Security Lab
Threat Modeling 102

Threat discovery and risk-assessment

ROTTERDAM UNIVERSITY OF APPLIED SCIENCES

Agenda

Recap of yesterday

Threat discovery: STRIDE

Ranking vulnerabilities by severity: Dread & CVSS

Recap: WWWWH

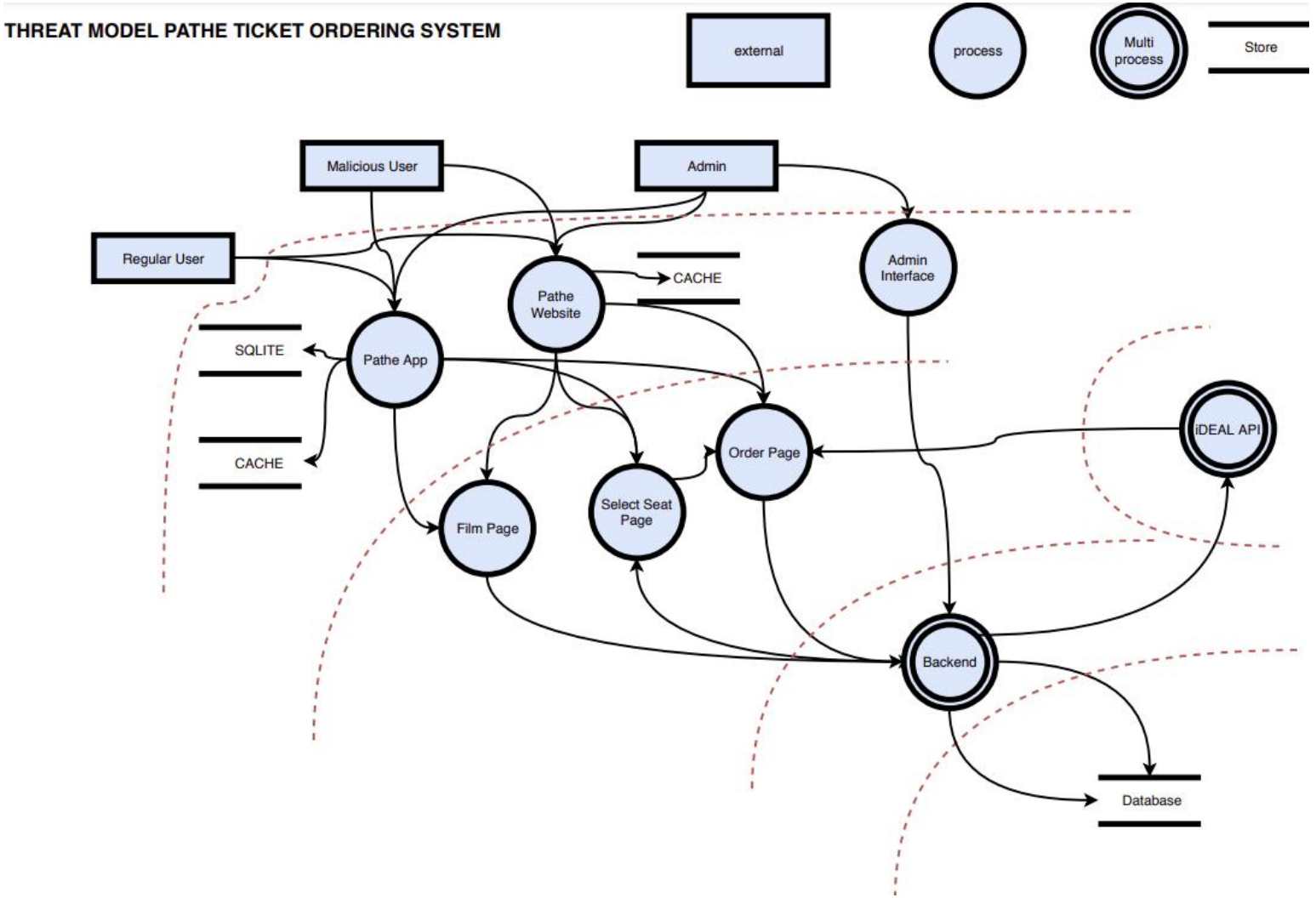
Ask yourself: **who** wants to attack **what**, **where**, **why**, and **how**?

