

Voting, RFID

- Originally, both product are propriety trade secret
- Leaked out

Lesson:

- Open source
 - More eyes to detect bug
- Security through obscurity is bad
- Use good industry standards

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

Voting

- People can only vote once
- Only citizen can vote
- Tamper resistant
 - Vote counts
 - Electronic definitions
 - Keys
- Availability
- Recoverability
- Early results
- Privacy of vote
 - Coercion
 - Vote selling

Alternative to DRE

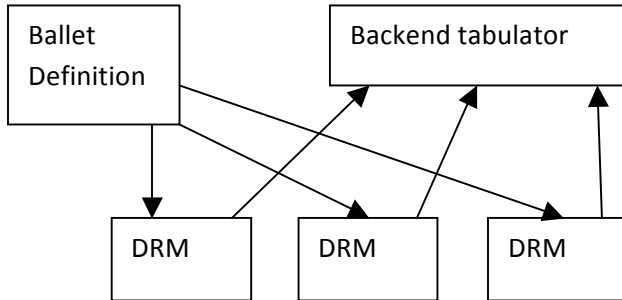
- VVPT - Voter Verification Paper Trail
 - Voter interact with computer
 - Computer print out ballet
 - Voter drop ballet in box

Current DRE

- Completely black box
- Everyone must trust DRE
- Certified through teaching
 - Extreme on election day

Solution:

- Choose test machine randomly on election day
- Enter simulated vote into machine
- Check accuracy at the end of day
 - Down: don't detect bug until after election end



- Smart cards specify voter vs. admin and party affiliation
 - Ballet definition: candidates, races, etc.
1. Distribute keys (EC public key)
 2. Create Ballet Definition
 - Party correct
 - Races correct
 - All candidates presents
 3. Distribute BS to DRE
 - Sign by election commission key
 4. Verify DB and DRE
 - (AccuVote does not do any of this)
 5. Transport DRE to election
 - TPM (Trusted Platform Modules, hash software)
 6. Start election
 - Initiate vote counter to 0
 7. For each voter
 - Init smart card
 - Verify smart card at DRE
 - Easily spoof
 - Obtain vote
 - Record vote
 - Cancel vote
 - Trust DRE, compromise privacy
 - Cancel card
 - Custom smart card can ignore cancel msg.
 8. End Election
 - Insert admin card
 - Easily spoof
 - Enter pin
 - Easily spoof
 - Insert command
 9. Transmit result to central tabulator
 - Signed, encrypted

Alternative: instead of trusting hardware, software, people generate a proff that the election ran correctly

Fancy key distribution:

- DRE have all parties key
- SD signed by all party

- AccuVote does not stored who (voters) voted for
- It only stores the position of the candidate listing
 - Attack: switching candidate names

- Session key so user cannot run out with the card
- Split keys, DRE contain public key, insert card require card to proof

- Admin cmd require pin while stored on the card

- Record vote sequentially in file
 - Take a camera and record who goes in and out

Failure of security through obscurity

- DST 40
- GSM (reading phone traffic, charge other account)
- Microsoft DRM
- Apple DRM (play fair)
- HOCP
- Enigma (use by German)