Network and Web Security

# Tutorial 1: Threat Modeling[*]

January 18, 2021

## Question 1: Identifying risks

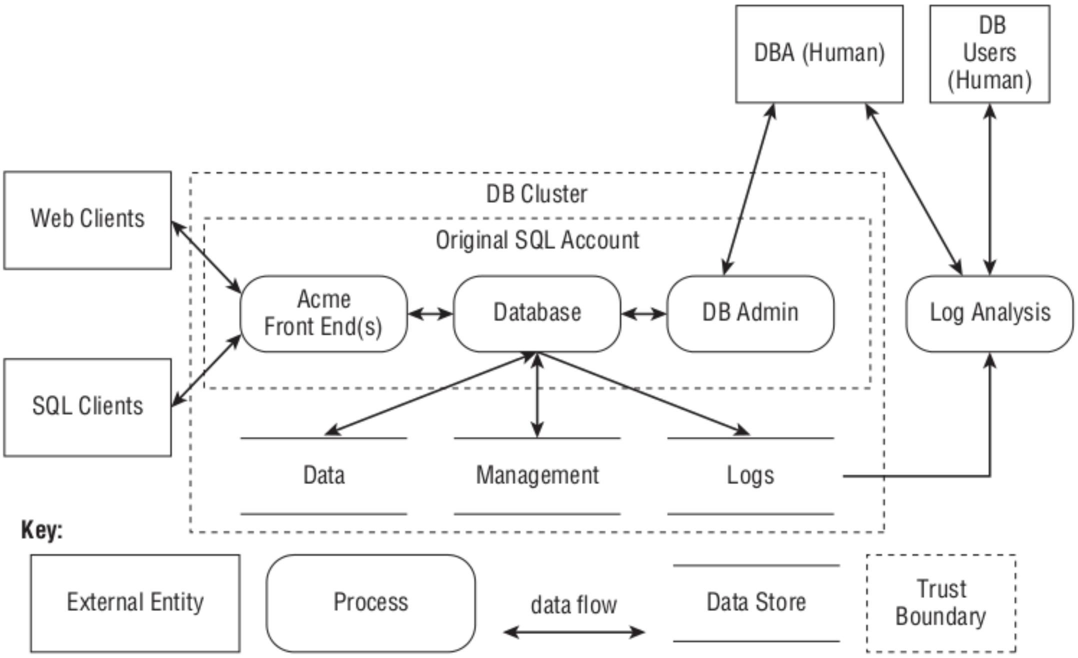
Below is a data flow diagram for Acme, an online retailer.

(a) From this diagram, identify three risks that Acme might face. (Hint: risks occur when data crosses trust boundaries.)

(b) Assign each of the risks you have identified to appropriate **STRIDE** categories:

| | | |
|---|---|---|
| **S**poofing | **T**ampering | **R**epudiation |
| **I**nformation disclosure | **D**enial of service | **E**levation of privilege |

(c) Propose two methods of addressing each risk you have identified.



Adam Shostack, *"Threat Modeling: Designing for Security"*, Wiley, 2014.

[*] Thanks to Chris Novakovic `c.novakovic@imperial.ac.uk` for preparing this material.

## Question 2: Attack trees

Your goal is to gain access to a building. Draw an attack tree for achieving this goal.

A good attack tree should list a comprehensive range of actions that directly or indirectly contribute to achieving the goal. To get started, you may want to structure your attack tree in the following way:

- Your goal is to gain access to the building. This should be the root element in your attack tree.
- Identify the ingress points of the building. Gaining access to the building via any of these could be the first tier of your attack tree.
- For each ingress point in the first tier, identify the states that the ingress point could be in (if appropriate); they might be secure states, or insecure states. Gaining access to the building while the ingress point is in one of these states could be the second tier of your attack tree.
- For each of the states in the second tier, consider how the ingress point being in this state helps you achieve your goal: if the ingress point is in a secure state, how can you put it into an *insecure* state? If it's already in an insecure state, under what circumstances could it be in that insecure state? The actions necessary to ensure the ingress point is in the given state could form the third tier of your attack tree.
- Keep going! For each tier, create new child tiers for conditions that need to be met in order to achieve the goal in the parent tier.