Help answer these questions by making a Data Flow Diagram.

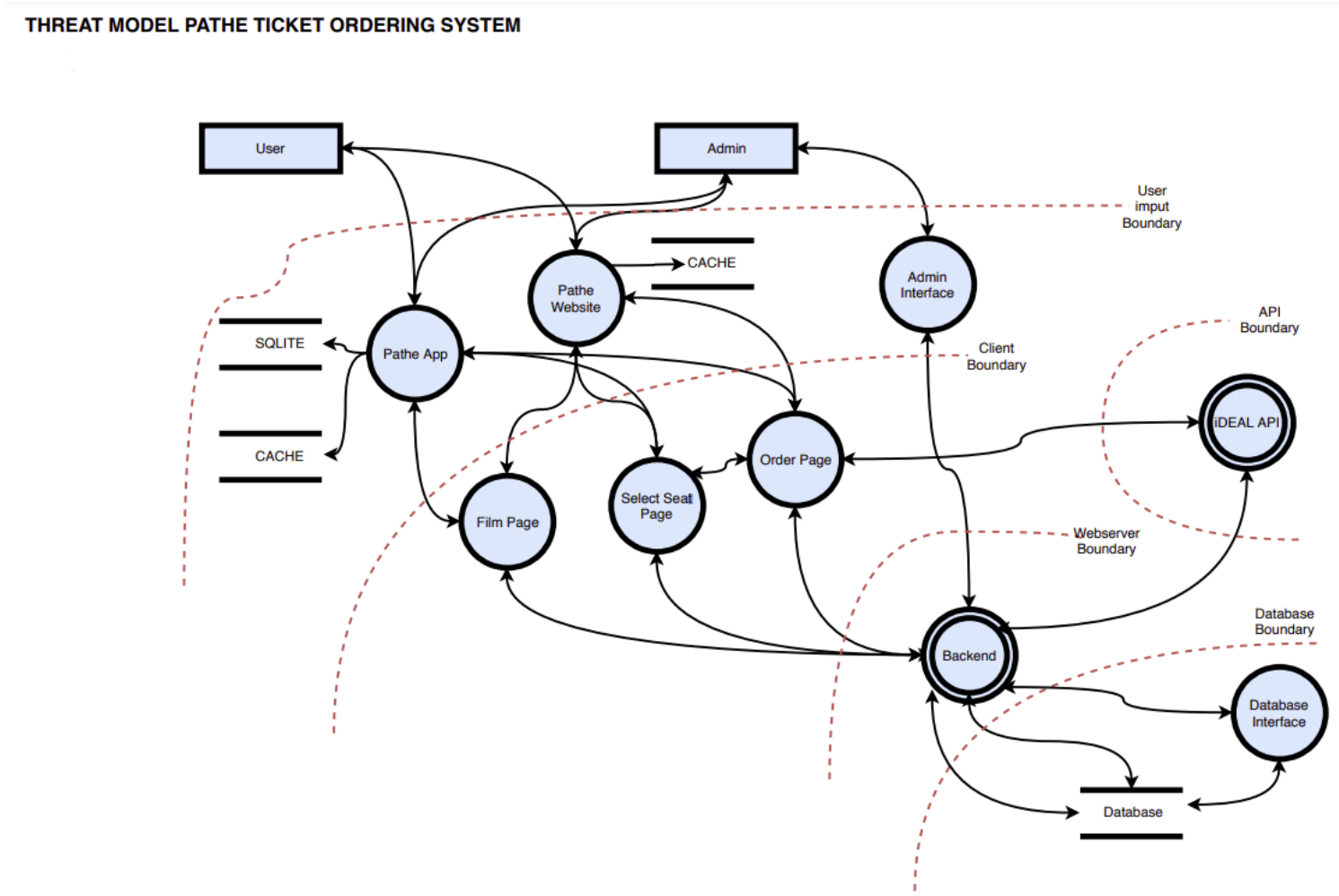
Try to get as specific as you can answering the **how**, using the information you have.

If you are missing crucial information: do more reconnaissance!

