# Security Lab

## Threat Modeling 101

General strategy, scoping, data flow diagrams

ROTTERDAM UNIVERSITY OF APPLIED SCIENCES

# Agenda

Exercise

Guiding principles

Mapping a system

Attack exercise

# Definition

**Threat modeling** is the process of determining vulnerabilities within any given environment, depending on the present threats to the environment and the assets you are protecting.

Having a complete and clear overview of the system you are protecting/attacking is required for a comprehensive threat model.

# Let’s get straight into an exercise (15 mins.)

In the next slide you will find a simple map from a bank.

You are a back robber and wish to rob this bank.

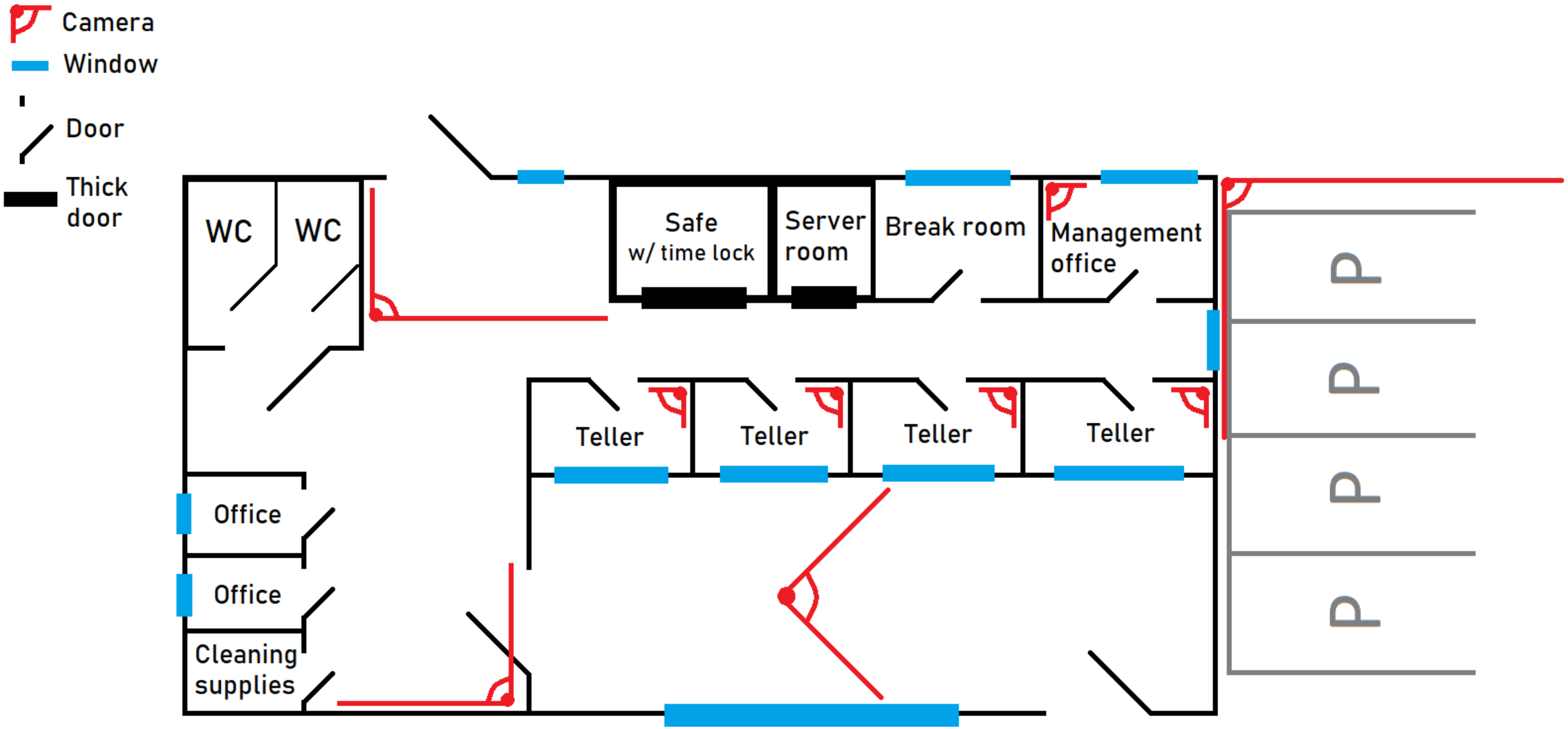
What is your plan? **Prepare a plan of attack**.

