Mobile Security
Fall 2015

Patrick Tague

#10: Mobile Sensing Risks

Announcements

- Reminder: assignment #3 due today

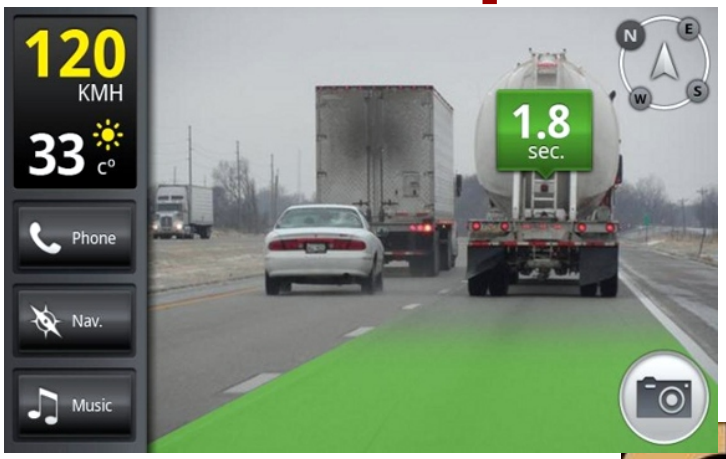
Classes #10-11

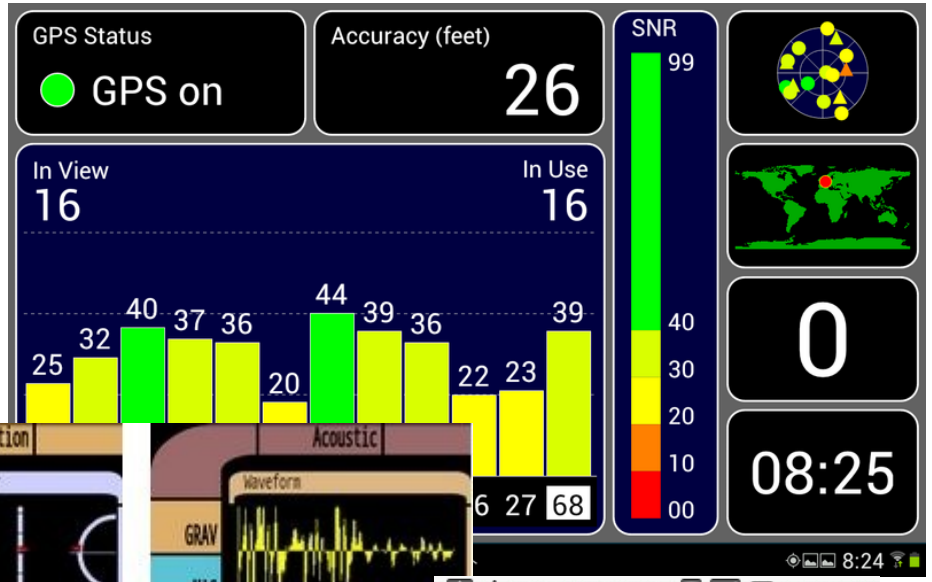
- Sensing in mobile devices
- Risks of mobile sensing
- Benefits of mobile sensing

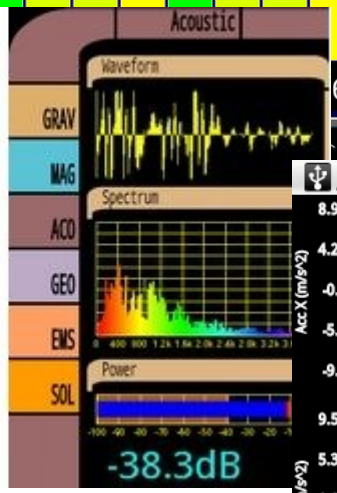
Agenda

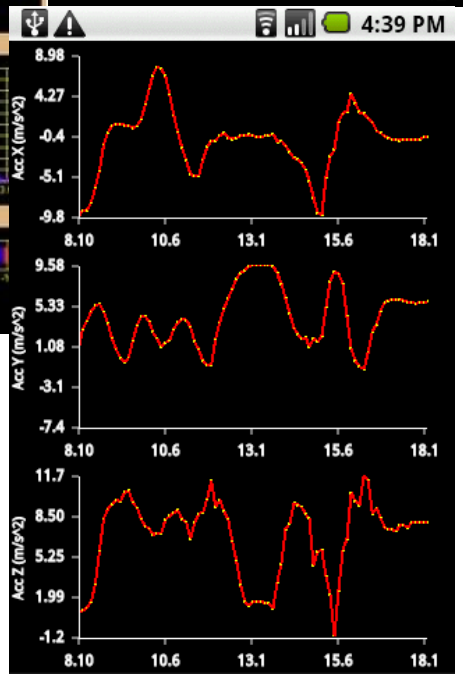
- Smartphone Sensing
  - What sensors are included in mobile phones, and what are they used for?
  - Smartphone sensor networks
  - Security and privacy risks, threats, benefits, etc.

