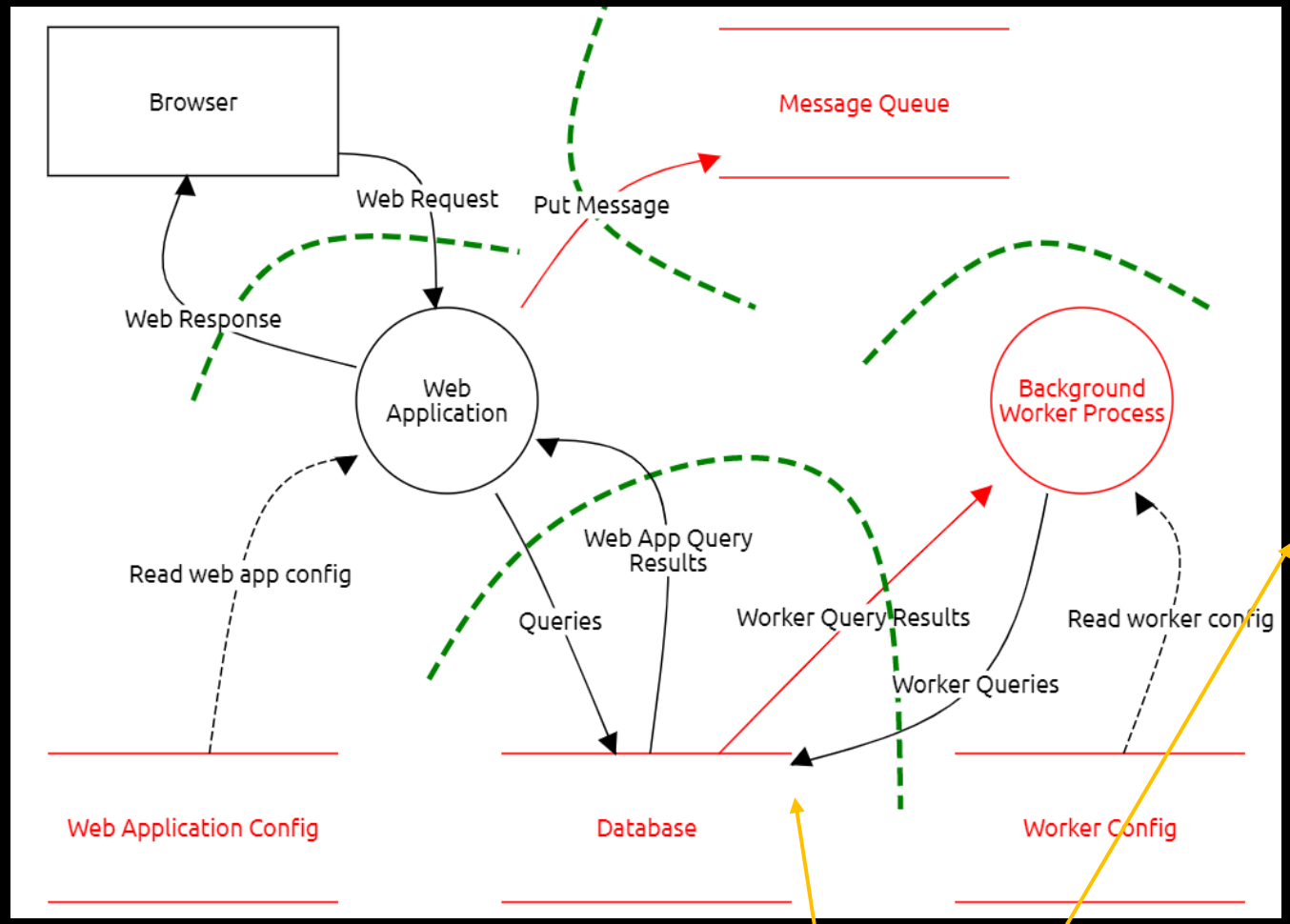
- ✓ Evaluate the impact
- ✓ Frequency of occurrence
- ✓ Calculate risk = likelihood x impact
- ✓ Risk handling mechanism
- ✓ What would be the priority then?