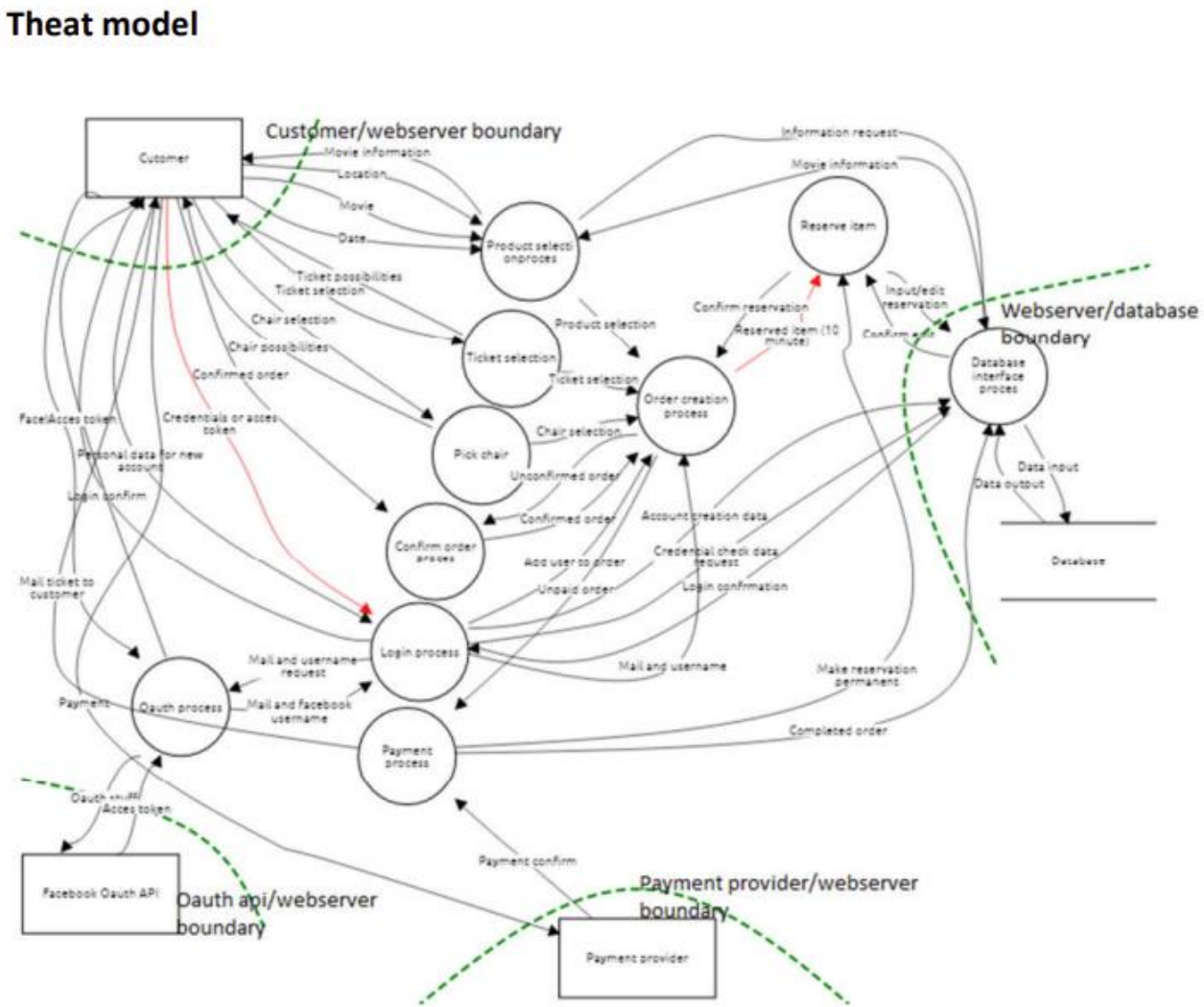
Recap: Data Flow Diagrams



Recap: Data Flow Diagrams



Recap: Data Flow Diagrams



What to look for and where?

Threat modelling an IT system is harder than threat modelling a physical object/building.

The nature of possible threats is completely different

STRIDE can help with that.

