x) Threat modelling is a process of analysing a system to find security and privacy issues. It involves asking four key questions: What are we working on? What can go wrong? What are we going to do about it? Did we do a good enough job? This process is crucial for anyone concerned about system security and privacy.

The Threat Modelling Manifesto provides values and principles for effective threat modelling, emphasizing a culture of problem-solving, collaboration, and continuous improvement. The goal is to enhance security and privacy through early and iterative analysis, aligning with an organization's practices, and using dialog and documentation to communicate findings and improvements.

Principles for effective threat modelling:

1. Start early and analyse frequently.

2. Align with development practices.

3. Deliver meaningful outcomes.

4. Prioritize dialogue and documentation.

Beneficial patterns:

1. Follow a systematic approach.

2. Combine creativity with established methods.

3. Include diverse teams.

4. Utilize helpful tools.

5. Apply tested techniques.

Common anti-patterns to avoid:

1. Don't rely on a single hero; involve the team.

2. Move beyond problem analysis to practical solutions.

3. Avoid overfocusing on specific aspects.

4. Use multiple threat modeling representations.

**Shostack 2022:**[**Welcome to the Worlds Shortest Threat Modeling Course**](https://www.youtube.com/playlist?list=PLCVhBqLDKoOOZqKt74QI4pbDUnXSQo0nf)

Ep1 intro, Ep2: Threat model to anticipate problems before they become expensive to deal with this is before any production.

Ep3: 4 questions to know about threat modelling.

Ep4: collaboration in answering what are we working on?

Ep5: sketching to answer what are we working on? to present our ideas to others.

Ep6: We need to keep records of things discussed in the threat model.

Ep7: Data flow diagrams in threat modelling, symbols: external entities (pointy corners) processes (little drums), data flows, data stores

Ep8: what can go wrong? Express concerns.

Ep9: Add structure to answer questions. Mnemonic STRIDE.

Ep10: What are we going to do about it? track the set of threats we discussed in answering what can go wrong?

Ep11: Risk management in relation to what we are going to do about it.

Ep12: A way of answering did we do a good job?

**Chapter 1Dive In and Threat Model!**

Threat modelling is a skill that anyone can and should learn. It involves using models to spot security problems, collecting away details to see the bigger picture. This helps find issues in things that haven't been built yet and prevents issues from occurring. It's a practical discipline, focused on gaining experience rather than theory. Like learning to play an instrument, it may be difficult at first, but with lots of practice, it becomes easier and more effective.

1. - Basic security hygiene includes using strong passwords and enabling 2FA.

* Updating software on devices.
* Avoiding clicking on scam like links because it might be phishing
* Securing Wi-Fi,
* Backing up data.

For instance, setting up and managing a personal firewall or configuring advanced privacy settings on certain devices might be considered above the average Joe’s skill level.

1. Make-belief boogie-man - a threat model for imaginary company.

What are we working on?

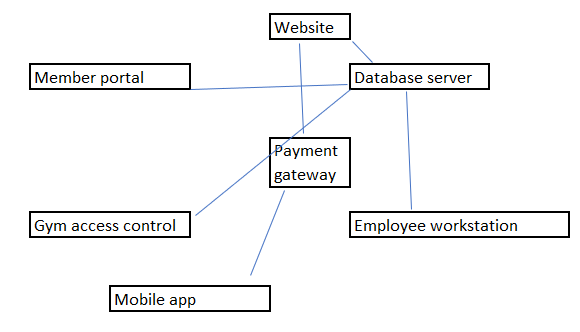
Gym-Tikkurila is an imaginary fitness company that provides various fitness classes, wellness services and products to its members. It operates a single gym and offers personalized training programs, health assessments, and dietary guidance to its customers through its personal trainer program. Gym-Tikkurila Oy collects and stores customer health data, including medical history, fitness goals, and workout routines, as part of its services. Key assets include:

Customer Health Data: This is one of the most important assets. It includes sensitive information like medical records, fitness assessments, and dietary preferences. Unauthorized access or breaches of this data could result in terrible legal and reputational consequences.

Financial Data: Gym-Tikkurila processes payments for memberships and services, storing financial data such as credit card information. Any compromise of this data could lead to financial loss and legal problems.

IT Infrastructure: The company relies on a network of servers and databases to store and process customer data, schedules, and payment processing.

**Gym-Tikkurila Company Diagram:**



Gym-Tikkurila IT infrastructure consists of several interconnected components:

Member Portal: A web application where customers can book and sessions, view fitness plans, and provide health information.

Database Server: Stores customer data, membership details, and financial records.

Payment Gateway: Handles transactions securely.

Gym Access Control System: Controls access to gym facilities based on membership status.

Employee Workstations: Used by staff for managing customer accounts and schedules.

Mobile App: Allows customers to access services and make reservations from their smartphones.

**2. What can go wrong?**

To assess potential threats, we'll apply the STRIDE model:

Spoofing: Attackers could impersonate gym employees or members to gain unauthorized access to systems and data.

Tampering: Data integrity could be compromised if an attacker changes customer records or payment information.

Information Disclosure: Sensitive customer health data or financial information could be exposed.

Denial of Service (DoS): Attackers might disrupt services, preventing members from accessing the gym schedules and online services.

Elevation of Privilege: Unauthorized users could increase their privileges to gain administrative access to systems.

**(3) What are we going to do about it?**

Gym-Tikkurila faces security risks like data breaches, payment fraud, and service disruption. To mitigate these, we'll implement strict access controls, limit entry points, update software, and provide security training.

(**4) Did we do a good enough job?**

We'll also use encryption, intrusion detection, and conduct regular audits. Continuous evaluation and incident monitoring are key. Our focus is on safeguarding customer data and financial information to comply with regulations and build trust.