Smartphones have Sensors?







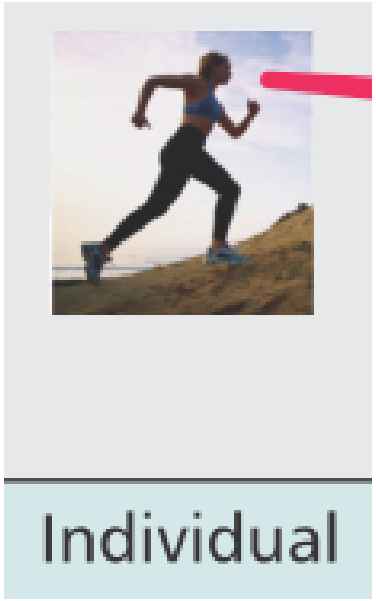


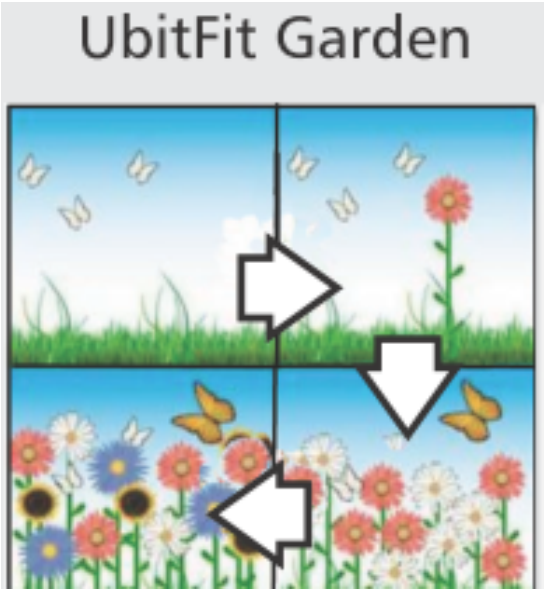
Intended Sensor Uses

- Most commonly:
  - **Accelerometers**, for UI and camera use (initially)
  - **Gyroscope and compass**, for orientation and mobility tracking (e.g., for location-based services)
  - **Proximity sensor**, for features like turning off the screen when against your ear or in your pocket
  - **Light sensor**, for auto-brightness and others
  - **GPS**, for navigation, LBS, photo tagging, etc.
  - **Microphone(s)**, for measuring sound or noise levels
  - **Camera(s)**, for taking pictures, sensing colors, reading IR beacons, measuring heartbeat, etc.
  - Other **radios** (WiFi, Bluetooth, etc. can help LBS)

Sensing Apps

- Mobile apps that leverage sensor data range from small- to large-scale
  - Individual sensor data, used on the phone, can monitor a personal environment

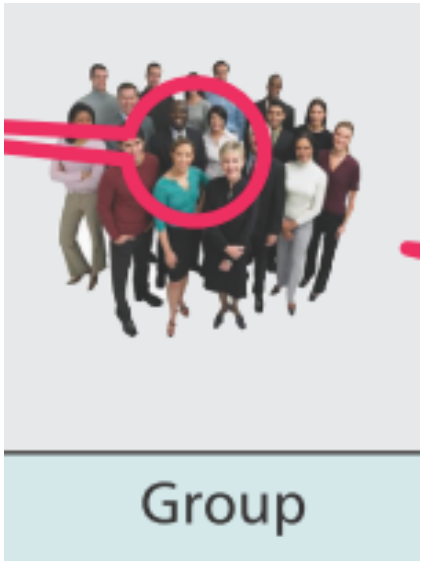




  - Images from [Lane et al., IEEE Comm. Mag., Sept 2010]

Sensing Apps

- Mobile apps that leverage sensor data range from small- to large-scale
  - Group sensor data, shared among a small number of individuals, can enable data- or service-sharing



