RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications

By: Bo Qin

RFID

- Radio-frequency identification provides contactless communication between **tags** and **readers** using radio v
- **Tags:**

- **Reader**

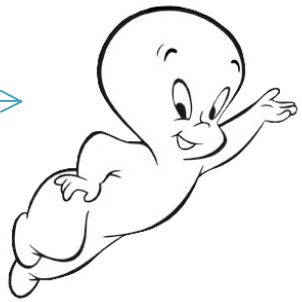
Problem

- Ghost-Leech attack (Relay attack):
  - Tags are always ready to be read

Authentication Data

Secure Relay Channel

Authentication Data

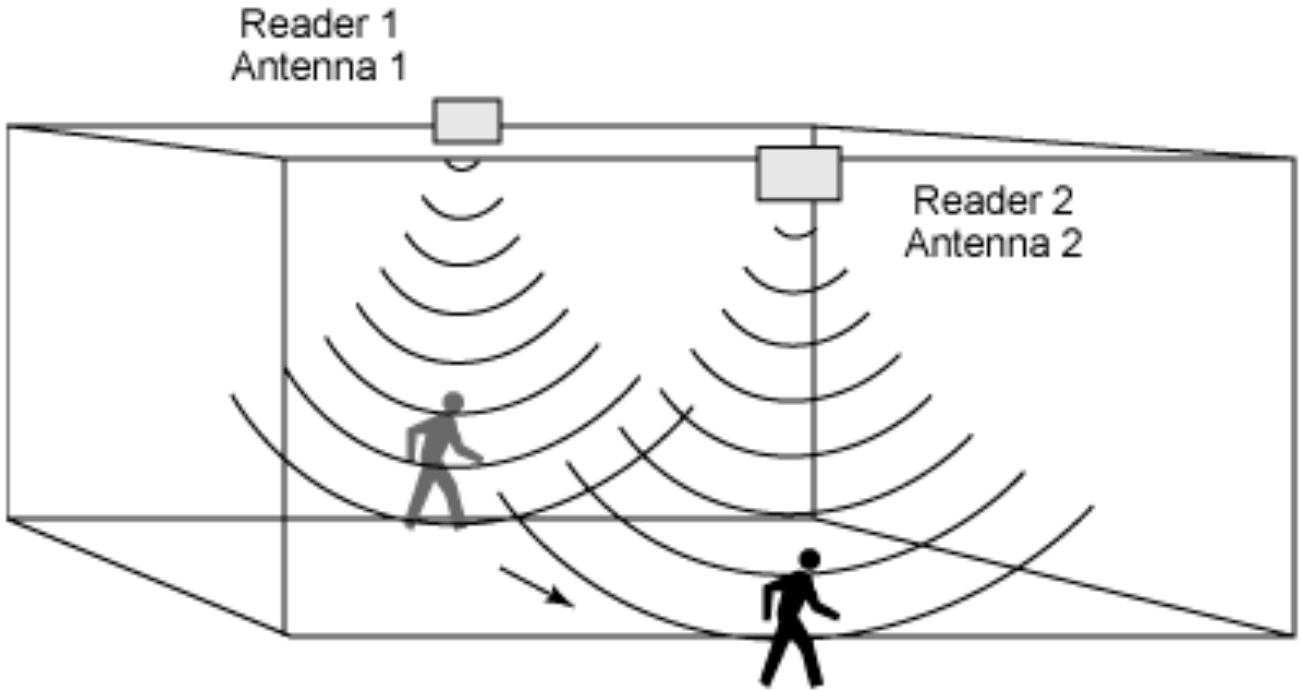


Emulate Reader

Emulate Card

Problem

- Tracking (privacy issue):



Problem

- Goals:
  - Backward Compatibility
  - Consistent Usage
- Possible solutions:
  - Sleeve – BC: Yes, CU: No

