

CSE 509: COMPUTER SYSTEMS SECURITY
SPRING' 09: LECTURE NOTES

Date - 05/04/09

Submitted by : Raveesh Ahuja

Case Studies:

Electronic Voting and RFID

- Originally both products were proprietary trade secret
- In case of electronic voting the details were bashed out and in case of RFID paper the details were given out at the presentation by Dr Ulrich Kaiser

Lessons Learnt:

- Open source : more eyes to detect bugs
- Security through obscurity is bad
- Use industry standards
- Real systems are complicated and should be designed with security in mind

Security Goals for Electronic Voting :

- People can only vote once
- Only citizens should be allowed to vote
- Tamper Resistant – Vote Counts , Election Definition and Secret Keys
- Availability & Recoverability
- Early Results/ Exit Poll
- Privacy of Voters
 - Coercion : Forcing voters to vote
 - Vote Selling
- Cast as intended
- Count as cast

Alternative to DRE's:

VVPT (Voter Verifier Paper Tool)

- Voter interacts with computer
- Computer prints at ballot
- Voter s drops bulletin box

Current DRE's

- Completely black box
- Everyone must trust DRE's

- Certifies through testing on election day
- Choose test machine randomly on election day
- Enter simulated notes into machine
- Check accuracy at end of the day. Disadvantage of the approach: Bugs not discussed till after election.
- Smart cards specify Voter Vs Admin and party affiliations.

Steps Involved in Electronic Voting System

1. Distribute election commissioner's public key to DRE's.
2. Create ballot definition: Correct Parties, Races and all candidates.
3. Distribute ballot definition to DRE which is signed by election commissioner's key.
4. Verify BD's in DRE
5. Transport DRE's to election centers using remote attestation.
6. Start election and initialize all vote counts to zero
7. For each Voter
 - Initialize Smart Card
 - Verify Smart Card at DRE (can be forged!!)
 - Obtain Vote
 - Record Vote : a) Trust DRE b) Compromised User Privacy
8. Cancel Card: Cancel Message. But custom smart cards which ignore this message can be built!!
9. End Election: Using the Ender Card or the Admin Card. (Can be easily spoofed!!)
10. Transmit results to central tabulator
 - Should be digitally signed
 - Remote attestation should be added

Alternatives:

Instead of trusting the Hardware, Software, People, generate the proof that the election ran correctly.

Examples of Failures of Security through Obscurity:

- GSM
- DST40 (RFID Case Study)
- Microsoft DRM
- Enigma
- HDW
- Apple DRM (Fairplay : SONY DRM Case Study)