Creating a Threat Model

Imagine Acme Inc. has won a contract with the Government of Norway to design and develop a Voting System to assist with electronic voting and prevent voting fraud. The system is made-up of 4 components:

1. Database (Using MySQL)

2. Backend Server (Using Java)

3. Admin Client (Using Java)

4. Voting Client (Using Java)

Database:

The database is behind the Government's Firewall and only Acme's Backend Server will be able to communicate with it. Assume that the database is inside a private network with only itself and the backend server as the nodes in this private network.

Backend Server:

The Backend Server allows us to do the following:

1. Authentication

- Allow Voting Client users (Citizens) to authenticate
- Allow Admin Clients (local government officials) to authenticate

2. Authorization

- Allow Voting Clients to vote on measures and candidates
- Allow Admin Clients to upload Measures and Candidates

Admin Client:

For simplicity we will have two levels of Admins.

1. Election Admin

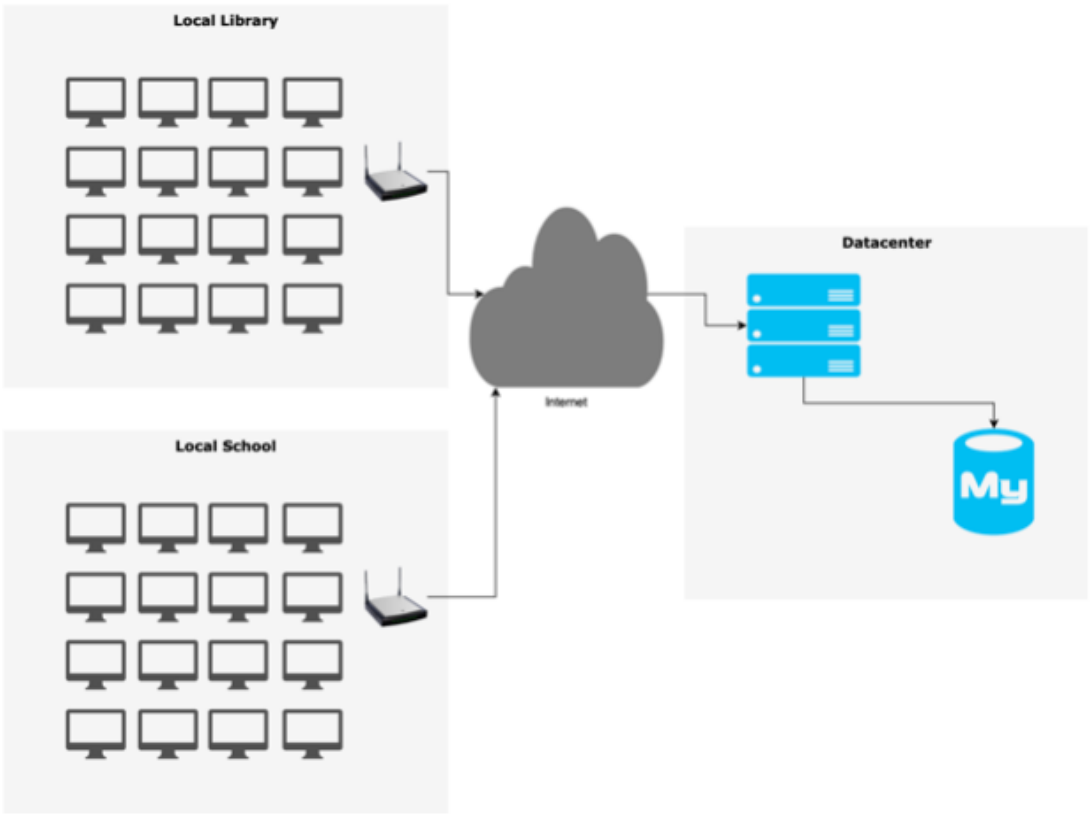
Election admins can run reports: See the result of election thus-far – (e.g. how many individuals have voted for measure 3)

2. System Admin

- Can enable and disable user accounts
- Run sanity checks to make sure the database has not been tampered with

Voting Clients

Voting Clients provide a portal for citizens to vote. They will have the ability to answer multiple choice questions and submit their results. Voting Clients also have the ability to login after voting and ensure that their vote has not been tampered with. See architecture diagram *(Design Document and System Architecture Requirements, Courtesy of: Joubin Jabbari)*.



STRIDE model

The STRIDE model categorizes different types of threats and simplifies the overall security conversation.

Category	Description
Spoofing	Involves illegally accessing and then using another user's authentication information, such as username and password
Tampering	Involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet
Repudiation	Associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-Repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package
Information Disclosure	Involves the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers
Denial of Service	Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability
Elevation of Privilege	An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed

Review criteria less

You will create a threat model of a voting application that has been designed by Acme Inc. The design details are outlined below. They require to see a diagram. You will submit a PDF of your work that can be a screenshot of your Google Docs, Microsoft Word, or Paint drawing, with the following details:

The diagram is a system diagram of the components of the whole system. This system diagram should include:

- Backend database
- Web server
- A client

It also needs to include:

1. Arrows showing how the data flows between each component, e.g The data-flow diagram overlayed on top of the system diagram.
2. Included in the diagram, show the trust boundaries, as dashed lines.
3. A description of possible STRIDE threats. Please come up with at least three different threats from the STRIDE acronym. e.g) Spoofing, Tampering, and Repudiation

So that it is easy to distinguish parts of your diagram, please include a legend, like the following: