Case studies of 2 products were discussed:
- Electronic Voting System.
- RFID Device - DST (Digital Signature Transponder)
These products were studied by experts and found to be faulty or having vulnerabilities.

Similarity between the products:
- Originally both products were proprietary trade secrets.
- Details leaked out.

Lessons Learnt:
- Open Source.
- More eyes to detect bugs.
- Security through obscurity is bad.
- Use good industry standards (Eg. Standard algorithms)

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

Desired properties in case of Voting Systems: (Security Goals)
- People can vote only once
- Only citizens can vote
- Tamper resistant
  - Vote counts
  - Election definitions
- Availability
  - Recoverability
- Early Status
- Voter Privacy
  - Avoids coercion
  - Avoids vote selling
- Cast-as-intended
- Count-as-cast
Alternate to DREs:

**VVPT (Voter Verifiable Paper Trial)**
- Voter interacts with computer.
- Computer prints out ballot.
- Voter drops ballot in box.

Current DREs:
- Completely black box
- Everyone must trust DREs
- Certified through testing

On Election day:
- Choose test machine randomly on election day
- Enter simulated votes into machine
- Check accuracy at the end of the day
- Bugs not discussed till after election

Diagram:

- Smart Cards specify Vote Vs Admin and party affiliation.
- Ballot definitions – gives candidates, races etc.

Election/Voting System:
1. **Distribute EC (Election Commissioner) public key to DREs.**
2. **Create ballot definition (BD)**
   - Parties correct
   - Races correct
   - All candidates present etc.
3. **Distribute BD to DREs:**
   - Signed by election commissioner key
4. **Verify BDs on DREs.**

5. **Transport DREs to election (Most vulnerable step)**
   - Trusted platform mode could be used in this case
   - Remote Attestation?

6. **Start Election**
   - Initialize all vote count to 0.

7. **For each voter:**
   - Initialize smart card
   - Verify smart card at DRE (easily forged!!)
   - Obtain vote
   - Record vote (Trust DRE, Compromised privacy through ordering)
   - Cancel card (Custom smart card ignores cancel message)

8. **End Election:**
   - End card (easily spoofed)
   - Admin card (easily spoofed)

9. **Transmit results to central tabulator:**
   - Should be digitally signed
   - Add remote attestation?

**Alternative:**
Instead of trusting hardware/software/people, generate a proof that the election ran correctly.

**Lessons Learnt / Conclusion:**
- **Failure of security through obscurity.**
  
  Example of cases demonstrating the above fact->
  - DST40
  - GSM
  - Microsoft DRM
  - Apple DRM
  - HDCP
  - Enigma

- **Get experts to review the tools/software developed.**