E-Votiing Project, Part #2
Specification of E-Voting System

Brian Cohen, Joe Hanauer, John Scillieri, Mark Brocato

Introduction

We accomplish remote poll-site voting in a secure, relatively private fashion. The design is described below.

Design and Operation

Each poll site has a series of computer systems:

- 1 Tally server (tallier)
- 1 Voter Registration and Validation Server (VRVS)
- Some number of voting kiosks

The election office in the county capitol has another series of computer systems:

- 1 duplicate checking server (dupecheck)
- 1 tally server (master tallier)

The VRVS contains a local copy of a county-wide database of registered voters. A sample table structure would be:

Election_ID
Voter_ID
SSN
Drivers' License Number
Last Name
First Name
Middle Name
Street Address 1
Street Address 2
City
State
Zip code
PUBLIC KEY
PRIVATE KEY
STATUS

PUBLIC KEY and PRIVATE KEY are generated in advance, in a batch process before each election. All registered voters are generated a unique keypair. 2048-bit RSA is used.

There is a public/private keypair unique to the master tallier. RSA 2048 bit is used. Of this pair, the private key is stored on the master tallier only, while a copy of the public key is on each VRVS. These are the MT keys (Master Tallier key).

Each VRVS has its own 2048-bit DSA keypair. These are the VRVS keys.

A voter shows up at any polling station in the county and presents valid photo identification, such as a drivers' license. The election official has a workstation with access to the VRVS, who does a search against the DB and finds the voter record. The official clicks a button which marks the voter's STATUS as 'PRESENT' and uploads the PUBLIC KEY, PRIVATE KEY, MT_pubkey and Voter_ID to a smart-card containing a small amount of ROM and a microprocessor.

The election official presents the smart-card to the voter, and instructs the voter to proceed to a voting kiosk.

At the kiosk, the voter is welcomed by a screen which instructs him to insert his smart-card into the kiosk, much as he would an ATM card. The voter is presented with a ballot on the touch-screen. Through a series of well-designed interfaces, the voter makes his choices and is given several opportunities to make corrections before committing to his choices.

Upon finalizing his vote, the kiosk then engages in a cryptographic exchange with the validator and the tallier. The exchange goes like this (all signatures are DSA):

1. Voting choices are concatenated into a single string. (The Ballot)
2. Voting choices are written to a ribbon or card which can be read by an optical scanner, thus leaving a paper trail so that tallying can be still be done in case of an electronic tallying failure.
3. Ballot is encrypted with MT_pubkey.
4. Ballot is blinded by multiplying the ciphertext by a 1024-bit random integer (the OTP), generated on-the-fly by the chip in the smart-card. OTP is written to the smart-card.
5. Ballot is signed with the user's PRIVATE KEY.
6. Ballot is sent over a physically and cryptographically secure LAN to the local VRVS. The VRVS checks the ballot's signature against its database of voters' public keys until it finds one that matches. When it does, the signature is stripped off the ballot and replaced with the VRVS' DSA signature.
7. The blind, encrypted, VRVS-signed ballot is now returned to the kiosk.
8. Having obtained validation from the VRVS, the kiosk un-blinds the ballot by dividing out the OTP. This leaves behind a VRVS-signed ballot that is encrypted with the master tallier's public key.
9. Ballot, along with the Voter_ID, is sent over the LAN to the local tallier. Tallier checks if the signature on the ballot is truly that of the VRVS. If so, confirmation sent back to the kiosk that the vote was accepted.

10. All information is deleted off the smart-card, which is then collected by an election official as the voter leaves the booth.

The database on the local tallier will look like:

Voter_ID
Encrypted_Ballot

At the conclusion of the election, the local talliers and VRVS's are brought to the county office. The databases from each are transferred to the dupecheck. The dupecheck looks at the list of voters from each district that were marked as having voted. If a voter was found to have voted multiple times, any record in any tallier table that has that Voter_ID is deleted. The tables, now clean of duplicates, are stripped of all Voter_Ids and transferred to the Master Tallier. The Master Tallier concatenates the tables, decrypts the ballots with its MT_privkey, and tallies the results.

In the case of an all-out failure of the system (mechanical, electrical, etc), optical scanning systems for provisional ballots will be used. A front-end to the dupecheck system will allow input from these provisional ballots. Furthermore, input can be accepted from the paper backups produced by the kiosk.

Security and Privacy

Our system goes to great cryptographic lengths to ensure the security and privacy of the election. The "blind signature" approach in which the kiosk and VRVS verify a voter's status while hiding the contents of the ballot is well-documented and is currently used by systems such as VoteHere and Sensus.

The most glaring tradeoff in our system lies in the fact that Voter_ID is stored alongside the ballot on the local talliers and on the county Dupecheck machine. A corrupt election official, law enforcement officer, or criminal cracker could, theoretically, gain access to both the Master Tallier and the Dupecheck machine. If that happened, the private key from the Master Tallier could be used to decrypt the ballots while they are still associated with a Voter_ID. This would severely compromise the privacy of the election.

We feel this is a tradeoff that had to be made at some point. We simply cannot envision a secure system that would, at once, protect the identify of a voter while still allowing for tallies to be adjusted in the case of duplicate votes being detected. Real-time validation against a central, county-wide version of the VRVS is simply too much to expect, as it would introduce a central point of failure, a potentially crippling stream of traffic, and the additional problem of unstable or vulnerable telecommunications at the poll-sites. In addition, the risk of such collusion between the Master Tallier and the Dupecheck does not exceed the risk of the sort of corruption found in some modern elections, such as where uncast ballots were clandestinely cast by election officials on the take after the polls closed. Finally, there is the fact that even today, not all ballots are anonymous:

provisional ballots must have a person's name and other identifying information on them in order for them to be of any use.

So long as the source code of the system is open for public perusal, and so long as the actions of the election official performing the tallying are watched closely, we feel this is a secure system that has the potential to increase voter turnout and drastically speed up tallying.

References

Cranor, Lorrie: Sensus Voters' Manual.
http://lorrie.cranor.org/voting/sensus/man.html

CS594 Internet Voting
http://www.cs.utk.edu/~ffowler/cns-html/append.html

Farrel Lifson: The Security of Online Voting: Blind Signature Protocol
http://people.cs.uct.ac.za/~flifson/things/security/node8.html

Electronic Voting (list of sites)
http://www.tcs.hut.fi/~helger/crypto/link/protocols/voting.html