STRIDE

An acronym to help you with the most common classes of threats

Based on the desirable infosec properties we discussed earlier

You need to have a coherent overview of your application first(Data Flow Diagram).

Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

STRIDE

For each aspect there are several possible threats

For instance: You can spoof a person, a device, data, etc.

- Spoofing a person can be done by catfishing, or account hijacking.
- Spoofing a device can be done with DNS-poisoning, MAC-address spoofing, Evil Twin attack etc.

STRIDE makes it easier to answer yesterday's **How** question.

- And subsequently, makes attack trees easier to make

Risk modeling

Classification

You've found multiple vulnerabilities and hand over the report to management. Great!

"So, what the hell am I supposed to do with this technical mumbo jumbo?!"

- Mr. CEO

We need a way to clearly communicate the risk of specific vulnerabilities to stakeholders and STRIDE doesn't quite cut it.

DREAD

- **(D)amage**
- **(R)eproducibility**
- **(E)xploitability**
- **(A)ffected users**
- **(D)iscoverability**

- Provides a simple scoring scheme for specific vulnerabilities based on five properties.
- DREAD_SCORE = (D + R + E + A + D) / 5
  - Where each is scored 0-10
- E.g.: Damage
  - 0 = no damage, 5 = select (non-private) user data compromised/affected, 10 = full system pwnage

DREAD

Pros:

Very simple to use

Quantitative output (0-10) makes it easy to understand

Cons:

Small differences in scores don’t mean much (what is a 7 vs. 8 in Damage?).

Difficult to determine individual components that contributed to final score.

Not an objective scoring mechanism at its core.

You can use DREAD calculator if you need one.

CVSS

Common **V**ulnerability **S**coring **S**ystem v3.1

Rapidly becoming the de-facto standard vulnerability risk classification.

Gives a score and specifies how it calculated that score(vector).

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L/CR:H/IR:H/AR:H/MAV:N/MAC:H/MPR:N/MUI:N/MS:C

Composed of three metric groups

- **Base**: fundamental characteristics of the vulnerability, independent of time or user
- **Temporal**: can change over time (e.g. exploit maturity, report confidence)
- **Environmental**: dependent on user environment

CVSS

Fairly complex to use compared to DREAD

- Using online calculators does simplify things.

Doesn’t require all fields to be used

- Default values are assumed for empty fields

E.g.: Base - Attack Vector

- (N)etwork: attacker does not require local access (remotely exploitable)
- (A)djacent: attacker is limited to logically adjacent topology (at a protocol level)
- (L)ocal: attacker not bound to the network stack (local access or SSH, for example)
- (P)hysical: attacker needs physical access

CVSS specification can be found here

CVSS Vulnerability assessment

A vulnerability is found in Osiris, the student and grade management system of the RUAS, that enables an attacker to insert code in an input field that gets executed on the server serving the webpage of Osiris.

Calculator

CVSS Vulnerability assessment

Base Score — **9.9 (Critical)**

Attack Vector (AV)

- **Network (N)**
- Adjacent (A)
- Local (L)
- Physical (P)

Attack Complexity (AC)

- **Low (L)**
- High (H)

Privileges Required (PR)

- None (N)
- **Low (L)**
- High (H)

User Interaction (UI)

- **None (N)**
- Required (R)

Scope (S)

- Unchanged (U)
- **Changed (C)**

Confidentiality (C)

- None (N)
- Low (L)
- **High (H)**

Integrity (I)

- None (N)
- Low (L)
- **High (H)**

Availability (A)

- None (N)
- Low (L)
- **High (H)**

Vector String -
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Threat modeling from A to Z (Recap)

Create a clear and detailed overview of the application you are testing

- E.g.: **Data Flow Diagram**
- Answer the **what**, **why**, **where**, **who**, and **how**

Create attack trees to predict an attacker's steps

- **STRIDE** can help with this

Rank the risks by severity

- Quick 'n' dirty: **DREAD**
- In-depth: **CVSS** (be sure to specify the version you're using!)