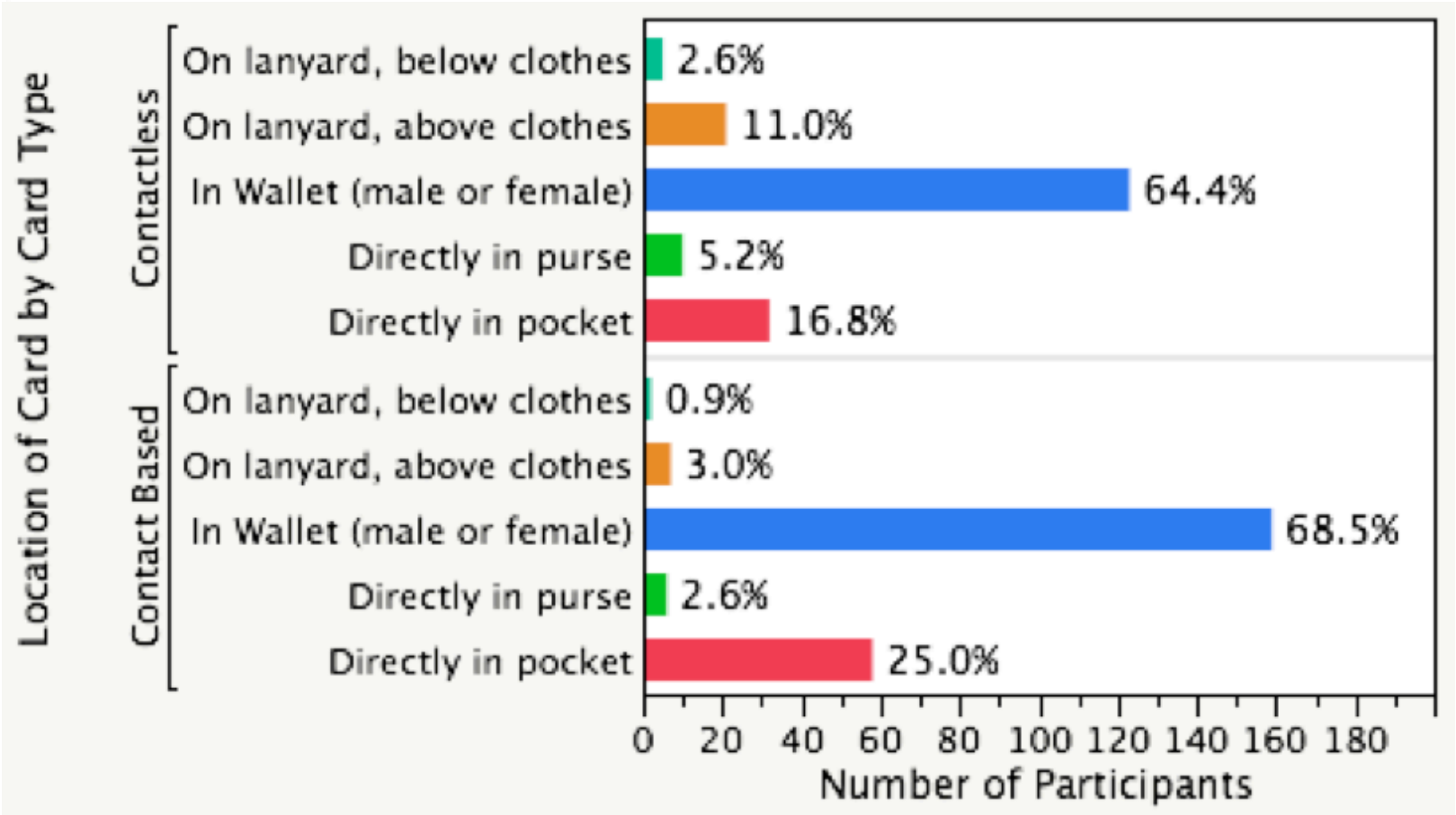
  - Button – BC: Yes, CU: N

  - Timing constraint – BC: No, CU: Ye

The tags should only be read when the user is using it near a card reader

