From DevOps to DevSecOps

How Establishing a Threat Modeling Process Can Help You Transition

NDC Oslo

June 2020 **Bruno Amaro Almeida**

futurice

@bruno_amaro

Photo by Praveesh Palakeel on Unsplash

futurice

Hello!

Bruno Amaro Almeida

PRINCIPAL ARCHITECT & ADVISOR

Cloud, DevOps, Security, Data Engineering & AI

Reach out on:

@bruno_amaro

@brunoamaroalmeida

BERLIN · HELSINKI · LONDON · MUNICH · OSLO · STOCKHOLM · TAMPERE

ABOUT FUTURICE

Nordic roots, global mindset

futurice

600+

People

19

Years in Business

38

Nationalities

8

Offices

30%

YOY Growth

3000+

Projects

Our family of companies

Columbia Road

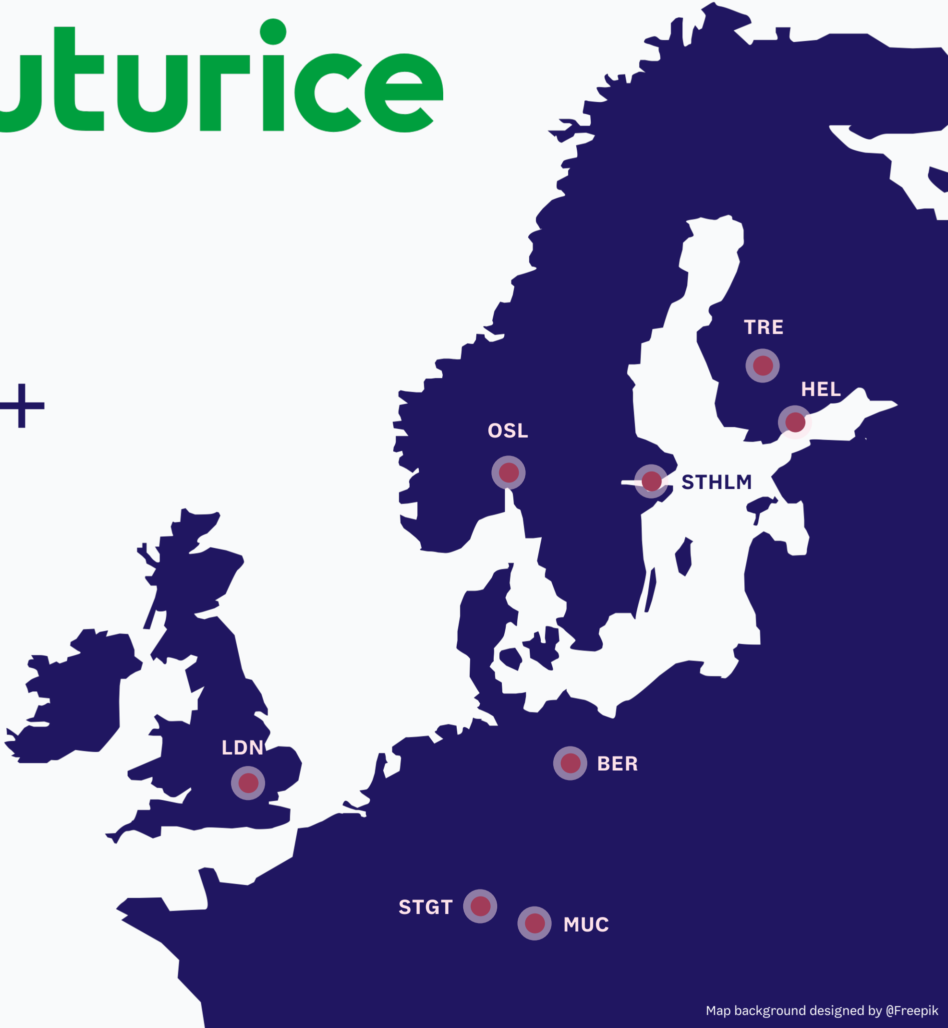
eCommerce and Growth-Hacking

aito

