Virtual Election Booth

8th February 2003

This project implements the secure election protocol described in [SCHN96], p. 127 (Voting with Two Central Facilities). A more theoretical discussion is found in [SALO96]. The implementation will provide a secure way for people to vote online, which eliminates the hassle of physically being present at designated election locations.

Since computerized voting will not replace general elections unless there is a protocol that both maintains individual privacy and prevents cheating, the ideal protocol must meet these requirements:

- Only authorized voters can vote.
- No one can vote more than once.
- No one can determine for whom anyone else voted.
- No one can duplicate anyone else's votes.
- Every voter can make sure that his vote has been taken into account in the final tabulation.
- Everyone knows who voted and who didn't

Your design should use two central facilities: Central Tabulating Facility (CTF) and Central Legitimization Agency (CLA). CLA's main function is to certify the voters. Each voter will send a message to the CLA asking for a validation number, and CLA will return a random validation number. The CLA retains a list of validation numbers as well as a list of validation numbers' recipients to prevent a voter from voting twice. Then, the CLA completes its task by sending the list of validation number to the CTF. CTF's main function is to count votes. CTF checks the validation number against the list received from the CLA. If the validation number is there, the CTF crosses it off (to prevent someone from voting twice). The CTF adds the identification number to the list of people who voted for a particular candidate and adds one to the tally. After all the votes have been received, the CTF publishes the outcome.

An effective way to implement this is via the web, using CGI programs to implement CTF and CLA, and a Java applet to do encryption on the client side.