  - Images from [Lane et al., IEEE Comm. Mag., Sept 2010]

Sensing Apps

- Mobile apps that leverage sensor data range from small- to large-scale
  - Community sensor data, shared among a large number of individuals can enable larger-scale data collection and richer analytics (e.g., Weather Underground)

  - Images from [Lane et al., IEEE Comm. Mag., Sept 2010]

Large Scale Sensing

- A few interesting large-scale sensing apps of note were discussed in [Lane et al., IEEE Comm. Mag., Sept 2010]
  - Traffic monitoring and navigation assistance (e.g., MIT VTrack or Mobile Millenium)
  - Mobile social networking (more on this later)
  - Environmental/pollution monitoring and aggregation (e.g., UCLA PEIR)
  - Health monitoring (e.g., UbiFit Garden, VMA)

Cloud/Crowd Sensing

- Instead of restricting sensor access to the mobile apps themselves, smartphones can be used as nodes in a large-scale sensor network
  - Each phone reports its sensor measurements to a cloud service or crowd-sourcing system
  - Aggregate information is used instead of base measurements
    - Protects the privacy of individual user data???

Sense-Making Systems

- In some cases, the sensor data itself isn't very helpful, but deeper analytics can help us make sense of the sensor data

- More on this during the next class

Unintended Sensor Uses

- Most of the sensors on a mobile phone are treated as “non-sensitive” information sources, and some OS models don't require apps to get permission to access the sensors directly
  - E.g., in Android, the accelerometer isn't a permission-restricted resource
- Malicious apps may be able to access sensor feeds directly to learn about device or user behaviors
- Cloud/crowd services can also use sensor data for purposes other than stated

Sensor Security Issues

- Use of data is difficult to track (basically a supply-chain problem)
- Integrity of sensor data is difficult (impossible?) to verify
  - Crypto-based integrity protection guarantees that the data packet content is as intended, but nothing ensures the measurement was generated correctly and the hardware is functioning as designed
- Scalability
- Privacy of user data

Security Issues

- Potential adversaries can target a number of different aspects of the system, including:
  - Environmental factors: changes to the environment (putting ice around temp sensors, spoofing GPS signals, etc.) affect measurements, need consistency?
  - Sensors: tampered, fabricated, spoofed, malware?
  - Cloud / network: eavesdropping, interception, injection, tracing, etc.?

