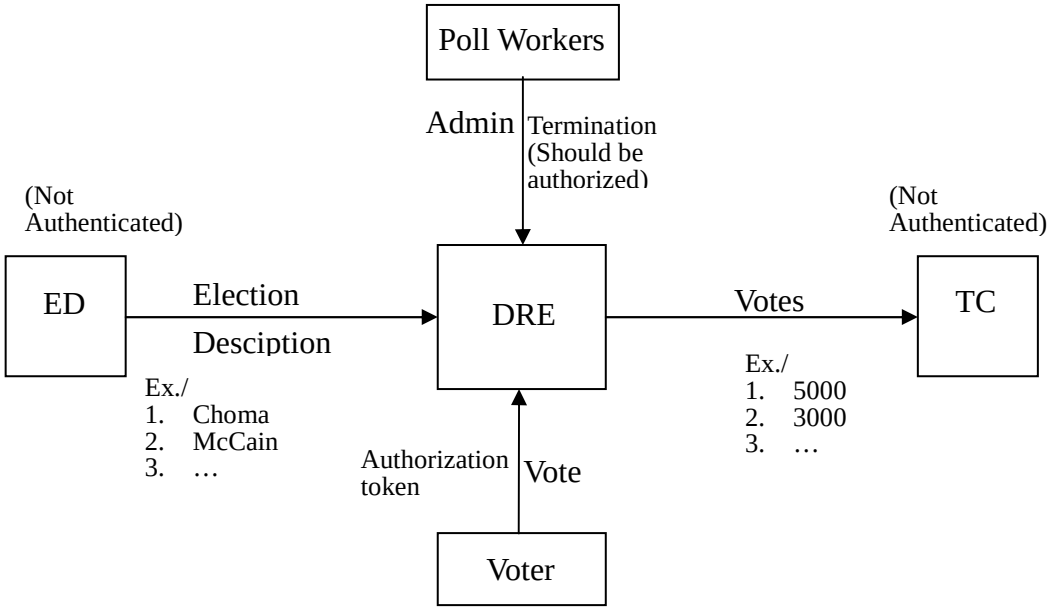
Class Note: April 26, 2007/4/26

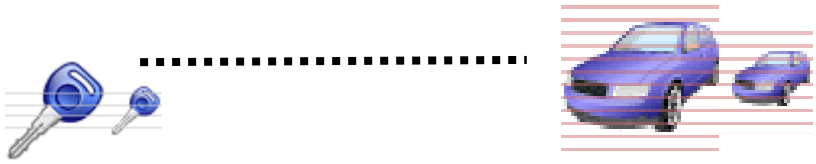
Electronic Voting (Cont.)



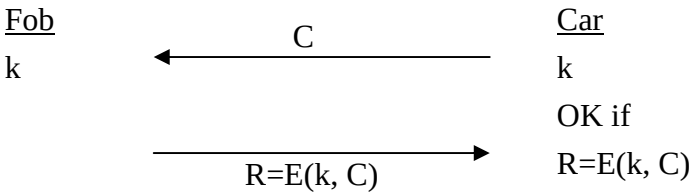
Attacks:

- Multiple voting
  - Forged authorization card ➔ No secret keys; easy to do
- Forged Election description
  - Candidate shuffleing
  - Confusion attack
- Denial of Service ➔ forged admin/ender cards
  - Pin # is stored in the card
  - No information log
- Votes transmitted with no authentication
- De-anonymize vote via storage

Cryptanalysis of RFID devices



Authentication Protocol:



For Power:

Reader & RFID should be few cm. apart

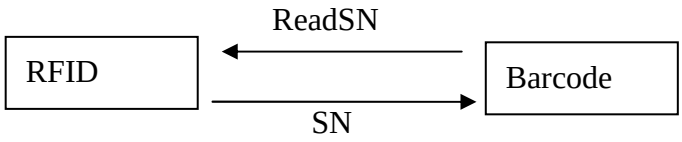
For information:

Reader & RFID can be few meters apart

RFID types:

1. Cryptographic
2. Barcode

Barcode:



Applications:

- Retail
- Libraries
- Passports

Main concern: privacy

- theifs prescan houses via RFID on goods inside
- obtain patron's reading book
- Identity theft

- Target screening

Defense:

- Authenticate readers
- Faraday cages
- Remove tags
- Disable tags

From the paper(reading):

Attacks:

1. Reverse engineering E
2. Build a key cracker
    1. given a Fob, V, query V on challenges, C_1 & C_2, and obtain response R_1 & R_2.
       $R_1 = E(k, C_1)$
       $R_2 = E(k, C_2)$
    2. for each possible k:
       if $E(k, C_1) = R_1$ & if $E(k, C_2) = R_2$
       ouput k