CS419 Virtual Election Booth

Billy Lynch wlynch92
Will Langford wtl17

Spring 2014

1 Protocol

Key:

$V = Voter$

$L = CLA =$ Central Legitimization Agency

$T = CTF =$ Central Tabulation Facility

$P =$ Publish

$$V \xrightarrow{Name|(Name)_{Sig_V}} L$$

$$V \xleftarrow{(Name|ValidationNumber|(Name|ValidationNumber)_{Sig_L})_{E_{KUV}}} L$$

$$L \xrightarrow{(ValidationNumber|(ValidationNumber)_{Sig_L})_{E_{KUT}}} T$$

$$V \xrightarrow{(ValidationNumber|VoterID|Vote)_{E_{KUT}}} T$$

$$V \xleftarrow{ACK|(ACK)_{Sig_T}} T$$

$$T \xrightarrow{(ID{:}Vote)_1|(ID{:}Vote)_2|...|(ID{:}Vote)_n} P$$

$$T \xrightarrow{(n|VN_1|VN_2|...|VN_n|(n|VN_1|VN_2|...|VN_n)_{Sig_T})_{E_{KUL}}} L$$

$$T \xleftarrow{(n|Name_1|Name_2|...|Name_n|(n|Name_1|Name_2|...|Name_n)_{E_{KUT}}} L$$

$$T \xrightarrow{Name_1|Name_2|...|Name_n} P$$

2 System Design

Assumption: We are given a list of valid voters and corresponding public keys to start off with.

2.1 Getting a validation number

To get a validation number, voters first requests a validation number from the CLA, signed with their private key. The CLA will then verify the message came from the user. If this is the first time the CLA has gotten a request from the voter, then the CLA will generate a new validation number. If the voter has already requested a validation number, then the CLA will return the same validation number that was previously generated. The returning message will be signed by the CLA and encrypted with the voter's public key (so only the user will be able to decrypt the message to get the validation number.

The CLA does not have to send all the validation numbers at once to the CTF. In order for voters to vote independently (not have to wait for all voters to get their validation numbers), we can send their validation number to the CTF as soon as it is generated, since the validation number will not change.

The CTF will continue to accept responses until the voting period ends.

2.2 Sending votes

To send a vote, the voter will use the validation number received from the CLA to contact the CTF with their vote. The user will also have to provide a unique user ID for the CTF. If the voter ID has already been taken, then the CTF will return an error saying that the ID is in use (this does not cause a threat since the authorization of the vote is based on the validation number). Otherwise, the CTF will acknowledge (ACK) the response was received regardless of whether the vote was successful or not (so that mallicious users can not use this as a means of checking whether they have successfully guessed a validation number).

2.3 Publishing Votes

When voting is complete (the voting period is over), the CTF can simply publish the result and all of the VoterID:Vote pairs. To satisfy the requirement of letting users know who did and did not vote, the CTF must contact the CLA with the validation numbers of those who voted. This list will not be sent in lexicographic order by validation number so that it is unlikely to create a relation between a votes and validation numbers. The CTF will then publish the list of those who voted.

3 Security Requirements

- Only authorized voters can vote.
  Because the CLA sends back the Validation Number for the voter encrypted using the voter's public key, the voter will only be able to decrypt and use it. Later on, the validation number is always encrypted using the CTFs public key, so it cannot be read if intercepted.

- No one can vote more than once.
  The CLA will keep a list of Validation numbers sent to each voter, so if someone requests another validation number, they will end up getting the same validation number again. The CTF will only accept one vote per validation number, so once it is used other votes with the same validation number will not be accepted.

- No one can determine for whom anyone else voted.
  Since results are published using the user defined random IDs, no one will know each others votes unless they have disclosed their ID.

- No one can duplicate anyone else's votes.
  Since every voter's validation number is encrypted whenever sent to the voter or CTF, it cannot be intercepted then used to change the user's vote. Since the CTF will only take one vote per validation number, replay attacks will fail.

- Every voter can make sure that his vote has been taken into account in the final tabulation.
  Since voter IDs are unique (the server will reject any IDs that are already in use), every voter will be able to look up their votes to make sure they are correct.

- Everyone knows who voted and who didn't.
  The CTF will contact the CLA at the end for the list of names given a list of validation numbers. Since these can be in arbitrary order (easiest means to do this is sort names lexicographically), it is fine to post them without creating a relation between voters and their votes (which would violate a requirement).