CECS 579 Project Design Document

Electronic Voting System

1. Identify Assets:

Votes- We need to protect the integrity of the actual vote. That each vote is counted once and only once.

Voter Information – We need to protect the private information that is used to create an account (special government ID, name, etc.)

Voter Anonymity – We need to protect the anonymity of the voters; the system should not be able to tell who voted for what.

1. Stakeholders:

Voters, nominees up for election, and the government hosting the election

1. Adversary Model:

See attack tree for attack surfaces.

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.

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

1. 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]

Other sources/ models

1. Solution:

Our voters will be issued a one time use private key with which to log in to the application. If a user logs in and finds that their key has already been used, they will have to petition to have their vote removed and recast.

The database will have two views, which will be supported by two different admins, because of the need to be able to revoke inappropriate or invalid votes. One view will contain the user information- voter ID, private key, a Boolean flag triggered once they log in, a Boolean flag once they have voted, and an automatically created administration number which will serve as the foreign key to the view containing vote information. The view containing vote information will have the administration number and the vote.

By separating these tables into two views, we allow the system to maintain anonymity, because no one user has access to all the information, while still being able to revoke votes if necessary. To obtain a vote to revoke it would take collaboration between multiple parties.