Rules:

You want to escape, alive.

You are a bank robber, not a murderer.

Any additional laws you violate will increase the heat from the police.


Camera
Window
Door
Thick door
WC
WC
Safe w/ time lock
Server room
Break room
Management office
Teller
Teller
Teller
Teller
Office
Office
Cleaning supplies
P
P
P
P

# How did you tackle it?

What kind of information would you have liked to have?

- More reconnaissance!

# Questions to ask yourself

**What** assets are you protecting?

**Where** are they located?

**Why** are they valuable?

**Who** could be potential attackers?

**How** would the attacker accomplish their goals?

Now, knowing the answers to these questions:

How would you prevent this, or minimize damage?

# Securing a building is easy

Most components and data flows in an IT system are hidden from view.

**What** are the assets?

**Where** are they stored?

**Why** are they valuable?

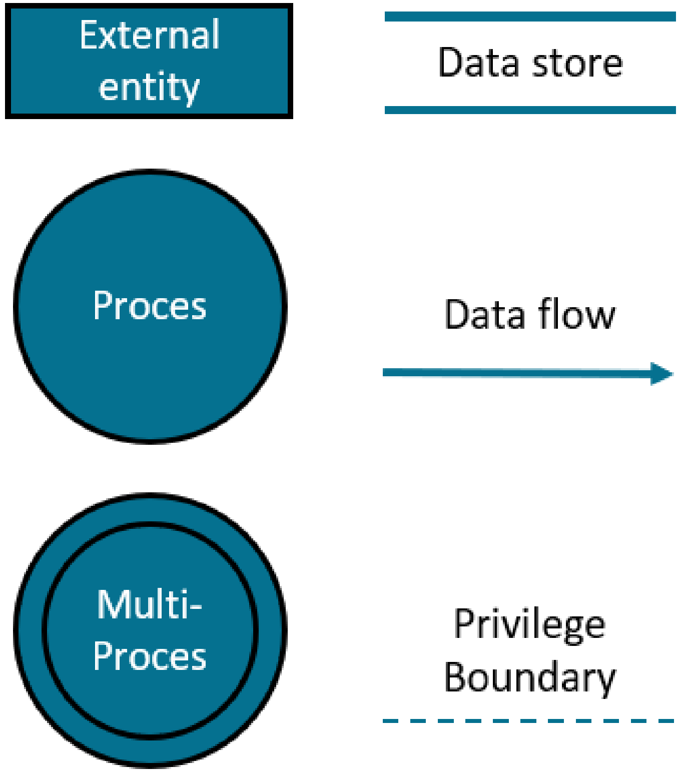
**Who** could be potential attackers?

**How** would they attack your system?

- What kinds of users are there, and how do they interact with the system?
- What kinds of information are requested/returned/sent between components?
- Where are the *trust boundaries* in your system?
- ...

A common way to depict this is in a **Data Flow Diagram**.