Risk = likelihood x impact

Other models

- PASTA – Process for Attack Simulation & Threat Analysis (risk-centric approach)
- VAST – Visual, Agile, & Simple Threat modeling
- OCTAVE – risks from breached assets (non-technical)
- TRIKE – unique implementation & risk-modeling process (risk-based approach)
- hTMM (hybrid threat modeling method)



Title

Potential SQLi

STRIDE threat type

Information disclosure

Threat status

Open | Mitigated

Severity

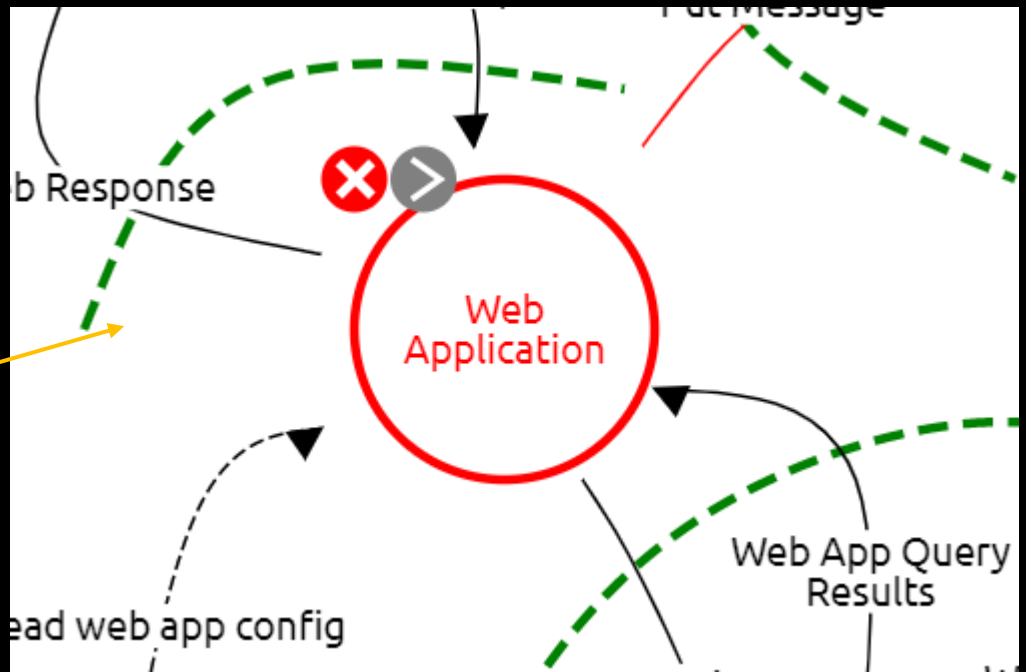
High | Medium | Low

Description

There is a potential BLIND SQLi within two hosts

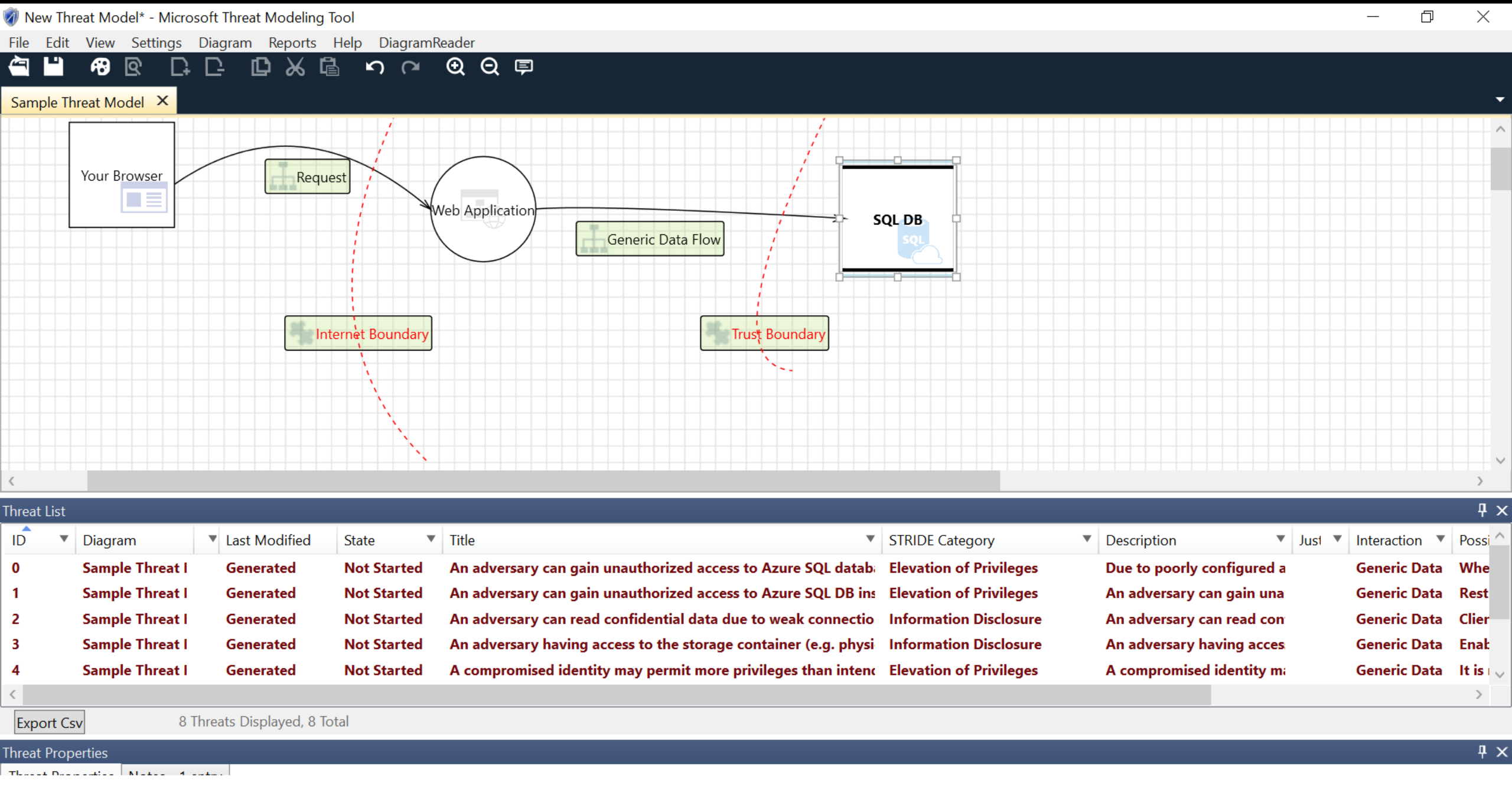
Mitigations

Separate the data channel from the control channel.

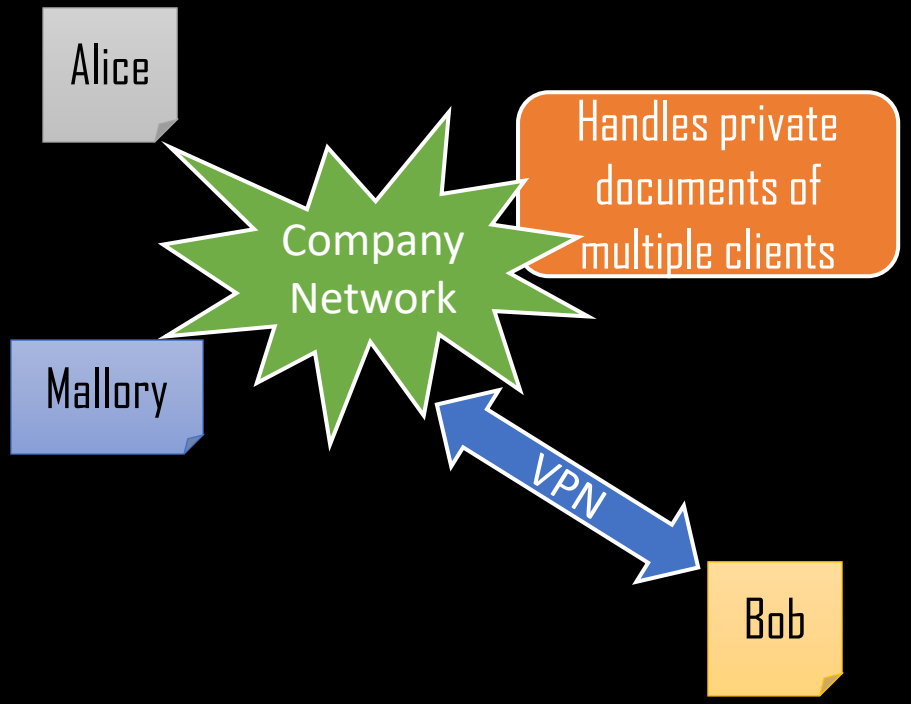


OWASP Threat Dragon implementation

Microsoft Threat Modeling tool



Threats Relevant from customer access?