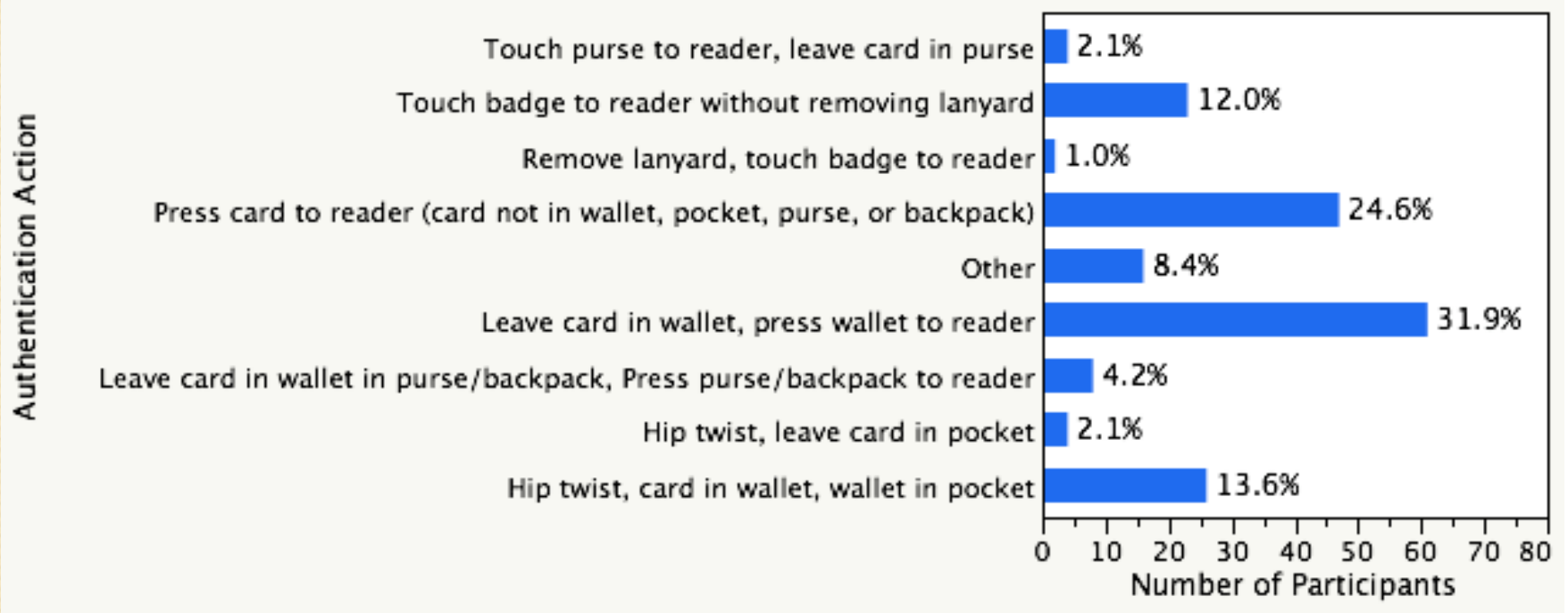
Survey:

- Where is your card?



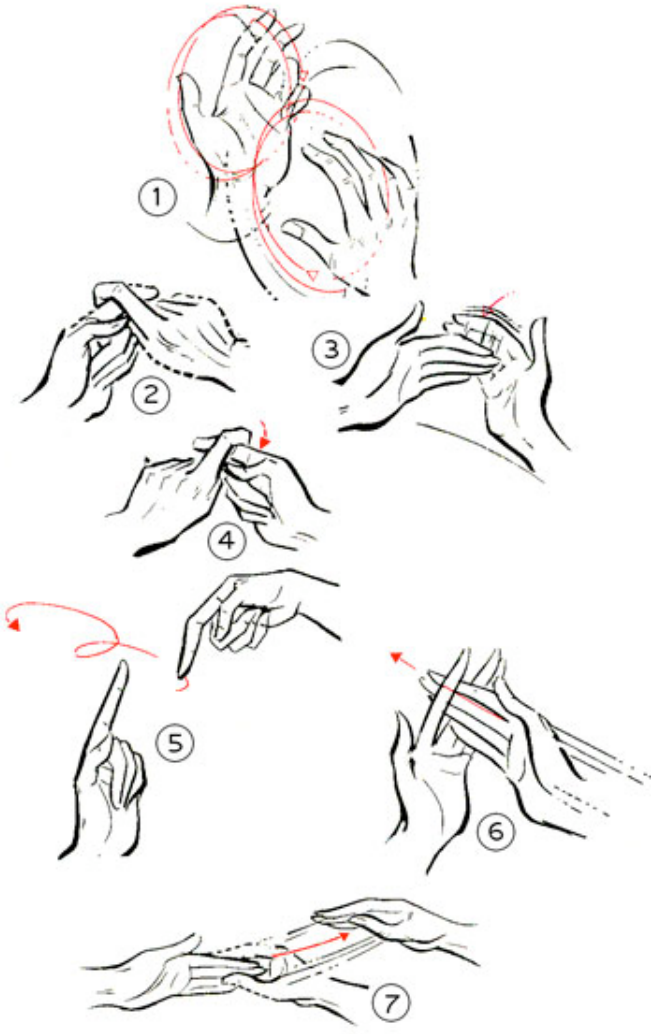
Survey:

- How do you use your card?

