

Case Study

An Electronic Voting System

Submitted by Arunkumar Senthilnathan on 05/04/09

Two case studies under consideration:

Electronic Voting System & RFID

Common between the two case studies:

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

Lessons to be learnt from the two case studies:

- Keep it open source
- Security through obscurity is bad
- Use good industry standards
- Real Systems are complicated and must be designed with security in mind through out

Voting System – Security Goals

- People should vote only once
- Only citizens should vote
- Tamper resistance
 - Vote counts
 - Election definitions
 - Secret keys
- Availability
 - Recoverability
- Early Results
- Confidentiality
 - Privacy of Votes
 - Coercion
 - Selling of votes
- Cast-as-intended
- Count-as-cast

Alternatives to Direct Recording Electronic (DRE) System

Voter Verifiable Paper Trail

- Voter interacts computer
- Computer prints out ballot

- Voter drops ballots in box

Current DRE System

- Completely black box
- Everyone trusts DRE
- Certified through testing
 - On Election Day
 - Choose test machine randomly on election days
 - Enter simulated votes into machine
 - Check accuracy at the end of the day
 - We don't get to detect the bugs until the end of the day
- Smart Card Specification
 - Vote Vs Admin and Party Affiliations
- Ballot Definitions
 - Gives Candidates, races etc

Steps involved in the electronic voting system

- Distribute Election Commissioner public keys
- Create Ballot Definitions (BD)
 - Correct parties
 - Correct races
 - All candidates
- Distribute BD to DREs
 - Signed by Election Commissioner key
- Verify BDs in DREs
- Transport DREs to election centers
 - Remote Attestation
- Start Election
 - Instantiate all vote counts to zero
- For each vote
 - Initialize smart card
 - Verify Smart Card at DRE
 - Easily forged
 - Obtain vote
 - Record vote
 - Trust DRE
 - Privacy compromised
 - Cancel card
 - Custom smart card which ignores cancel message can be built!

- End Election
 - Ender Card
 - Admin Card
- Transmit results to central tabulator
 - Should be digitally signed
 - Remote attestation should be added

Alternative

Instead of trusting hardware, software and people generate a proof that election can run correctly

Example of failures of security through obscurity

- DSTGO
- GSM
- Microsoft DRM
- Apple DRM
- HDCP
- Enigma