Smart Phones: Tracking Your Every Move
By Jon Martin
Purpose

• Discuss the current and future security risks caused by the individual and combined smartphone sensors

• Data bases that collect this data
Smartphones

• New Smartphones contain 20+ sensors (see figure 1)

• Measure every aspect of our lives

• Many beneficial reasons to collect smartphone data.

• Data can be collected to infer and predict human behavior.

See Table 1 for explanation on some of these sensors. See Table 2 for smartphone sensor applications.
Figure 1: Smart Phone Sensors

[Communication]
Cell Phone
Wi-Fi
Bluetooth
NFC
IrLED
Microphone

[Location]
GPS
Magnetic Field

[Optical]
Camera (16MP)
4K Video
360° Video
Barcode scanner
Night Vision (IrLED)

[Health / Emotion]
Heart Rate Sensor
Perspiration
Microphone

[Environment]
Temperature
Altimeter
Barometer
Humidity
RGB Ambient Light

[Motion]
Accelerometer
Linear Acceleration
Gravity
Gyroscope
Hall
Orientation
Pressure
Proximity
Rotation

[Human]
Finger Print Reader
Touch Screen
<table>
<thead>
<tr>
<th>SENSOR</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
<th>COMMON USES</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCELEROMETER</td>
<td>H/W</td>
<td>Measures the acceleration force in m/s² that is applied to a device on all three physical axes (x, y, z), including the force of gravity.</td>
<td>Motion detection (shake, tilt, etc.).</td>
</tr>
<tr>
<td>AMBIENT TEMPERATURE</td>
<td>H/W</td>
<td>Measures the ambient room temperature in degrees Celsius (°C).</td>
<td>Monitoring air temperatures.</td>
</tr>
<tr>
<td>GRAVITY</td>
<td>S/W or H/W</td>
<td>Measures the force of gravity in m/s² that is applied to a device on all three physical axes (x, y, z).</td>
<td>Motion detection (shake, tilt, etc.).</td>
</tr>
<tr>
<td>GYROSCOPE</td>
<td>H/W</td>
<td>Measures a device’s rate of rotation in rad/s around each of the three physical axes (x, y, and z).</td>
<td>Rotation detection (spin, turn, etc.).</td>
</tr>
<tr>
<td>LIGHT</td>
<td>H/W</td>
<td>Measures the ambient light level (illumination) in lx.</td>
<td>Controlling screen brightness.</td>
</tr>
<tr>
<td>LINEAR ACCELERATION</td>
<td>S/W or H/W</td>
<td>Measures the acceleration force in m/s² that is applied to a device on all three physical axes (x, y, z), excluding the force of gravity.</td>
<td>Monitoring acceleration along a single axis.</td>
</tr>
<tr>
<td>MAGNETIC FIELD</td>
<td>H/W</td>
<td>Measures the ambient geomagnetic field for all three physical axes (x, y, z) in μT.</td>
<td>Creating a compass.</td>
</tr>
<tr>
<td>ORIENTATION</td>
<td>S/W</td>
<td>Measures degrees of rotation that a device makes around all three physical axes (x, y, z).</td>
<td>Determining device position.</td>
</tr>
<tr>
<td>PRESSURE</td>
<td>H/W</td>
<td>Measures the ambient air pressure in hPa or mbar.</td>
<td>Monitoring air pressure changes.</td>
</tr>
<tr>
<td>PROXIMITY</td>
<td>H/W</td>
<td>Measures the proximity of an object in cm relative to the view screen of a device. This sensor is typically used to determine whether a handset is being held up to a person’s ear.</td>
<td>Phone position during a call.</td>
</tr>
<tr>
<td>RELATIVE HUMIDITY</td>
<td>H/W</td>
<td>Measures the relative ambient humidity in percent (%).</td>
<td>Monitoring dew point, absolute, and relative humidity.</td>
</tr>
<tr>
<td>ROTATION VECTOR</td>
<td>S/W or H/W</td>
<td>Measures the orientation of a device by providing the three elements of the device’s rotation vector.</td>
<td>Motion detection and rotation detection.</td>
</tr>
<tr>
<td>TEMPERATURE</td>
<td>H/W</td>
<td>Measures the temperature of the device in degrees Celsius (°C).</td>
<td>Monitoring temperatures.</td>
</tr>
</tbody>
</table>
Table 2: Smartphone Sensor Application Examples

<table>
<thead>
<tr>
<th>[Scientific Uses]</th>
<th>[Health Care]</th>
<th>[Location Services]</th>
<th>[Future Uses]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thermal Vision</td>
<td>Personality Diagnoses</td>
<td>Assisted GPS/GLONASS</td>
<td>Air Quality</td>
</tr>
<tr>
<td>Florescent Microscope</td>
<td>Physical Disorders</td>
<td>Digital compass</td>
<td>Mind Control of Devices</td>
</tr>
<tr>
<td>Chemical Air Sensor</td>
<td>Exercise Objectives</td>
<td>Predictive Modeling</td>
<td>UV Light</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td>Ultrasound</td>
</tr>
<tr>
<td>3D Mapping</td>
<td></td>
<td></td>
<td>Radar/Sonar</td>
</tr>
<tr>
<td>Weather Station</td>
<td></td>
<td></td>
<td>Predictive Modeling</td>
</tr>
<tr>
<td>Predictive Modeling</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** There are approximately 1.5 million smartphone applications. Only 40% are used, 25% are only used once after installation. 10
Current Security Threats

• Today’s cell phones are standard equipment for billions of people.

• As of 2014, there are 6.9 billion cell phone subscriptions worldwide, with 90% of American adults owning a cell phone, and 58% of American adults owning a smartphone.³

• It is well known that computers and smartphones are targets of malicious malware intent on stealing money and information; however, there is another privacy concern relating to smartphone sensors (see Table 3).

• Smartphones can provide many benefits with their 20+ sensors.

• Sensors common on new smart phones may hide a potential for misuse.

• Sensors can tell us your location, how fast you drive your car, know that the phone is being viewed, just being held, and whether or not the owner has possession of the smartphone.
Current Security Threats

• Many inferences could be made about the user by all this sensor data.

• The following is the ramifications of using one sensor.

  – “The United States Court of Appeals for the District of Columbia Circuit stated that GPS data can reveal whether a person is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts”. \(^{11,12}\)

• All sensors on a smart phone are tracking the user.

• What happens when 2 or 3 of these sensors are used in concert to collect data?

• What happens when **ALL** these sensors are used in concert to collect data?

• One of the first losses of privacy due to correlation of sensor data was with photographs tagged with GPS data (camera + GPS) called **Geo-Tagging**.

  – A picture on Facebook can tell anyone where military personnel are deployed.
### Table 3: Smartphone Sensor Security Threat (Examples)

- **Surreptitious forms of communication**
  - a. Speaker to microphone
  - b. Sub-audible tones
  - c. Infrared
  - d. Gyroscope (as a microphone)
  - e. Accelerometer (detect key strokes)

**Cheap fabrication of new smartphone sensors**

**Hijack Project examples**

![Hijack Project examples](image)

**Attaches to iPhone ($349)**

- FLIR One Thermal Imaging / Enhanced Night Vision / See Through Walls

![Attaches to iPhone](image)

- 3-D mapping

**Google Tango 3-D Phone**

- Google Tango 3-D Mapping

![Google Tango 3-D Phone](image)

- 3-D mapping
Misuse

- Smartphone sensors can be misused by applications and internet browsers built into the smartphones. Certain smartphone operating systems have no mechanism to prevent access to some sensors (See Table 4).

- Accelerometer sensor can be used to determine keystrokes (record passwords)

- Gyroscope sensor can be used like a microphone (record conversations)\(^7,8,9\)

- Smartphones can be uniquely identified using several sensors and other aspects of the smartphone

- Thermal Cameras (FLIR for iPhone) can be used to steal ATM pin codes\(^18\)

| [Finger Printing Methods]\(^5\) | Note: Due to the uniqueness of imperfections, some sensors offer less varying degrees of accuracy. Combining sensors could allow for more accurate fingerprinting that positively identifies and tracks smart phone users.  
The following finger printing methods are not done with smartphone sensors:  
(a) Date and time that a phone first went online, as well as the date and time that a phone last went offline.  
(b) Total number of calls, and the ratio of unique contacts to calls |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Finger print</td>
<td></td>
</tr>
<tr>
<td>Human Voice</td>
<td></td>
</tr>
<tr>
<td>How Person Walks</td>
<td></td>
</tr>
<tr>
<td>How Phone is Held</td>
<td></td>
</tr>
<tr>
<td>Radio Transmitter</td>
<td></td>
</tr>
<tr>
<td>Accelerometer</td>
<td></td>
</tr>
<tr>
<td>Other sensors</td>
<td></td>
</tr>
</tbody>
</table>
Inference of Human Behavior

• Current data analysis techniques can use smartphone sensor data to infer (examples):

  • Past, Present Location

  • Purpose of travel (Groceries, Gas, Bank, etc.)

  • Driving Habits

  • Physical Activity (laying, sitting, standing, walking (level, up, down))

  • Situational Activity Awareness

  • Physical & Mental Health

  • Emotional State
Prediction of Human Behavior

- Current data modeling predictions can use smartphone sensor data to predict (examples):
  - Future Location \(^{17}\)
  - Future Purchases
  - Disease Progression
Benefits & Consequences

• The uses of human behavior inference and prediction could have many benefits and misuses such as:

  • Marketing company knows that while you are stressed (voice analysis) you can be easily influenced (text coupon) to go to a specific bar (near you) and order a drink (favorite).

  • Based on road conditions, car models, driving history and current emotional state, emergency planners could predict there is a high percentage chance there will be a vehicle accident and pre-stage emergency personnel.

  • Police could automatically issue a speeding ticket

  • Insurance company could change your insurance rates (driving habits)

  • Criminal organizations know that while you are stressed out, at a bar drinking alcohol you are now more susceptible to influence.
DOCTOR FUN

NSA TRACKING DEVICES

“Yeah - we used to call them cell phones.”
Historical Data Collection and Analysis Threat

- Figure two is a **Code Breaking** example of how the Allies broke encrypted Japanese messages which completely exposed years of their military secrets. The data was considered safe from misuse (protected by encryption) but now, due to data analysis, it is completely exposed (See Figure 2).

**Figure 2: Japanese Code Breaking example**
Current & Future Data Collection and Analysis Threat

- Figure two is a **data collection** example of how years of a persons private data is collected (See Figure 5). The data was assumed harmless, but now, due to data analysis, many different meanings and purposes can be derived.

Figure 5: is a data collection example of your cell phone data with the possible dire consequences
Current Smartphone Sensor Data Collection and Analysis Threat

- Current process of smartphone sensor data collection (See Figure 3)

1. Software Agent is installed on a smartphone

2. Software Agent sends smartphone sensor data to a data base over the internet

3. Data base stores smartphone sensor data

4. Analysis techniques infer and predict human behavior

Figure 3: Smartphone sensor data collection
Future Smartphone Sensor Data Collection and Analysis Threat

• Now compare collected encrypted messages to a smartphone sensor database.

• Future analysis will eventually “break the code” on uncorrelated information on smartphone sensor data.

• What this means is new analysis techniques will “connect the dots” on what was previously considered unrelated data and infer very private information and unleash a whole new era of complete and total loss of privacy.

• The “Sleeping Security Threat” is years of “harmless” smartphone sensor data sitting in a database that becomes very dangerous overnight due to new analysis techniques.

• Users can choose to stop using their smartphones, but will have no control over old data bases that hold years of their now very personal information.

• This new analysis technique will provide information that infers and predicts important human behavior with a high level of accuracy to marketing companies, health care providers, future planners, police departments, intelligence agencies and criminals.

• Although beneficial in many ways, some organizations will choose to abuse this intimate knowledge (See Figure 4).
Figure 4: Ground breaking smartphone sensor analysis with unforeseen consequences

Smartphone → Sensor Data → Database (Indefinite Storage) → Future Analysis Techniques → Complete and Total Loss of Privacy

4K, 360°, IR LED, Camera, Microphone, GPS, Health, Database, Future, Privacy

The flowchart illustrates the process from a smartphone capturing sensor data, which feeds into a database for indefinite storage. This leads to future analysis techniques, ultimately resulting in complete and total loss of privacy.
Future of Smartphone Sensors

• Current trend in smartphone technology is to install as many sensors as possible

• More privacy concerns

• New threat vectors
Recommendations

• Further study is recommended to catalogue smartphone sensor threats.

• Discussion questions for organizations (examples):
  
  – How are our smartphones sensors being used in applications and internet browsers?
  
  – What are the data analysis techniques available now and in the future?
  
  – What intelligence can be obtained when all smartphone sensor data is completely correlated?
  
  – How much damage can an insider do with a smartphone?
  
  – What organizations are collecting smartphone sensor data?
  
  – Who has access to the smartphone data (smartphone owner, manufacturer, phone company, marketing companies, domestic governments, foreign governments, intelligence agencies and criminal organizations)?
  
  – What organizations are correlating smartphone sensor data with new analysis techniques?
  
  – What organizations are at the leading edge of data base correlation?
  
  – Can and/or should an organization restrict/prevent the collection of smartphone sensor data?
  
  – Should all smartphone sensor data be considered Personally Identifiable Information (PII)?
  
  – Should laws be passed that put limits on data collection?
Bibliography