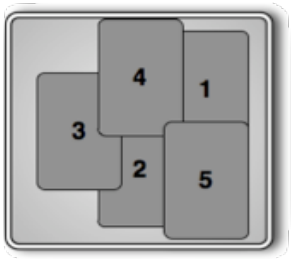


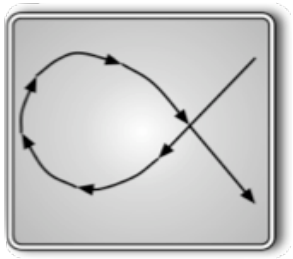
“We” have the solution

- Secret Handshake
  - User performs a gesture with the card to **activate** the card to communicate with the reader

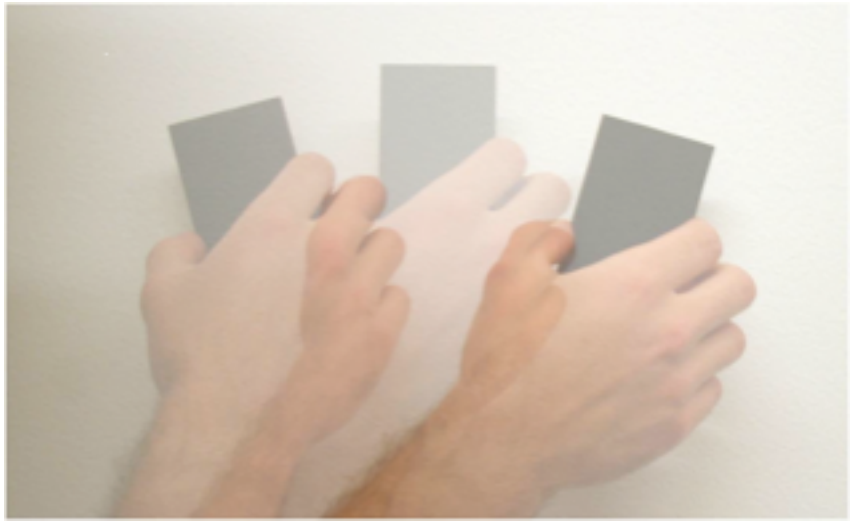


Gestures



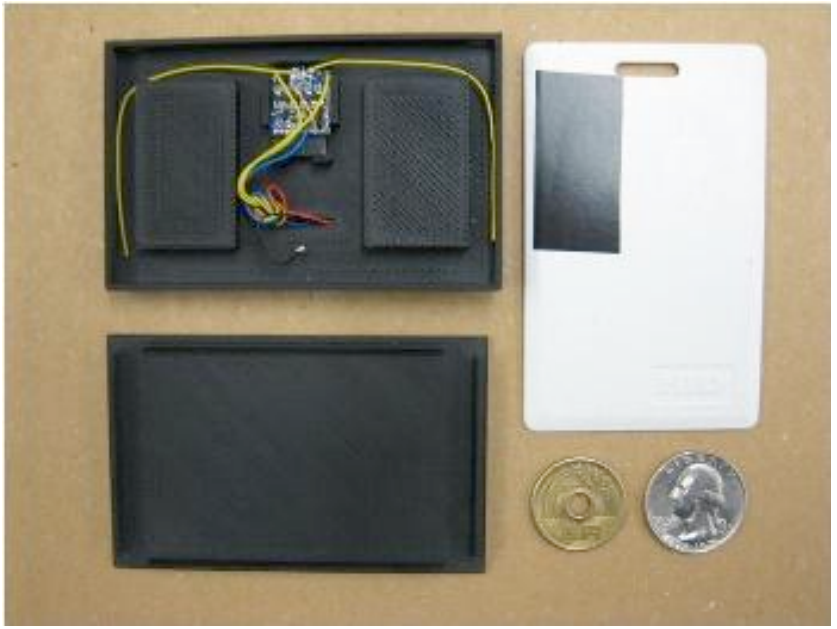


- Alpha
- Circle/Double circle
- Triangle
- Key Twist
- 1.5 Wave
- Hip Twist



Implementation

- Goals:
  - Cost Effective
  - Passive (no battery!)
- Hardware
  - Intel's WISP (Wireless Identification and Sensing Platform)
    - Only passive RFID device that's programmable
    - MSP430



Hardware Limitations

- Memory
  - Only 144 bytes of RAM for accelerometer data
- Power
  - Turning on accelerometer consumes most power
  - Sampling rate: 40Hz
- Gestures < 1 sec

Experiment

- Gather data for effectiveness of gestures
  - 8 gestures
  - 3 participants
  - Collected accelerometer data during daily activities
    - Sit, Walk, Stand, Bike, Fidget, Play Ping Pong, etc.

Gesture comparison

- False Negative (FN): Card failed to activate
- False Positive (FP): Card activated when not
- Threshold (simplified): values for calculating what is a gesture from accelerometer data
- Best gestures:
  - 1.5 wave and double circle
    - Largest range of threshold values with 0 FN and 0 FP
- Worst gesture:
  - Hip twist

Extension

- Different gestures for different cards
  - Bob's bus card (in wallet) with one gesture prevents driver, Eve, from reading Bob's credit card

Thank You

- Alexei and Yoshi for the slides