

# Case Studies

Monday, May 04, 2009

12:57 PM

## Voting, RFID

- Originally, both products were proprietary trade secrets
- Details leaked out

## Lessons

- open source
  - o More eyes to detect bugs
- Security through obscurity is bad
- Use good industry standards

Real systems are complicated and must be designed with security in mind throughout

## Voting Security Goals

- People could only vote once
- Only citizens can vote
- Tamper resistant
  - o Vote counts
  - o Election definitions
- Availability
- Recoverability
- Early Results
- Privacy of voters
  - o Coercion
  - o Vote selling
- Cast-as-intended
- Count-as-cast

## Current DREs

- Completely black box
- Everyone must trust the DREs
- Certified through testing
  - o On election day
    - Choose test machine randomly
    - Enter simulated votes into machine
    - Check accuracy at the end of the day
  - o Bugs not discovered until the after election

## Backend tabulator

### DREs

- o Ballot definition inputted
  - Specified candidates, races, etc.

### Smartcards

- o Specify voter or admin and party affiliation

## DRE Steps

0. Distribute Election Commissioner's key
1. Create ballot definition
  - a. Party is correct
  - b. Races correct

- c. All candidates present
- d. Etc.
- 2. Distribute it to the voting machines
  - a. Signed by election commissioners key
- 3. Verify BDs on DREs
- 4. Transport DREs to Election
  - a. Trusted Platform Modular's, Remote Attestation
- 5. Start Election
  - a. Initialize all vote counts to 0
- 6. Voter
  - a. Given Smart Card
    - i. Easily spoofed
  - b. Verify Smartcard at DRE
  - c. Obtain vote
  - d. Record vote
    - i. Trust DRE
  - e. Cancel card
    - i. Could make a smart card which cancelled the cancel message
    - ii. Verify the card is real
      - 1) Have a private key on the card with the public key on the DRE

The whole system was botched

You could video everyone entering and figure out which person voted for who.

- 7. End election
  - a. voter card easily spoofed
  - b. admin card easily spoofed
- 8. Transmit results to central tabulator
  - a. should be signed
  - b. remote attestation

#### Alternative - instead of trusting hardware software people

- generate a proof that the election ran correctly, a proof that anyone could verify.

#### Failures of Security through Obscurity

- DST40
- GSM
- Microsoft DRM
- Apple DRM
- HDCP
- Enigma

#### Alternative to DREs

VVPT (Voter Verifiable Paper Trail)

- o Voter interacts with computer
- o Computer prints out ballot
- o Voter drops it in ballot box