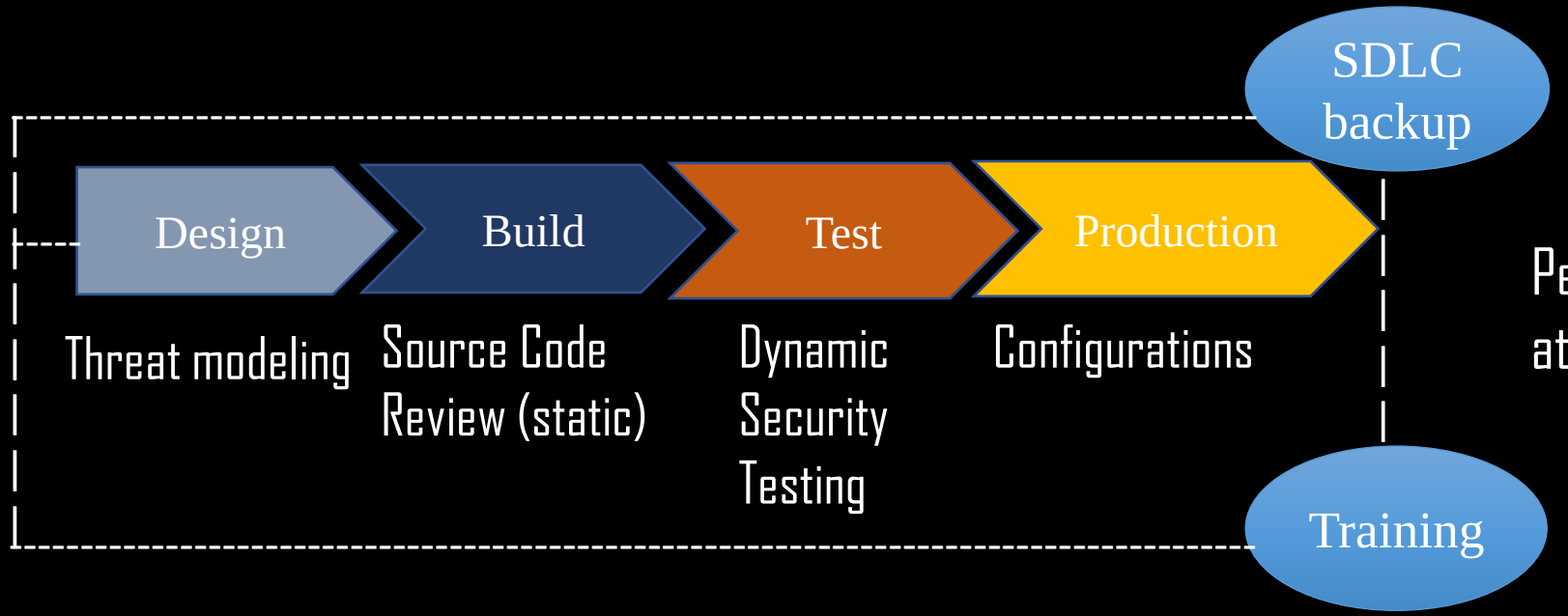
Alice (admin) handles user accounts within the company

Bob (handler) with access to documents; preferably remote with VPN

Mallory (handler) with access to private documents and insurance information (limited visibility)

Authenticate with user: pass

Secure Development Lifecycle



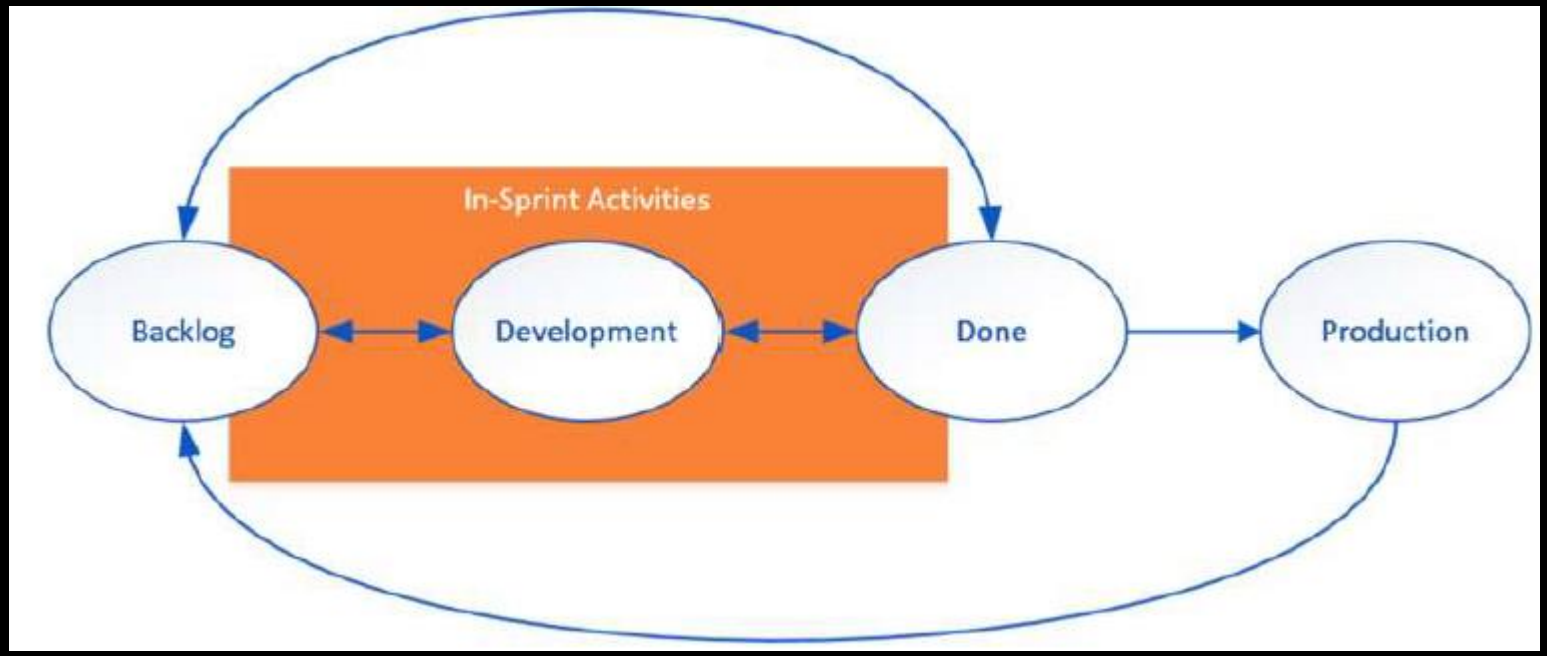
Perform threat modeling preferably at the early stages of SDLC

