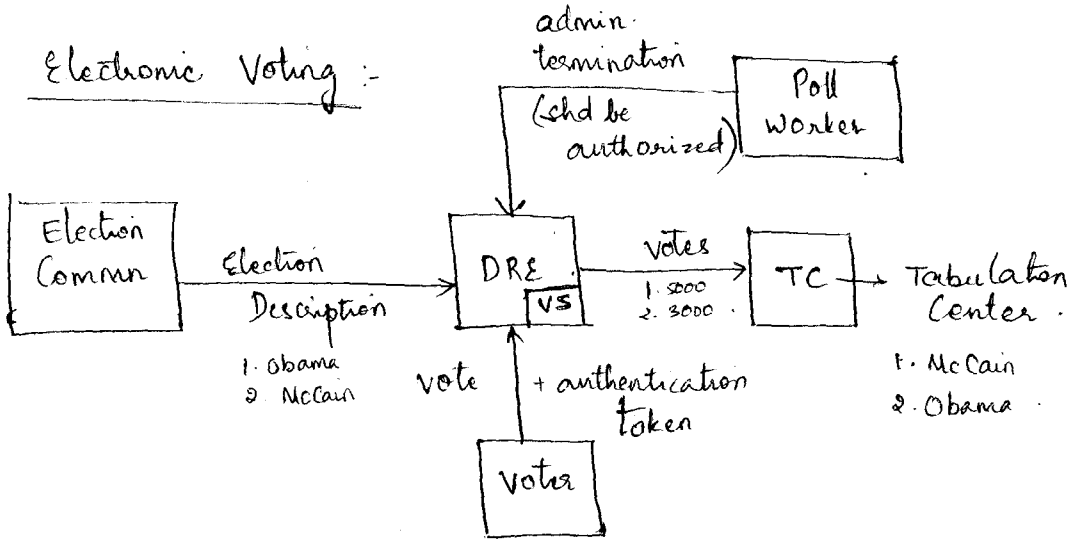
26/4/2007

Electronic Voting :-



VS - Vote Storage

Attacks :-

- Multiple Voting :-
  - Forged authorization cards ⇒ No secret, easy to do.
- Forged Election Description :-
  - → Candidate shuffling attack
  - → Confusion attack.
- Denial of Service via Forged Admin/ender cards.
- Votes transmitted with no authentication from DRE to TC.
- De-anonymize via Vote storage (based on the order in wch votes were voted)
- Security by Obscurity doesn't work. It is not enough to do just black-box testing.

Cryptanalysis of RFID Device :-

Cryptanalysis of RFID Device

Fob		Car
k		K
	challenge C ←	
E	R = E(k, C) →	ok if
	24 bits	R = E(K, C)

For power :- The Reader and RFID shd be a few cm apart

For information : " " " " .. meters "

RFID Types :-

- Cryptographic
- Bar Code

RFID — Reader

Read SN (serial no) ←

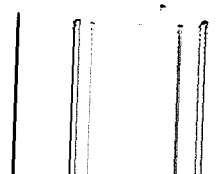
SN →

Bar Code Applns :-

- Retail
- Libraries
- Passports

Privacy Issues with Bar code

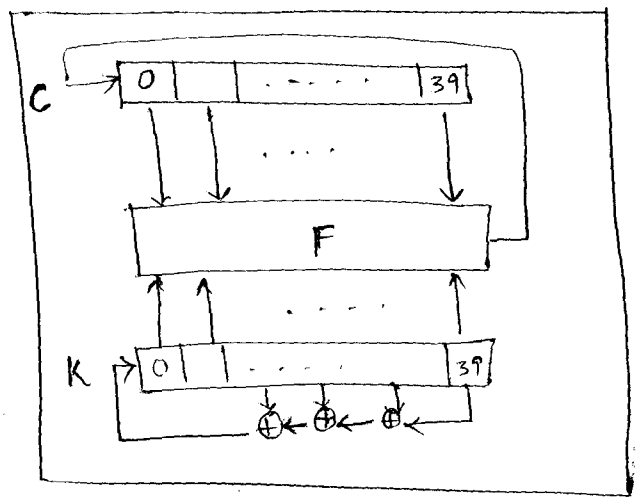
- Thieves prescreen houses via RFID on goods inside
- Obtain patron's reading list
- Identity theft



To prevent privacy attacks : we cd authenticate readers →

Faraday Cages. -- Remove tags

Disable Tags.



Attack :-

(1) Reverse Engineer E (Encryption function)

(2) Build a Key Cracker.

(a) Given a Fob, V, query V on challenge C_1, C_2 and obtain response $R_1 = E_k(C_1)$, $R_2 = E(k, C_2)$.

(b) for each possible K, if $E(k, C_1) = R_1$ && $E(k, C_2) = R_2$, output K