Artificial Intelligence and Machine Learning

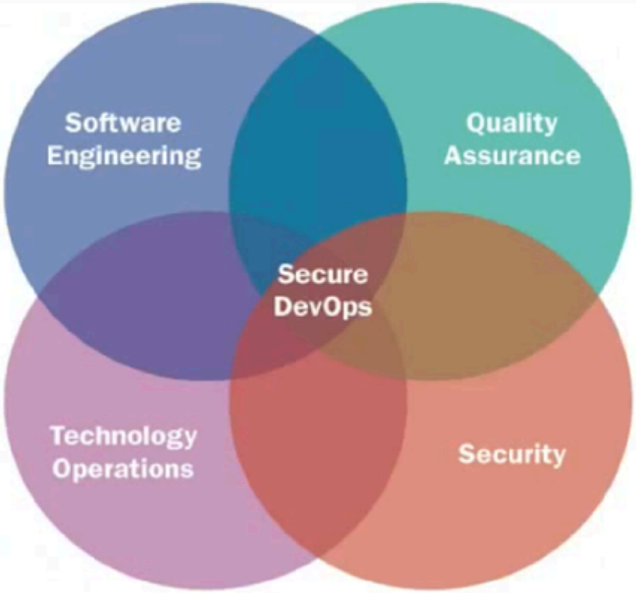
Tentimes

Platform for freelance tech professionals



Map background designed by @Freepik

”What is DevOps?



source: devops.com

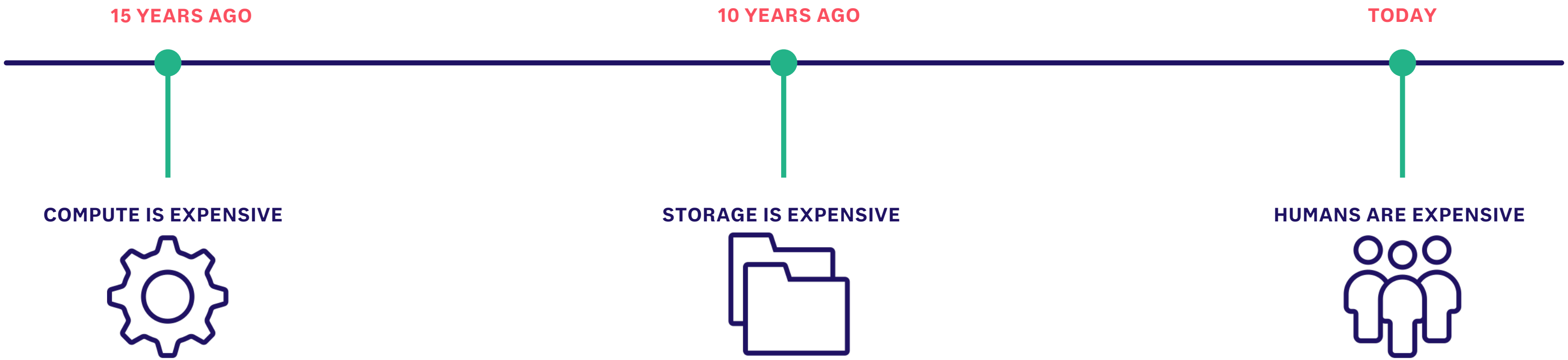
“**DevOps is** the combination of **cultural philosophies**, **practices**, and **tools** that increases an organization’s ability to deliver applications and services at high velocity(...)”

source: aws.amazon.com

“**DevSecOps** is the **philosophy of integrating security practices** within the **DevOps process**. DevSecOps involves creating a ‘**Security as Code**’ culture with ongoing, flexible collaboration between release engineers and security teams.”

