EECS 159A/CSE 181A
Paper project:
Attendance System

Motivation

- Need to take attendance
  - regular course, advising session, etc
- Current solution: attendance sheet
  - distracting, inefficient, manual entry by TA,
  - no way to check forged signature
- How to improve it?

Exploration

Explore

application

cool idea

mapping

technology

app

radios

battery

boards

sensor

chips

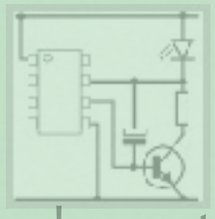
cloud

tinkering

Design

flowchart (temporal)

block diagram (spatial)



schematic

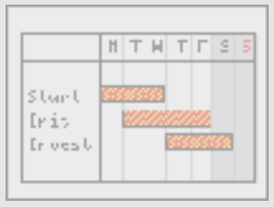
mechanical design

design tool, version control

Plan

team communication progress report

statement of work



Gantt chart milestones deliverables

development tools

version control

Build

firmware, app, server,..

hardware, network

3D modeling & printing

Evaluate

performance (throughput, latency)

power (battery life, peak power)

correctness

cost

manufacturability

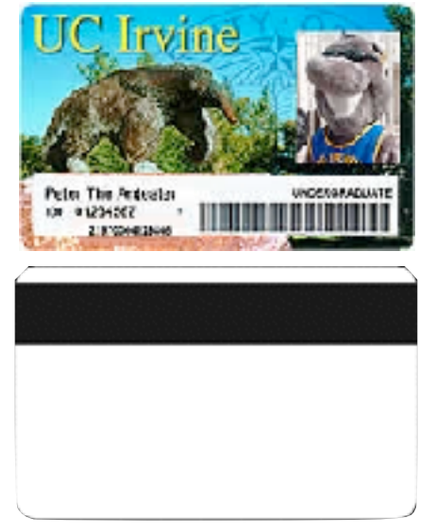
broader impact

management

Exploration of Technology Options

- Sensing Technology
  - ID card (barcode, magstripe, QR code)
  - RFID, Bluetooth or BLE
  - Biometrics
    - facial recognition, fingerprint recognition
- System Realization
  - Smartphone-based
  - Custom embedded system

Technology Option 1: Wireless ID-Card Reader



- Approach
  - Taking attendance by swiping ID card
  - TA brings one or more card readers to class
    - Swipe as you enter, exit, or pass reader(s) around
- Want to improve over commercial solution
  - Real-time logging into database if possible
  - Store data locally if network is disconnected
  - Multiple readers, synchronized operation

Options 1.1.*: Smartphone-based Solution

- An add-on device to smartphone
  - add-on device performs actual card reading
  - magstripe, QR-Code, Barcode, etc
- Use smartphone's built-in camera
  - can do barcode or QR-code,but not magstripe
- Questions:
  - can it support multiple units in use?