Further resources

Interesting links that can help:

CVSS 3.1 specification

Microsoft on threat modelling for drivers

- A nice compilation of all the frameworks mentioned in a real (low-level) example

OWASP Threat Dragon

- “OWASP Threat Dragon is a tool used to create threat model diagrams and to record possible threats and decide on their mitigations.”
- Online- and desktop versions available

Exercise assignment

CoronaMelder application

The assignment

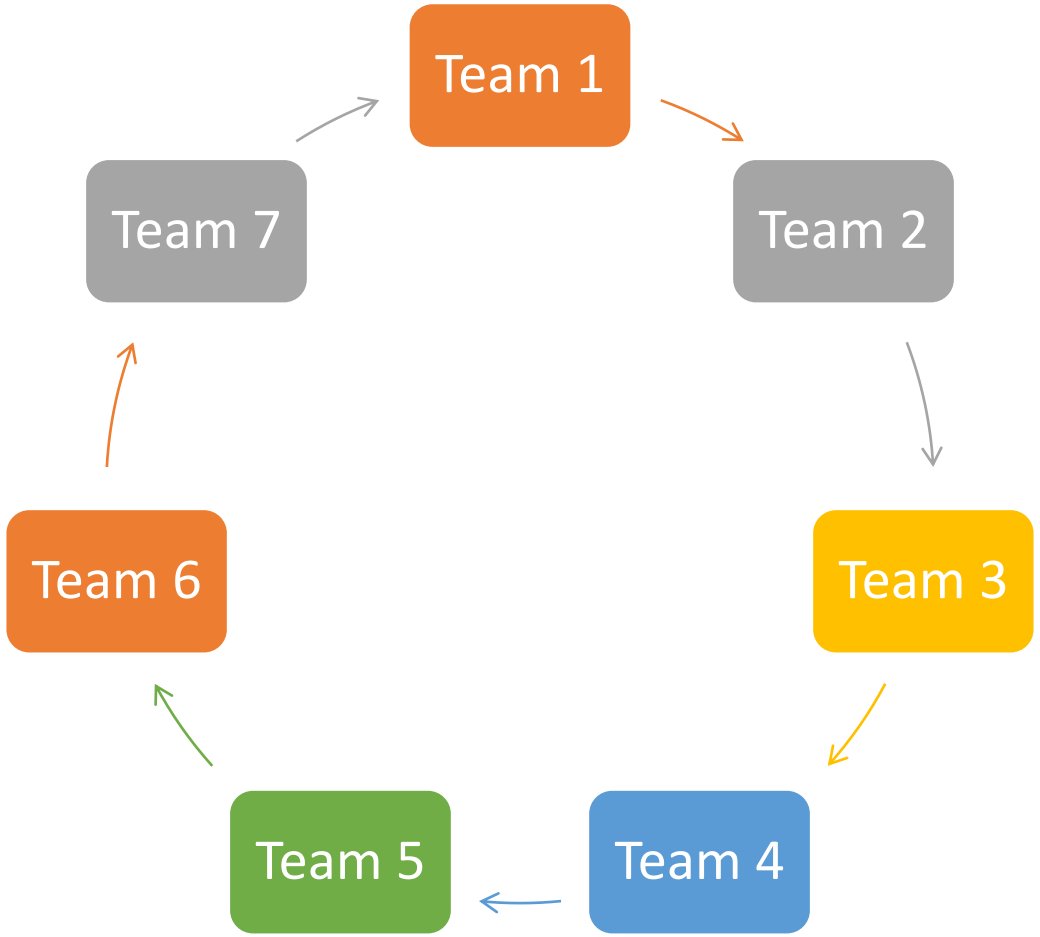
Per team, make a threat model of the CoronaMelder app by the Dutch Government based on the available documentation. The report must at least include:

- 2x Data-flow diagram
- Documented threats using STRIDE
- 5 attack trees of different scenarios(individual, 1 per team member)

If you want feedback on your work, turn it in by Sunday the 12th of September 23:59 together with written peer group feedback.

This is a practice round for the Code Review project.

Cross-team peer evaluation



The assignment no.2

Find a suitable name for your team. Starting tomorrow you will be operating under that name as though you were a start-up cyber security company.

Rules:

- Nothing offensive
- Keep it civil
- Easter eggs / references / jokes allowed but consider rule 1 and 2.

ROTTERDAM UNIVERSITY
OF APPLIED SCIENCES

exceed expectations