source: sumologic.com

Evolution of Cost Optimization in Tech



15 YEARS AGO

COMPUTE IS EXPENSIVE

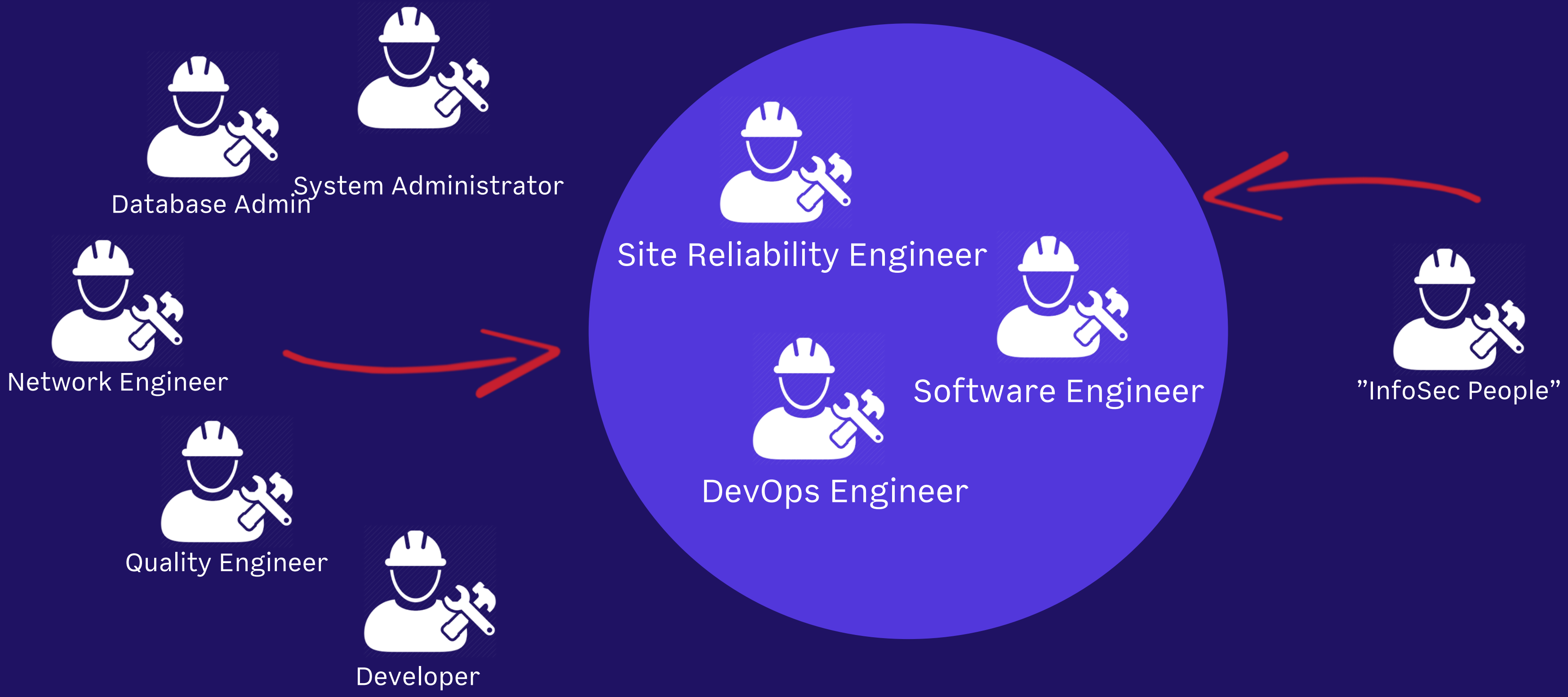
10 YEARS AGO

STORAGE IS EXPENSIVE

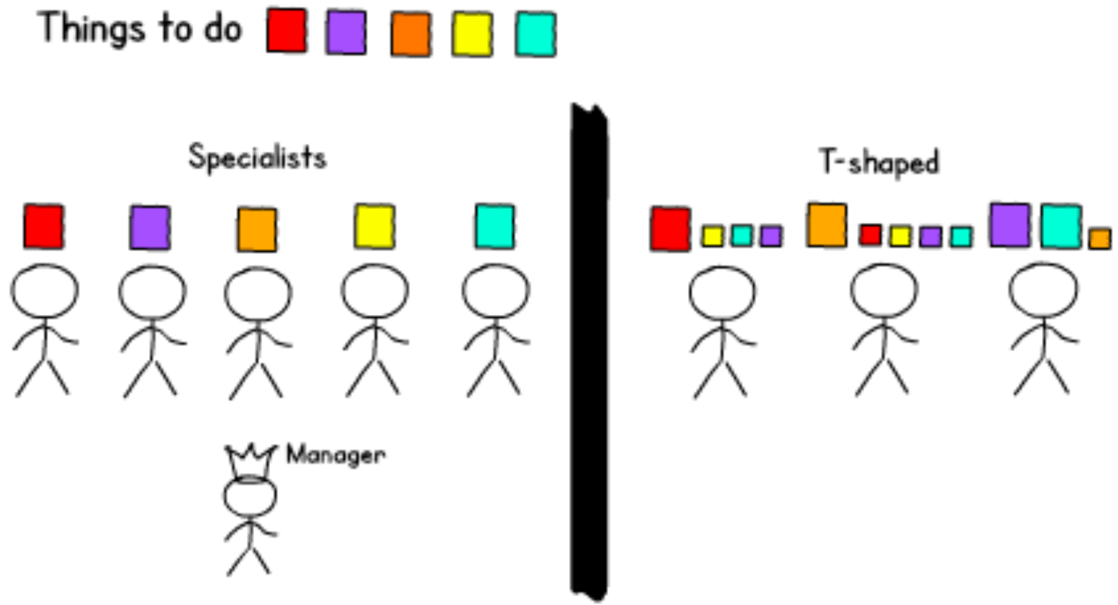
TODAY

HUMANS ARE EXPENSIVE

Role Convergence in Software Development



T-Shaped Professionals for Holistic DevOps



Source: Jason Yip

How Engineers Typically ”Sell” Security

Why should you care about DevSecOps?

