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 which 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
k
E

\[ R = E(k, c) \]
\[ 24 \text{ bits} \]

Car
k

\[ R = E(k, c) \]
\[ \text{OK} \]
\[ R = E(k, c) \]

For power: The Reader and RFID chip do not communicate directly.

For information: "..." "..." "meters" "...

RFID Types:
- Cryptographic
- Bar Code

RFID

\[ \text{Reader} \]
\[ \text{Read SN (serial number)} \]

Bar Code Applications:
- Retail
- Libraries
- Passports

Privacy Issues with Bar Code:
- Thieves presence in houses via RFID on goods inside.
- Obtain patron's reading list.
- Identity theft.
To prevent privacy attacks: we need to authenticate readers.

- Faraday cages
- Remove tags
- Disable tags

**Attack:**

1. **Reverse engineer** $E$ (encryption function).
2. **Build a key tracker.**
   
   a. **Given a Fob, V, query V on challenge $C_1$ and obtain response $R_1 = E_k(C_1)$, $R_2 = E(k, C_2)$.**
   
   b. For each possible $k$, if $E(k, C_1) = R_1$, output $k$. 

**Diagram:**

[Diagram showing the flow of data and entities involved in the attack.]