# Secure E-Voting System Design

## Assets

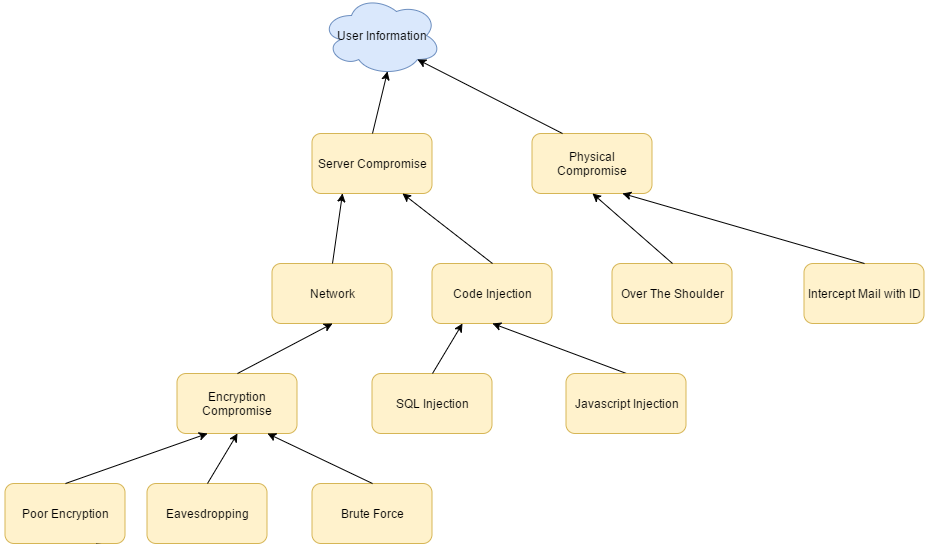
1. Votes - We need to protect the integrity of the actual vote. That each vote is counted once and only once.
2. Voter Information - We need to protect the private information that is used to create an account (special government ID, name, etc.)
3. Voter Anonymity – We need to protect the anonymity of the voters; the system should not be able to tell who voted for what.

## Stakeholders

1. Voters
2. Nominees up for election
3. Government hosting the election
4. Citizens (that can be affected by vote outcome)

## Adversary Model

### Attack Tree (Snippet)



(See Attack Tree.png for full attack tree)

### Potential Adversaries

In our system everyone is a potential adversary.

* Outside adversaries could want their votes to be counted more than once.
* Inside adversaries could want some votes not to be counted.
* Passive adversaries could be listening to observe who votes for what.
* Active adversaries could be attempting to make extra or invalidate votes.

Note: For the scope of the project we are assuming that the server is trusted, and that it is performing transactions accurately.

## Previous Research

* Estonian model- Voters are assigned a unique ID and a voter smart card that allows for both “secure and remote authentication and legally binding digital signatures by using the Estonian state supported public key infrastructure.”[1]

## Overall Design (Basic)



## Database Design

* The system will include 4 different databases, each at a different physical location.
* Each database will have a unique administrator, and each administrator will have the **only** access to these secure databases.
* Each administrator will be fully vetted and require security clearances and background checks to ensure secrecy.

### Voter Database

* The voter database will include a pre-populated list of every registered voter.
* This is the main entry point for the e-voting system.
* This database will include every registered voter ID (unique ID that was previously communicated to each registered voter via physical mail or other secure means)
* Upon logging in, the voter ID must match the hashed password.
* After logging in, the voter will submit their ballot.

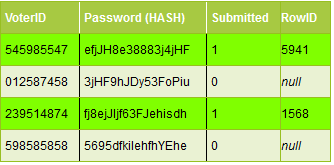
Upon a ballot submission:

1. The flag is marked “true” in the ‘submitted’ column.
2. A unique ID (‘row ID’) is created and entered into the Voter database. This same ID will be entered into the Vote database.
3. The ballot contents (votes for candidates and propositions) will be simultaneously entered in the duplicate Vote databases.
4. The ‘row ID’ from Step 2 is also entered to the corresponding voter’s ballot contents.
5. Once the ‘submitted’ column is marked “true”, the voter cannot log in again.

Note that the voter ID is **not** an entry in the Vote database. This is to ensure privacy so there is no direct link to see which vote entry belongs to which voter.

### Voter Table Contents

* **VoterID** **(9-digit #)** - Unique, government-provided ID (only registered voters)
* **Password (Alpha-numerical)** - Hash-encrypted password
* **Submitted (Boolean)** - 0 NO, 1 YES
* **RowID (Auto-generated)** - Unique number to identify row number in   
                                                  Vote database (null if not voted)



### Vote Database

* The vote database system will consist of 3 separate databases in different locations.
* Upon completion of a ballot, the ballot contents will be simultaneously entered in the Vote databases.

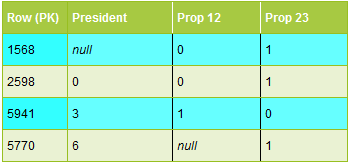
There are 3 duplicate vote databases for a few reasons:

* **Redundancy** – To ensure no data is lost in the case of a database or power failure
* **Integrity** – To ensure that the data is not corrupted in any way by a single adversary.
  + If all 3 databases match 100%, then we can ensure the voters that there was no corruption.
  + If two databases match 100%, and the 3rd database does not, then we know there was some kind of manipulation on database #3, and we can investigate the administrator of that database.
  + In the rare case that all 3 databases do not match, then we should have done better background checks on our secret administrators.

### Vote Table Contents

**Note:** This is a sample ballot. The RowID is the only required column. The remaining columns are specific nomination candidates or propositions.

* **RowID** - (PK to Voter Table) - Unique ID generated upon submission
* **President (Number - nullable)** - Number value for presidential candidate
* **Prop 12 (Number - nullable)** - 0 NO, 1 YES, null - no vote
* **Prop 23 (Number - nullable)** - 0 NO, 1 YES, null - no vote



## Citations

[1] – E-Voting Wikipedia, https://en.wikipedia.org/wiki/Electronic\_voting\_in\_Estonia