Having **DevSecOps practices** (e.g. Threat Modeling) in our organization enables us

FASTER TIME TO MARKET

- Documentation up to date
- Faster Feature Delivery

COST SAVINGS AND REDUCED OPERATIONAL COST

- Lean Security Audits
- Less Bugs and Vulnerabilities

HIGHER CUSTOMER ENGANGEMENT AND SATISFACTION

- Better User Experience understanding

CREDIBILITY AND NEW BUSINESS OPORTUNITIES

- Compliance (ISO 27001, GDPR)

> “**Threat modelling** works to **identify, communicate,** and **understand threats** and **mitigations** within the context of protecting something of value.”

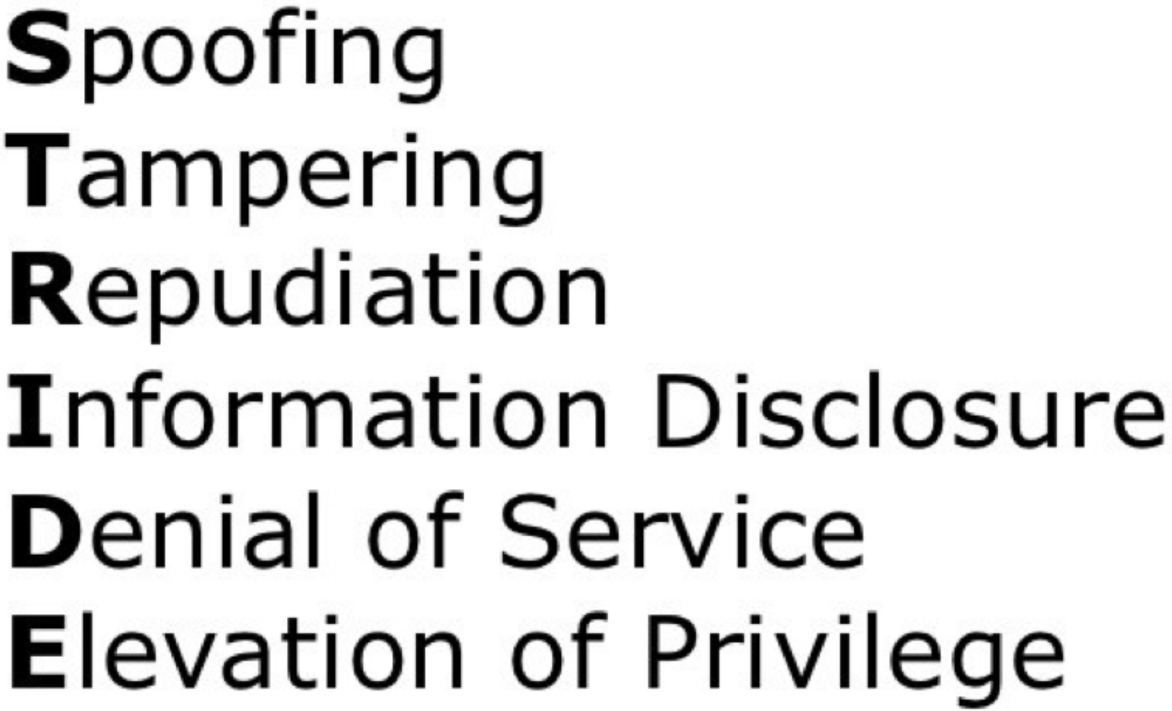
source: owasp.org

Different Methodologies

- **VAST**: Visual, Agile & Simple Threat Modeling
- **PASTA**: The Process for Attack Simulation & Threat Analysis
- **TRIKE**
- **STRIDE**
- …

Threat Modelling

Meet STRIDE



Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privilege

How does it work in practice?

What?

- Architecture or Sequence-Flow Diagram
- Define the Scope of the TM: be strict

Who?

- Facilitator, preferably neutral
- Development team
- Architect
- Product Owner
- Users
- …

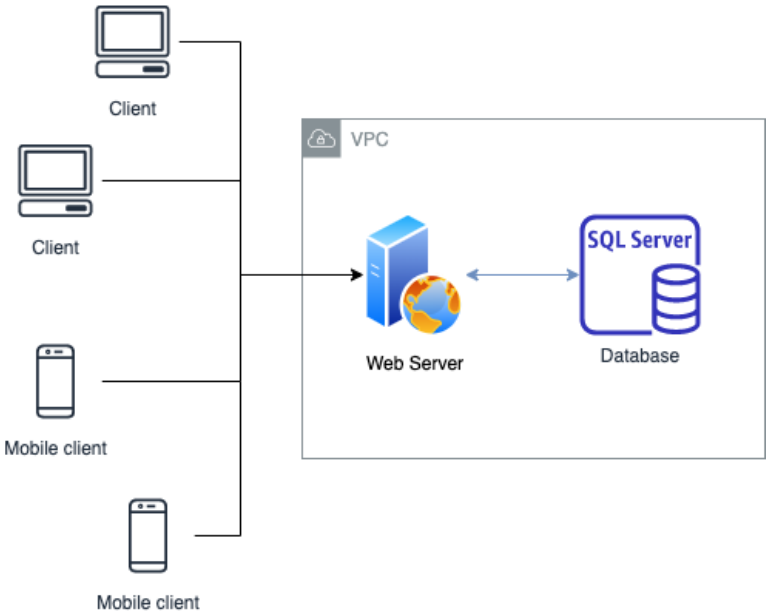
How?

- Format: Workshop
- Duration: 2-4 hours
- Frequency: Every 3-6 months
- **Iterate over STRIDE**

For each term in STRIDE:
Put yourself in an attacker shoes
Exhaust the term before moving to next one

Typical outcomes **Architecture changes, Security measures, Increased validation, Investigate further**

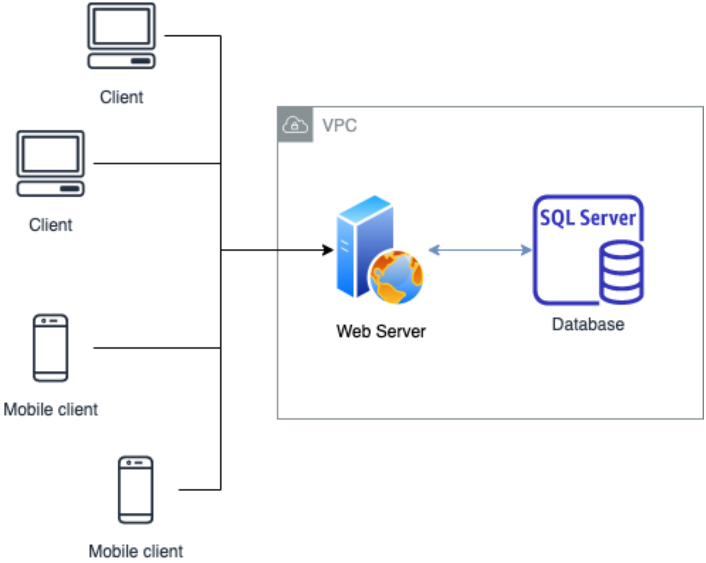
High Level Web Architecture



Source: sketchappsources.com

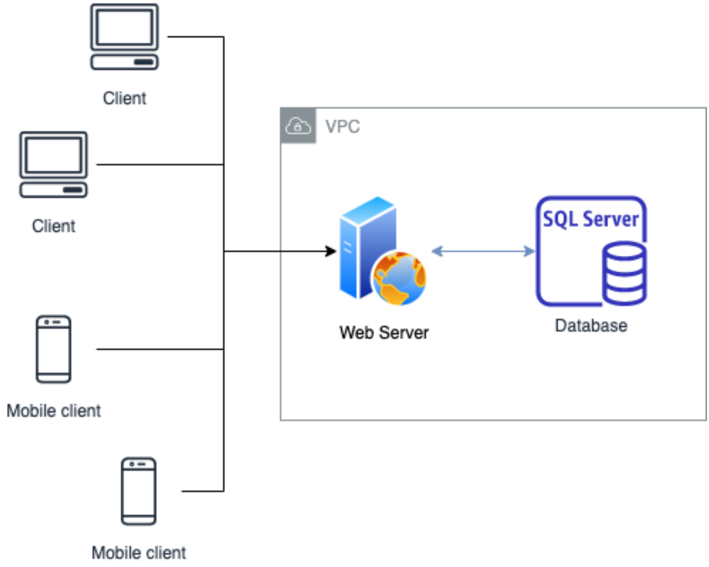
Spoofing

To pretend to be something or someone you are not.



How do you authenticate the user or service?
How do you authorize and validate it?
How could I impersonate other user?
(...)

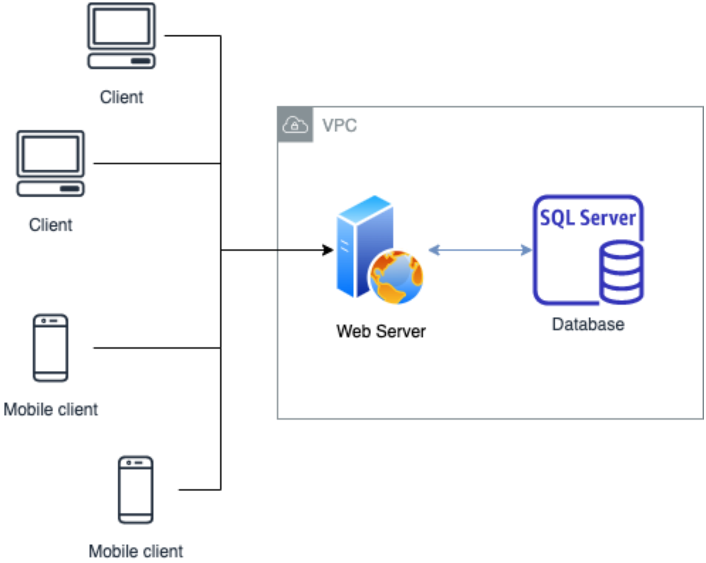
Tampering



To manipulate/change information you are not suppose to.

Can I change other person information?
How could I go around the business logic controls?
Can I change data directly in the database?
(...)

Repudiation

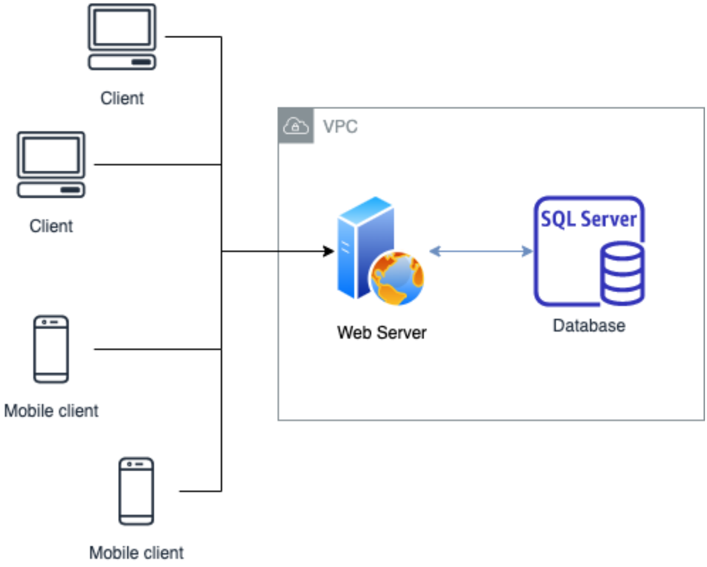


The ability to claim you didn’t do certain actions (no matter if you did or not).

How can you prove user X perform a certain action?
If needed (for auditing or troubleshooting purposes) can you retrace the steps of an user?
(...)

Information Disclosure

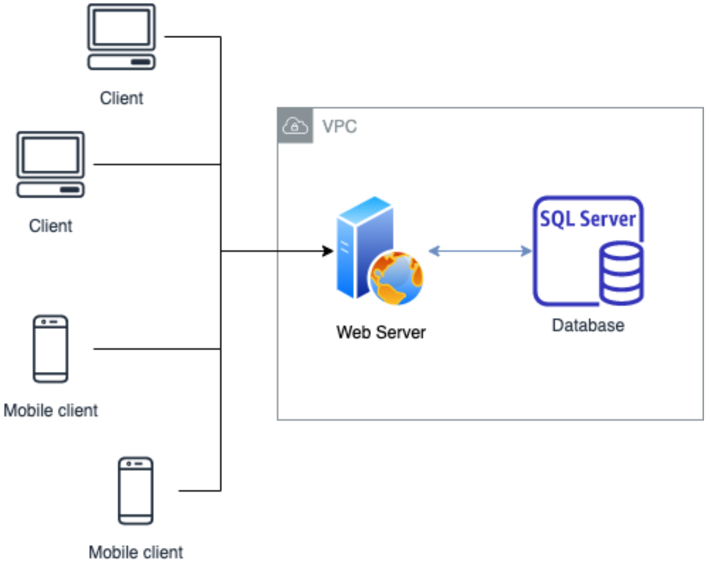
To leak or expose information.



Is the system information sensitive? Why?
What are the risks of unauthorized information exposure to public (or other users within the system)?
(...)