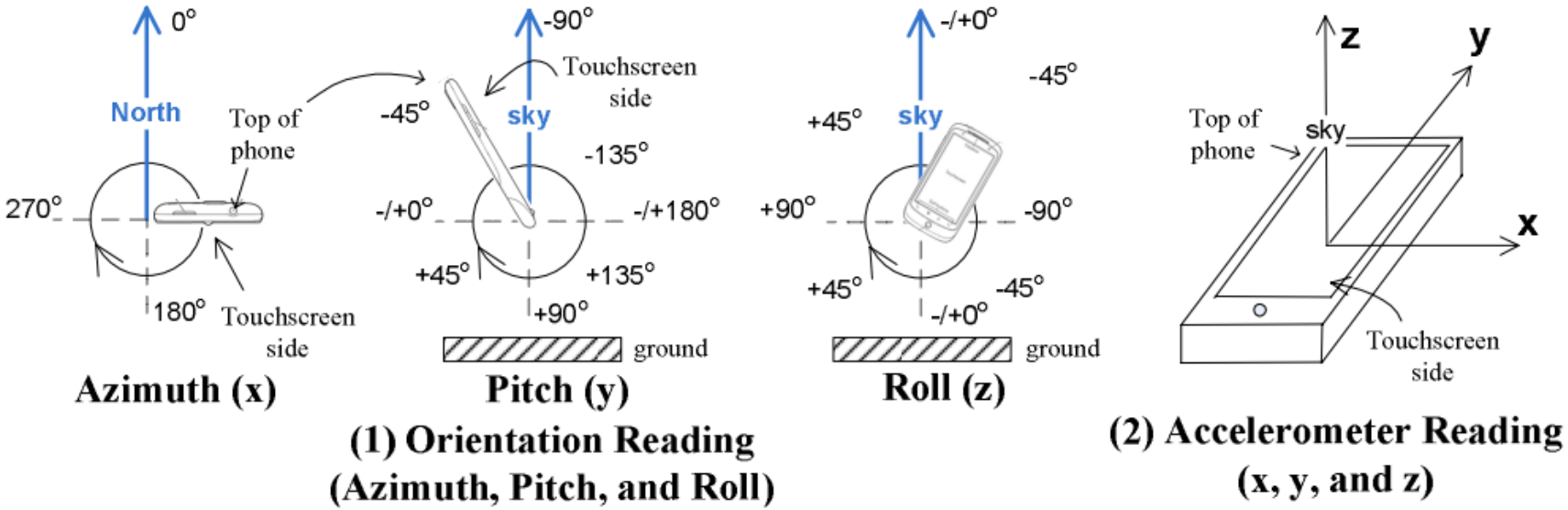
Approaching Secure Solutions

- Consistency checks on all (correlated) data can detect tampering, forgery, etc.
  - Correlation can be geographic (nearby temperature sensors should be similar), temporal (subsequent measurements should be similar), or otherwise
- Strong crypto (device authentication, data integrity, encryption, pub/sub access control)
- Trust management
  - If a sensor gives a bad measurement, give them a bad rating; ignore data from poorly rated devices

Ok, so what about the issues in standalone smartphone apps?

Local Sensor Scenario

- Suppose an attacker gains access to accelerometer and gyro/orientation sensor data



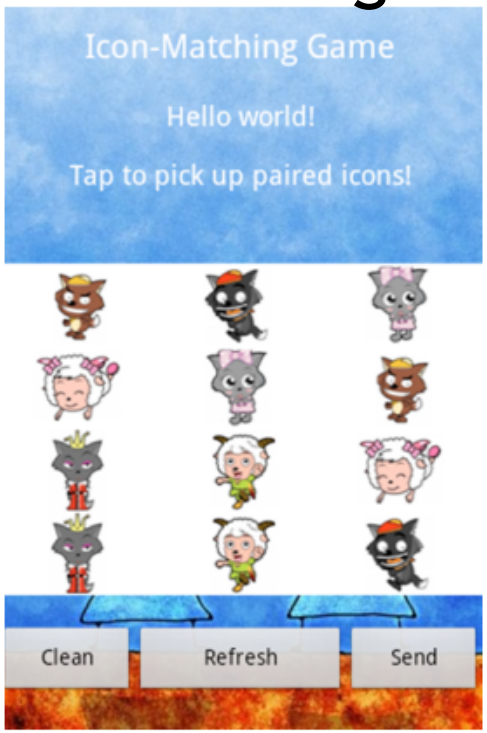
(1) Orientation Reading (Azimuth, Pitch, and Roll)

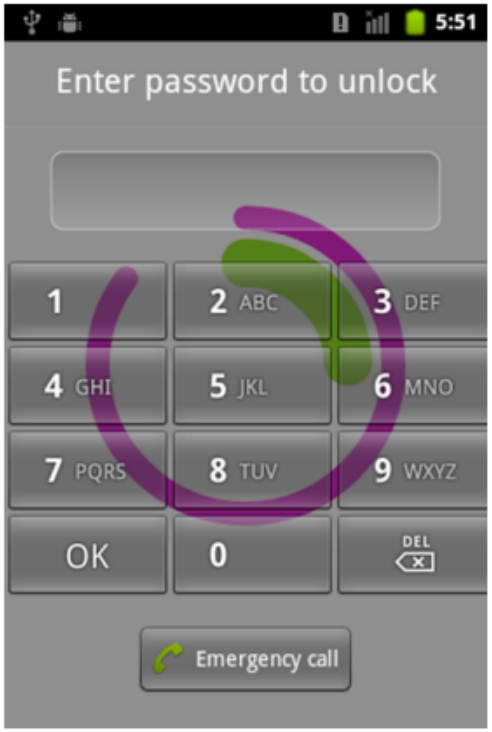
(2) Accelerometer Reading (x, y, and z)

- What can they do?