Option 1.1.1:
Smartphone + Magstripe Reader

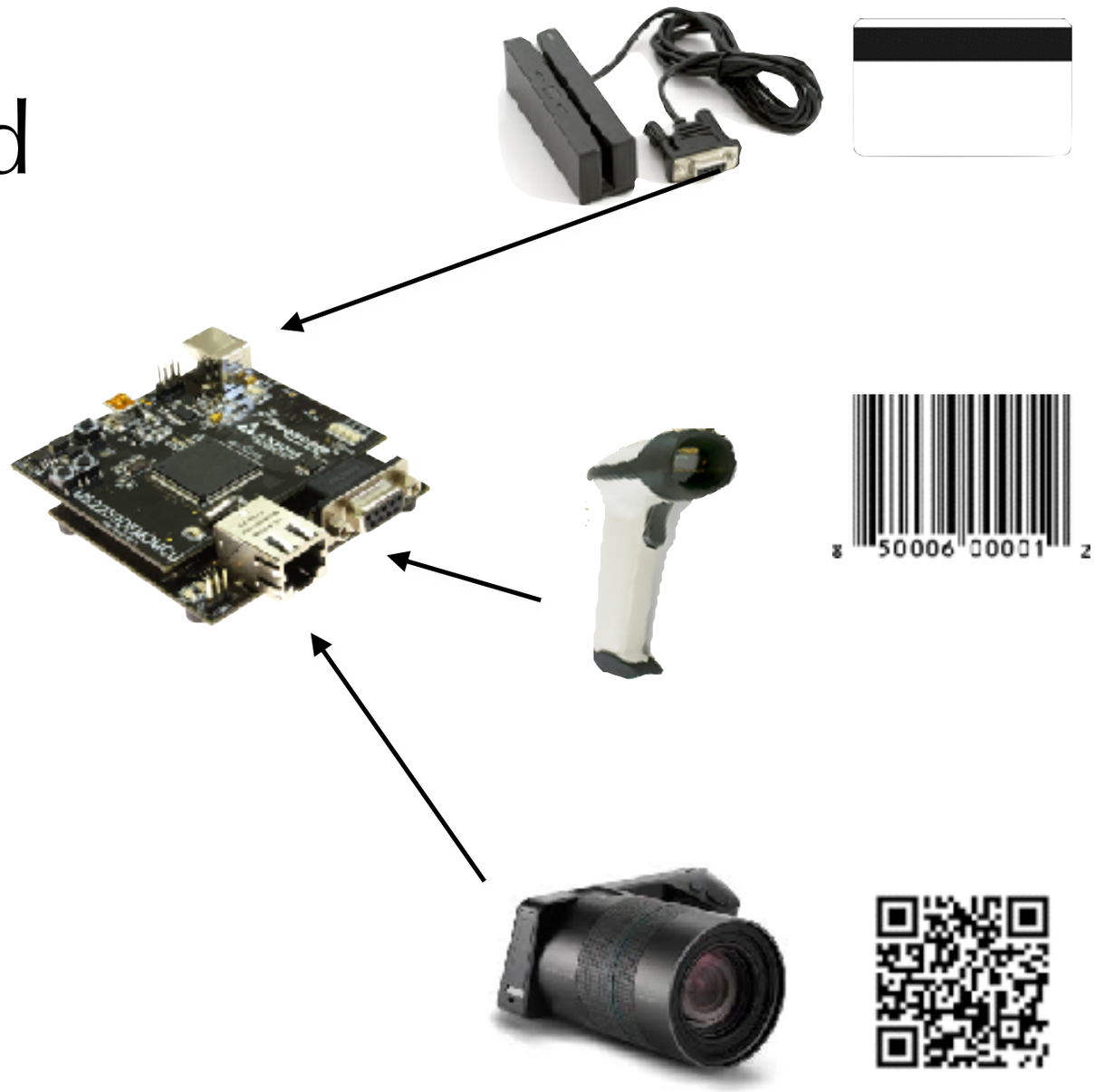
- Lightning connector
  - iPhone, iPod Touch,
- Price: $60-$80
- Pros: ready to use
- Cons:
  - someone might steal the iPhone or hardware
  - does not prevent forging

Option 1.1.2: Use Built-in camera for barcode or QR code

- All-software solution
- Existing app
  - Existing app probably just decodes the string, at most interpret it as URL
- Custom app
  - Calls existing library for decoding
  - can program with server to support concurrent operation

Option 1.2: Custom Board

- Build your own card scanner system!
  - Choose magstripe, barcode, QR code
  - No need to include smartphone — just scanner with wireless interface



Option 1.2: Custom Board (cont'd)

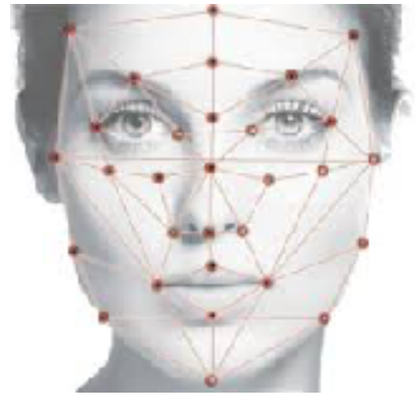
- Communication Options
  - RF: Wi-Fi? Bluetooth? Other custom RF?
  - Network: Direct TCP/IP to server? Going through a gateway? Local area connection only?
- Other Considerations
  - Cost? Size? Weight? Heat?
  - Security? easy or hard to hack?

Options 2.*:
RF-based ID Tokens

- Most popular options
  - RFID, NFC, BLE tags (incl. wristbands, smartwatches)
- Pros:
  - faster, more convenient than swiping card
  - can track entry and exit
- Cons:
  - more administrative overhead; does not prevent forging
- Options 2.1 vs 2.2:
  - Commercial vs custom solutions, like 1.1 vs 1.2

Option 3.*: Biometrics

- Physical features
  - Face, fingerprint, retina, …
- Pros:
  - difficult to forge identity
- Cons:
  - Speed is unclear?
  - Fingerprint => sanitation issue?
  - Facial recognition => accuracy?
  - Privacy concerns?



Bigger Picture

"Sensor"

ID-card Based	smartphone based	add-on vs. built-in 
	commercial or custom	barcode  QR code  magstripe 
RF token	smartphone based	RFID  NFC 
	commercial or custom	BLE 
Biometric	various solutions	face recognition  fingerprint  retina 

Gateway?

- Bluetooth
- ZigBee
- Wibree
- IR
- WiFi
- cellular

gateway in cellular network

Server

TCP/IP

database

Exploration at higher level

- Think beyond a single unit
  - How will multiple units work together?
  - Is there a limit on the number of units?
- Think beyond scanning action
  - What about administration and management?
  - What kind of data should be collected besides ID?
- Boundary cases
  - What if the network fails? (where is the data kept?)
  - What if one of the units break? (Do you lose all data collected so far?)

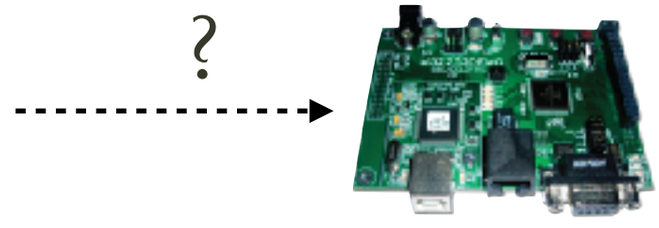
Approach 1: wireless synchronizing card readers

- Multiple readers
  - spread out throughout lecture hall, or scattered in an outdoors event
  - Any reader should be able to check if a person has been scanned by other staff
- Sync with Local Gateway
  - logging data when remote database is down
  - gateway takes care of Internet uplink

Approach 2: Unreliable Link Tolerance

- Gateway-to-Remote database
  - Database may be down; network link may be broken
- Reader-to-Gateway
  - Connection may be broken (too far)

- Best effort:
  - log data locally, propagate up when possible



data storage?

data archive?

Some Detailed Issues: Access Control

- Registering handhelds w/ gateway
  - by MAC address? by proximity? by shaking gesture?
  - how to prevent anyone with a smartphone from just connecting to the gateway
- Session granting
  - how to deputize any smartphone for the session (and not other sessions)?

Your Assignment

- Technology options
  - Classify and explain how it works
  - Add at least one more not covered in lecture
- Discuss the pros & cons in terms of
  - Convenience, efficiency, confirmation, completeness, forgiveness, authenticity, sensitivity, specificity, security, cost
- Selling points
  - List & explain selling points
  - Rank-order the points and explain relative importance

From Paper Project to Your Project

- Apply the exploration to your own project
  - Explore available technologies
  - Think outside the box (but realistic)
- For each technology option
  - Evaluate the pros and cons
  - Think of the selling points, prioritize features