Denial of Service

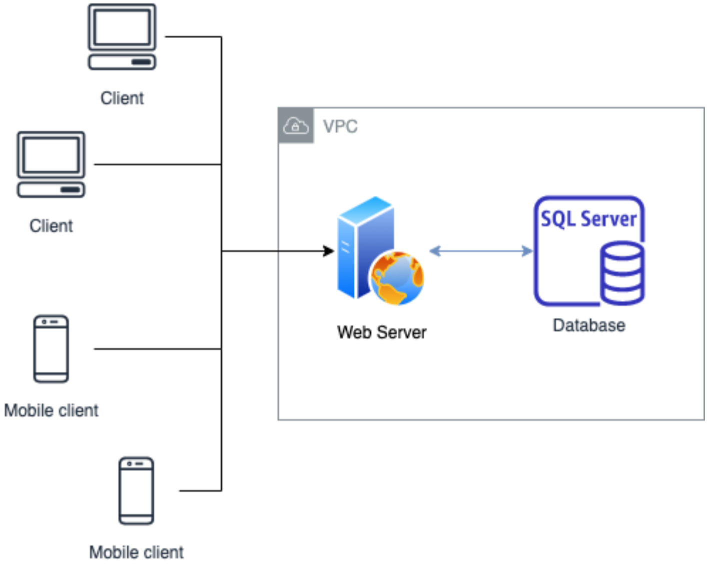
To prevent the system to provide a service.



What is the service(s) the system is providing?
What are the consequences if it gets interrupted?
How likely is that to happen?
(...)

Elevation of Privilege

To gain rights to do things you are not suppose to.



How could an user escalate to gain admin rights?
Can a user with an expired subscription continue to use the service?
(...)

Make it Fun

Elevation of Privilege card game easily and simply helps you define and examine possible threats to software or computer systems.

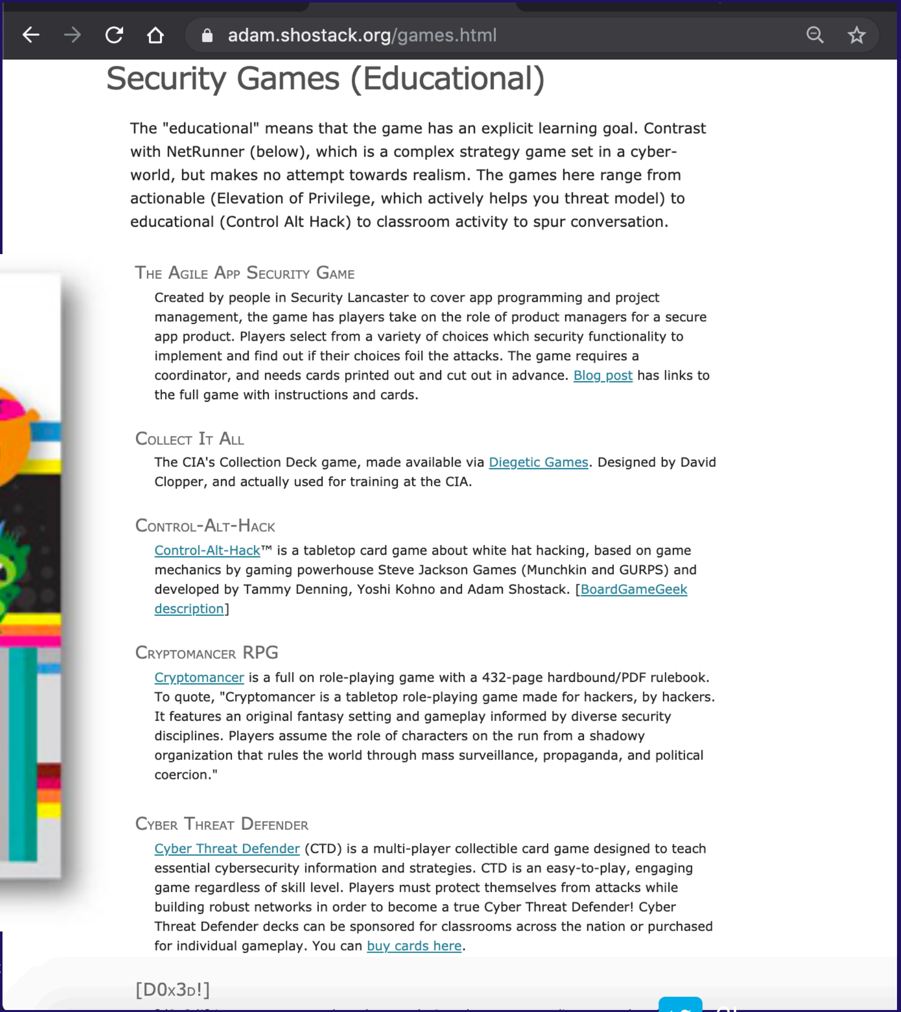
Until now, considering a bunch of possible attacks may have seemed hard to wrap your head around. But through 6 threat groups, EoP keeps you focused on identifying attacks: Spoofing, Tampering, Reputiation, Denial of Service and Elevation of Privilege.