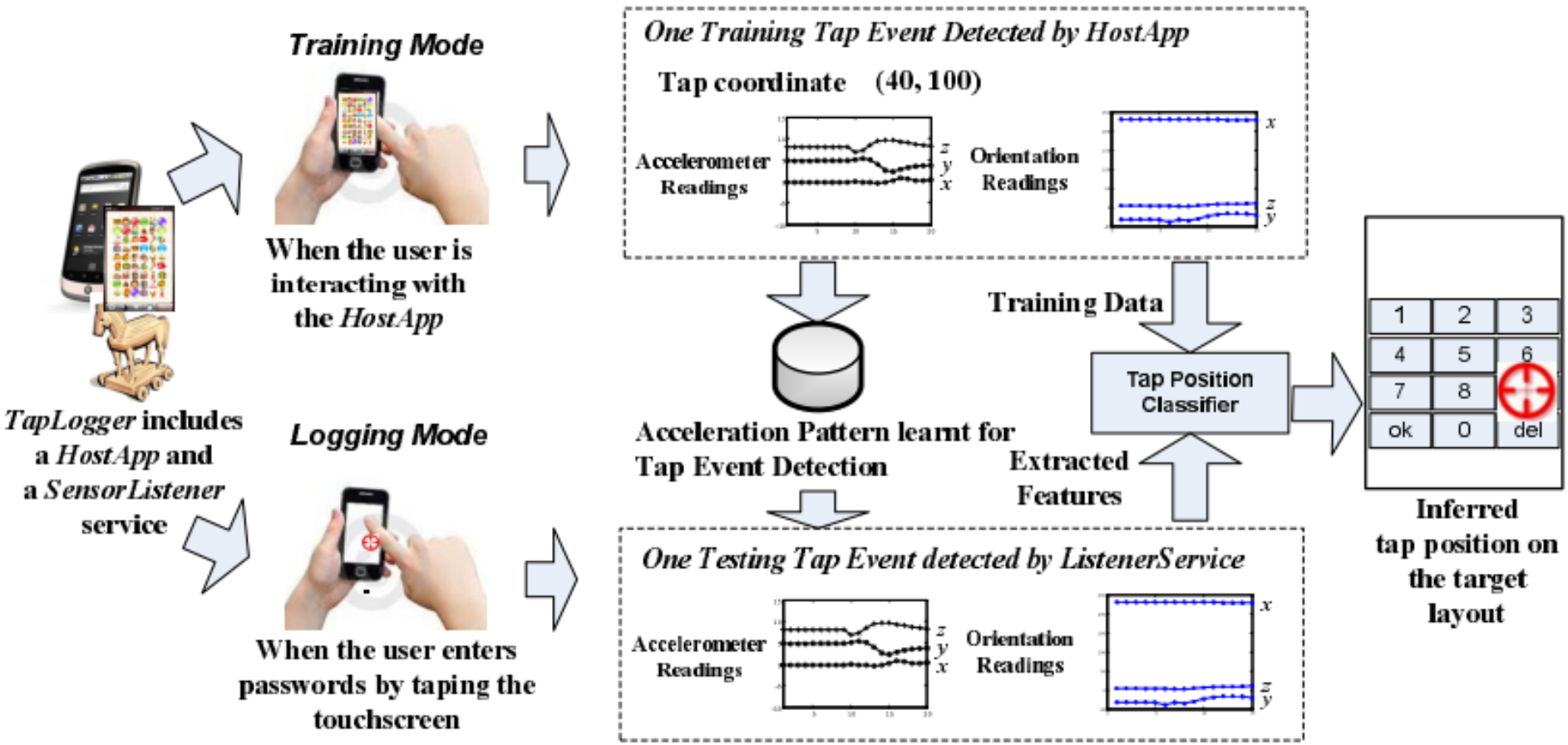
TapLogger Threat

- Xu, Bai, and Zhu [WiSec 2012] designed TapLogger to demonstrate possible sensor data risks
- TapLogger tricks users into providing training data, then uses the training data to learn PINs

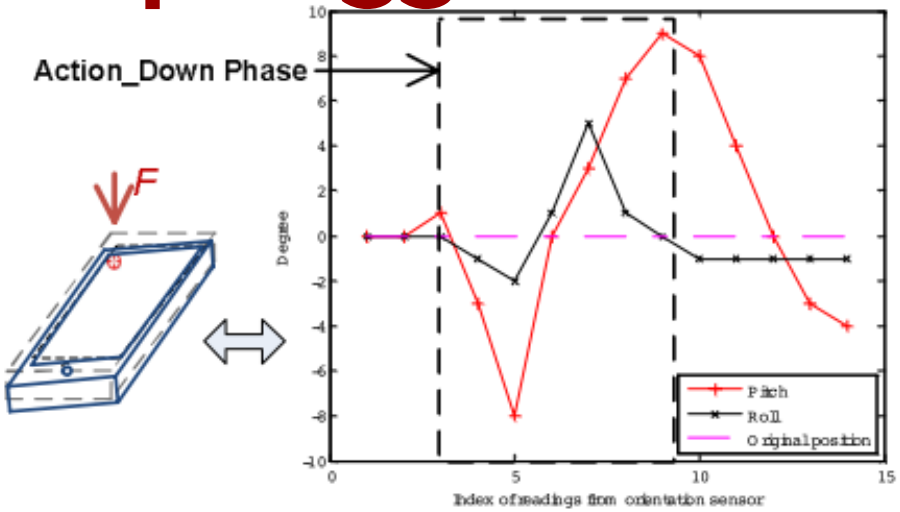




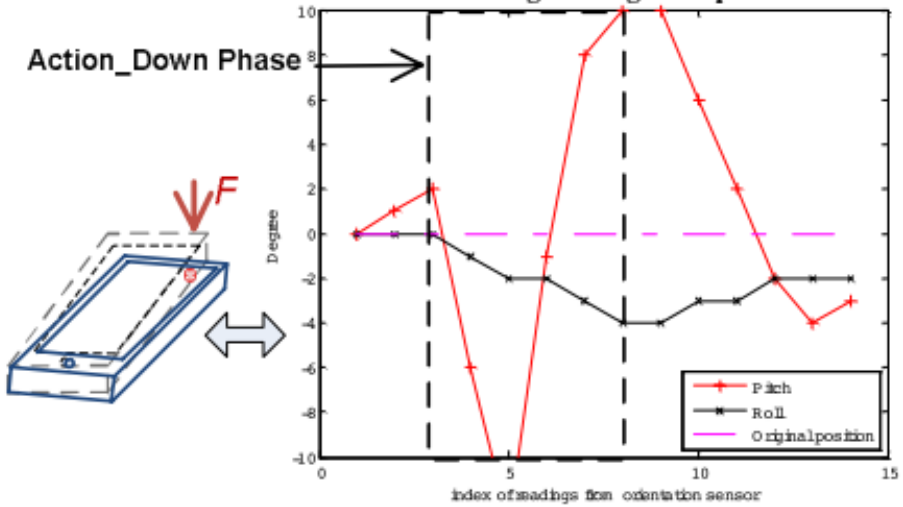
How Does it Work?



TapLogger Data



(1. a) when tapping the top left area of touchscreen (1.b) corresponding orientation sensor readings during the tap event



(2. a) when tapping the top right area of touchscreen (2.b) corresponding orientation sensor readings during the tap event

How Well Does it Work?

Layout of Number Pad		
1	2	3
4	5	6
7	8	9
*	0	#

Coverage rate with Top 1 ranked label		
0.2759	0.4643	0.5185
0.4138	0.1200	0.3333
0.2069	0.1250	0.2500
0.4348	0.3462	0.8750

Coverage rate with Top 1 & 2 ranked labels		
0.7931	0.75	0.7037
0.6897	0.4400	0.6061
0.4483	0.2917	0.6250
0.6087	0.4615	0.9583

Coverage rate with Top 1 & 2 & 3 ranked labels		
0.9310	0.8214	0.9259
0.8621	0.7200	0.9091
0.6897	0.5833	0.8333
0.6522	0.6154	0.9583

Coverage rate with Top 1 & 2 & 3 & 4 ranked labels		
0.9310	0.9286	0.9259
0.9655	0.8400	0.9394
0.8966	0.6250	1.0
0.8261	0.7692	1.0

Why Does it Work?

- We've been training users to always check the permissions the apps are asking for before clicking install (which they still don't do)

- In this case, it doesn't help, because the accelerometer is an unprotected resource, so no permissions are needed

- Should the accelerometer be a protected resource? What else should be protected?

More Sensor-Based Threats

- CMU researchers also showed that accelerometer readings can be used to expose:
  - Text entered into soft keyboards; ACCessory uses techniques sort of similar to what TapLogger did for 10-key pad
  - Driving route and starting location; ACComplice does location inference using probabilistic inertial navigation with map matching

What are the open research questions related to smartphone sensing security?

Sensing Challenges

- As in any sensor system, the quality and correctness of sensor measurements are fundamentally questionable
  - Consistency checks have been widely adopted in the WSN community and quickly spreading elsewhere
- Scalability of secure sensing platforms is hard
  - Key management, energy limits, bandwidth limits, computation limits, trust issues, …
- Privacy is a huge problem
  - Privacy of the data versus privacy of what can be learned from the data...

Oct 27:
Mobile Sensing Benefits