Software Development Lifecycle

- Ensuring secure SDLC throughout all phases:

  - Requirement gathering & analysis
  - Design
  - Implementation / coding
  - Testing

- Secure SDLC models:
  - OWASP SAMM
  - NIST
  - MS SDL



SDLC Agile

Threat modeling in DevSecOps

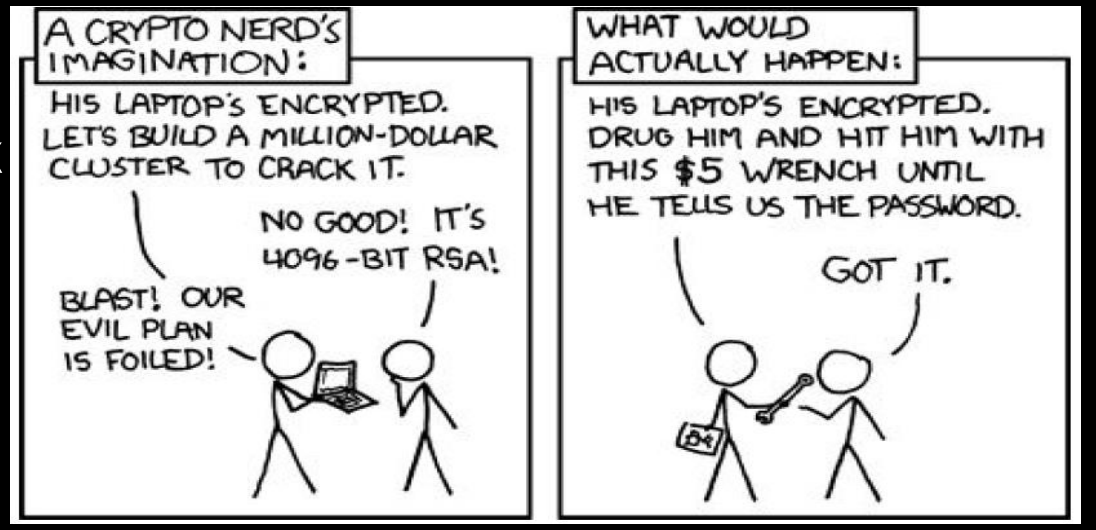
- Focus on enabling frequent operational and infrastructure changes
- Bring operations / infrastructure team, lead developers, solutions architect together
- Gather input from the entire team
- Threat modeling ensures constant robust performance

Spell your threat model

We cannot just “display” a security document
Intended parties often do not understand it

Departing thoughts

- For every threat discovered, leverage proven best practices the next time
- Use secure frameworks and apply appropriate secure design strategies
- Identify the defenses that will bring the system to a desired state
- Accept the vulnerability in design and associated risk



Thanks for tuning in!

@shail_official

shail@formassembly.com

https://github.com/spwn3r49sd3r00