And because EoP encorporates a simple point system, you can challenge other developers and become your opponent's biggest threat.

Includes 84 cards

© 2010 Microsoft Corporation

elevation of privilege
Microsoft
elevation of privilege
Denial of Service
Elevation of Privilege
K
Spoofing
Your system ships with a default admin password and doesn't force a change
Security Development Lifecycle
A Threat Modeling Card Game for Developers



adam.shostack.org/games.html

Security Games (Educational)

The "educational" means that the game has an explicit learning goal. Contrast with NetRunner (below), which is a complex strategy game set in a cyber-world, but makes no attempt towards realism. The games here range from actionable (Elevation of Privilege, which actively helps you threat model) to educational (Control Alt Hack) to classroom activity to spur conversation.

The Agile App Security Game

Created by people in Security Lancaster to cover app programming and project management, the game has players take on the role of product managers for a secure app product. Players select from a variety of choices which security functionality to implement and find out if their choices foil the attacks. The game requires a coordinator, and needs cards printed out and cut out in advance. Blog post has links to the full game with instructions and cards.

Collect It All

The CIA's Collection Deck game, made available via Diegetic Games. Designed by David Clopper, and actually used for training at the CIA.

Control-Alt-Hack

Control-Alt-Hack™ is a tabletop card game about white hat hacking, based on game mechanics by gaming powerhouse Steve Jackson Games (Munchkin and GURPS) and developed by Tammy Denning, Yoshi Kohno and Adam Shostack. [BoardGameGeek description]

Cryptomancer RPG

Cryptomancer is a full on role-playing game with a 432-page hardbound/PDF rulebook. To quote, "Cryptomancer is a tabletop role-playing game made for hackers, by hackers. It features an original fantasy setting and gameplay informed by diverse security disciplines. Players assume the role of characters on the run from a shadowy organization that rules the world through mass surveillance, propaganda, and political coercion."

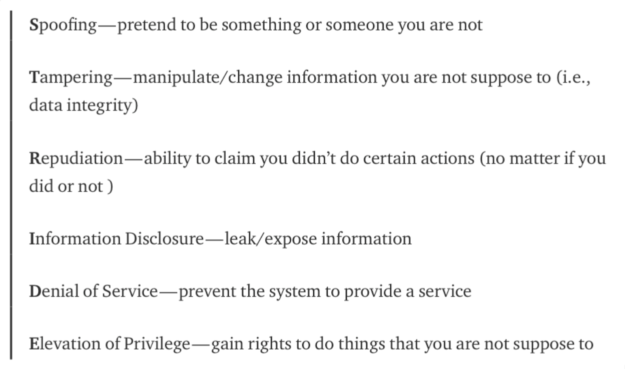
Cyber Threat Defender

Cyber Threat Defender (CTD) is a multi-player collectible card game designed to teach essential cybersecurity information and strategies. CTD is an easy-to-play, engaging game regardless of skill level. Players must protect themselves from attacks while building robust networks in order to become a true Cyber Threat Defender! Cyber Threat Defender decks can be sponsored for classrooms across the nation or purchased for individual gameplay. You can buy cards here.

[D0x3d!]

What is the value you create with this?

- *Security* backlog with all the findings and new work uncovered.
- Architecture and Flow diagrams up-to-date
- Security and Compliance (e.g. PIA for GDPR, PCI DSS, CCPA, etc)
- Alignment within the team
- Enhanced visibility



> **S**poofing—pretend to be something or someone you are not
>
> **T**ampering—manipulate/change information you are not suppose to (i.e., data integrity)
>
> **R**epudiation—ability to claim you didn't do certain actions (no matter if you did or not)
>
> **I**nformation Disclosure—leak/expose information
>
> **D**enial of Service—prevent the system to provide a service
>
> **E**levation of Privilege—gain rights to do things that you are not suppose to

Photo by Ricardo Rocha on Unsplash

@bruno_amaro

futurice

Thank you!
Kiitos!
Danke!
Tack!

BERLIN · HELSINKI · LONDON · MUNICH · OSLO · STOCKHOLM · TAMPERE

Bruno Amaro Almeida

PRINCIPAL ARCHITECT & ADVISOR

Cloud, DevOps, Security, Data Engineering & AI

Reach out on:

@bruno_amaro

@brunoamaroalmeida