# Basic composition of a DFD



External entity

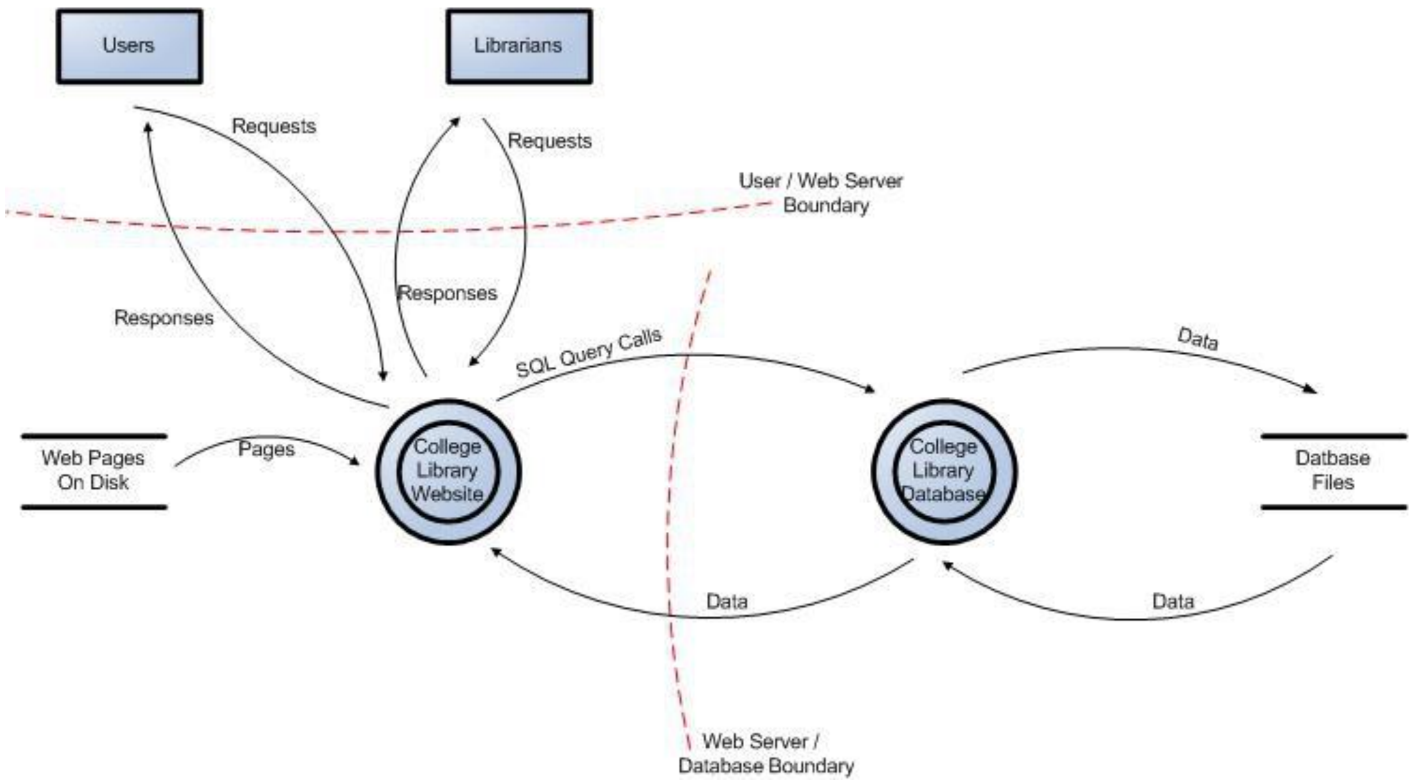
Data store

Proces

Data flow

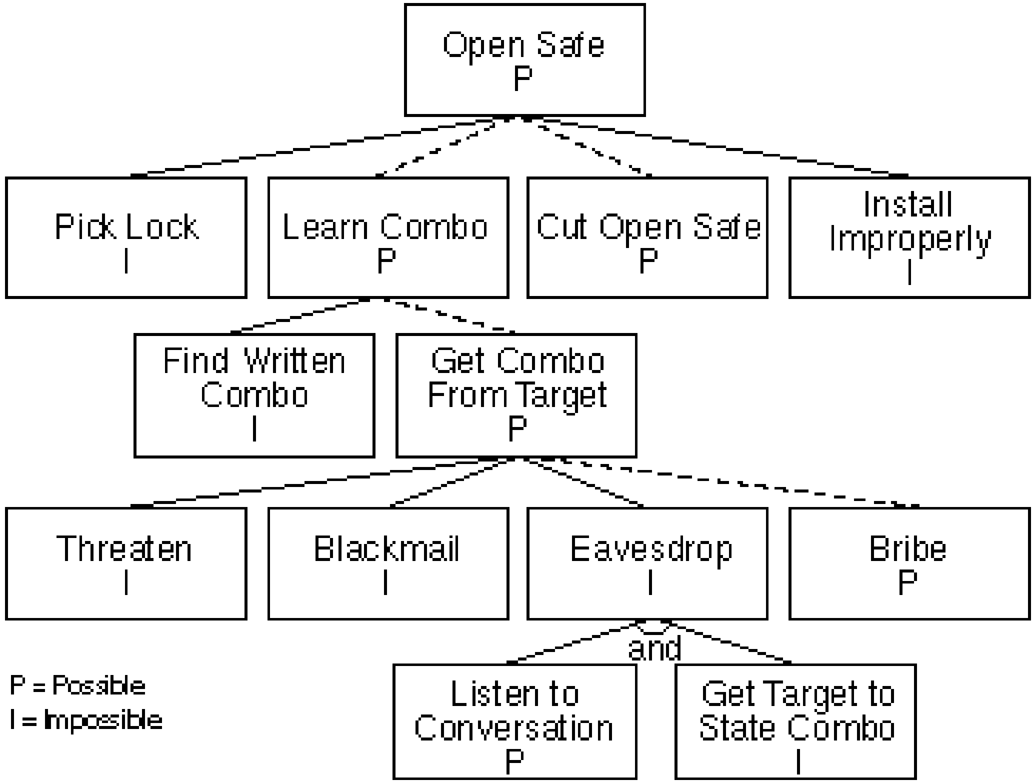
Multi-Proces

Privilege Boundary



# What can you see in the overview?

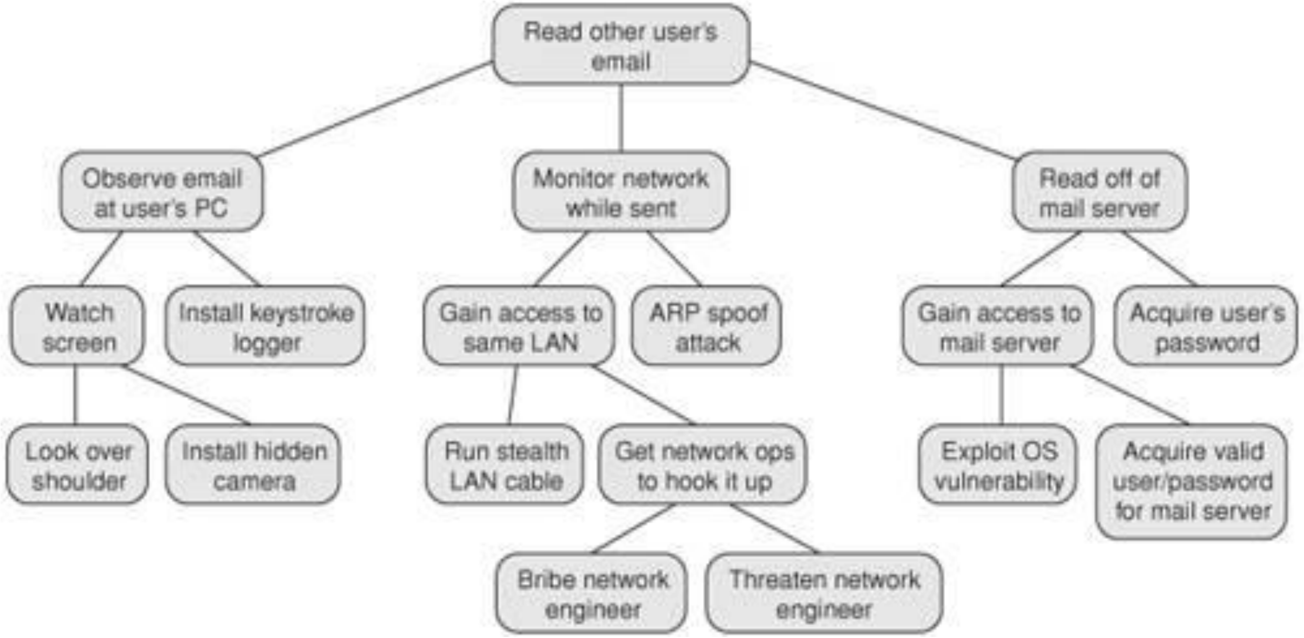
- **How** can it be attacked?
- We can identify attack vectors in **attack trees**



# What can you see in the overview?

- **How** can it be attacked?

- We can identify attack vectors in **attack trees**



# Recap

Ask yourself: **who** wants to attack **what**, **where**, **why**, and **how**?

Help answer these questions by making a Data Flow Diagram.

Try to get as specific as you can answering the **how.**

If you are missing crucial information: do more reconnaissance!

# Homework

**Team:**

- Find a free and open-source application to analyze for project 0: Code Review.

**Agenda for tomorrow**

- Threat modeling 102
    - Some frameworks to help with threat modeling & risk assessments
    - Finding specific threats: STRIDE
    - Risk assessment: DREAD & CVSS

# Further reading for inspiration

A Guide to Threat Modelling for Developers

- ➢ More development focused, but the general idea is the same.

OWASP Threat Model Cookbook

- ➢ A repository of threat modeling examples.

Speaking of OWASP: here is a Threat Modeling Cheat Sheet!

ROTTERDAM UNIVERSITY
OF APPLIED SCIENCES

**exceed** expectations