Voting System Threat Model

Name: Yengkong Sayaovong
Date: September 6th, 2024

Executive Summary

This document provides a threat model for a voting application designed by Acme Inc. The voting system consists of four components: the Backend Server, Database (MySQL), Admin Client, and Voting Client. The system enables authentication, authorization, and voting capabilities. This document identifies potential threats based on the STRIDE framework: Spoofing, Tampering, and Repudiation. A diagram depicting the system architecture, data flow between components, and trust boundaries is included to illustrate the flow of data and potential security vulnerabilities. By assessing these risks, Acme Inc. aims to enhance the security posture of the electronic voting system.

Data Flow Diagram

The following diagram illustrates the data flow between the major components of the voting system, which include the Backend Server, Database (MySQL), Admin Client, and Voting Client. The dashed lines represent trust boundaries. The arrows between components show the flow of authentication data, vote data, and administrative actions.

Components:

1. Backend Server
2. Database (MySQL)
3. Voting Client (Citizens)
4. Admin Client (Government Officials)

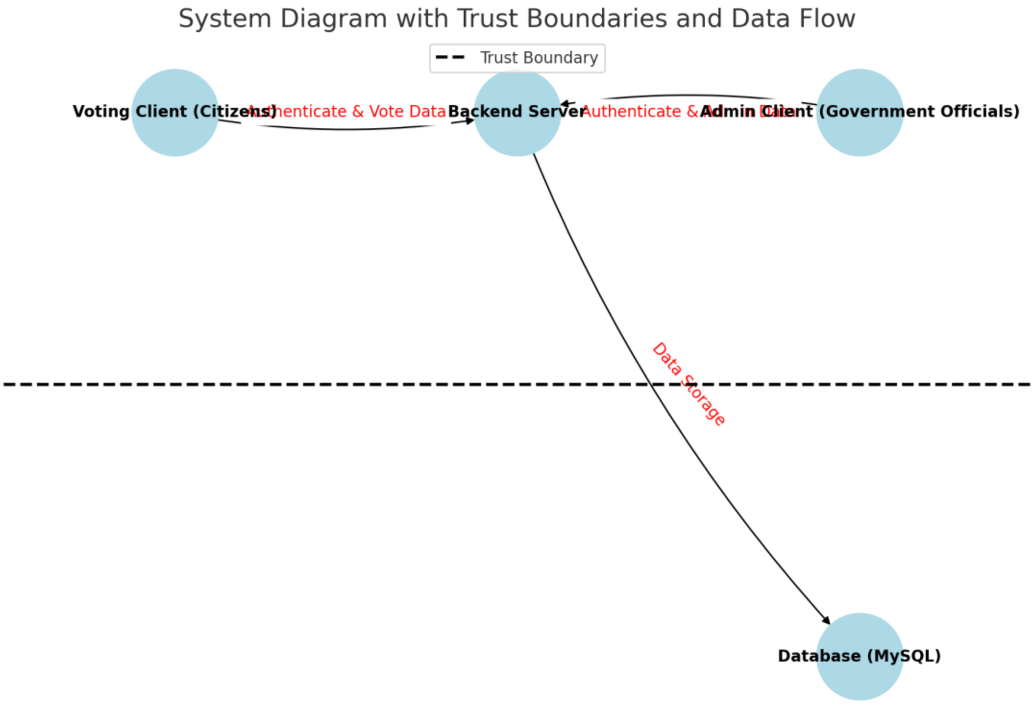
Data Flow:

- Voting Clients send authentication and voting data to the Backend Server.

- Admin Clients send administrative data to the Backend Server.

- The Backend Server interacts with the Database (MySQL) for data storage.

- The Database is behind a firewall, and only the Backend Server has access.


System Diagram with Trust Boundaries and Data Flow
Trust Boundary
Voting Client (Citizens)
Authenticate & Vote Data
Backend Server
Authenticate & Admin Data
Admin Client (Government Officials)
Data Storage
Database (MySQL)

References

1. STRIDE Framework: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.
2. Acme Inc. Voting System Architecture Design Document.
3. NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations.