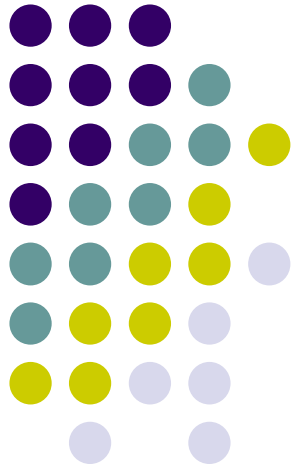
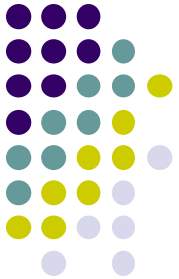
CS 4518 Mobile and Ubiquitous Computing

Lecture 11: Quantified Self, Smartwatches, Android Wear, Energy Efficiency, Security

Emmanuel Agu





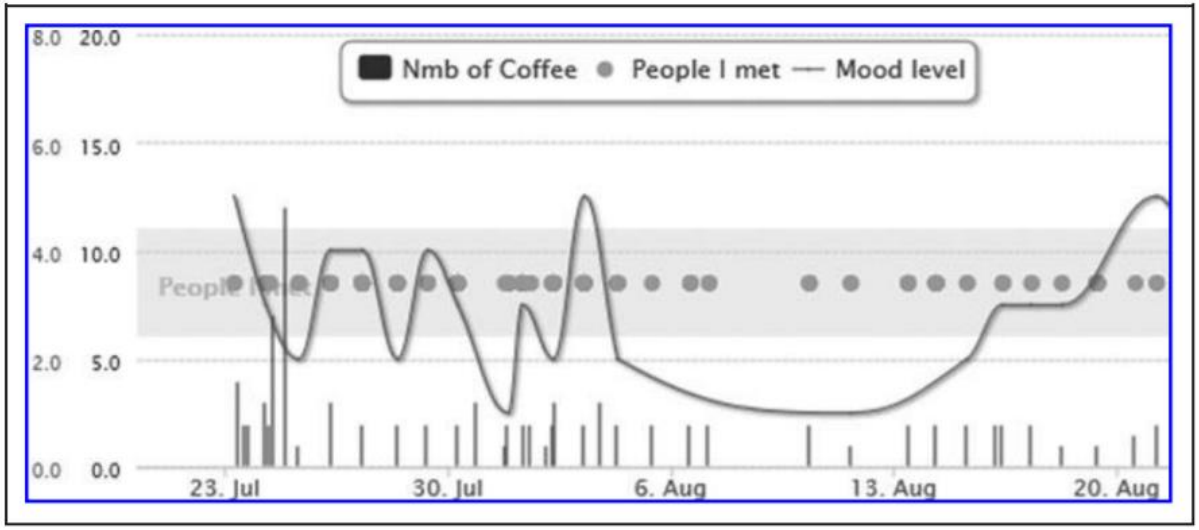
Quantified Self

Quantified Self (QS)

- QS: Community of People who want to measure, log, share metrics about various aspects of their lives. E.g.
  - Sleep, daily step count, food consumed, air quality, mood, etc.
- **Defn:** Obtaining self-knowledge through self-tracking
- Also known as personal informatics or lifelogging
- Measurements typically done using wearables/technology
  - Activity trackers, pedometer, sleep tracker, calories burned, etc
  - Now more available, cheaper

QS: Why Track?

- Why track? To figure out causes of certain behaviors, improve health/wellness
  - E.g. Why do I feel tired on Friday afternoons?
- Data to back up your choices/decisions
  - Did that 2nd cup of coffee make you more productive?
- Discover new patterns that are fixable
  - Whenever I go to my mother's house, I add at least 5 pounds on Monday morning
  - Am I happier when I meet more people or when I drink more coffee?



Courtesy
Melanie Swan

QS: How Popular?

- 69% of US adults already track at least 1 health metric (Pew Research)
- Local meetings, conferences, website
  - quantifiedself.com/

QS Wellness Tracking Devices

Smart fork: eating/calories

Sleep manager

Bluetooth scale

Body worn activity trackers
(steps, activities, calories)

Quantified Self Big Picture

1. Track

Physiological

Eating

Exercise

Sleep

Weight

Blood pressure

Heart rate

Stress

+ Other Context

Location

Travel

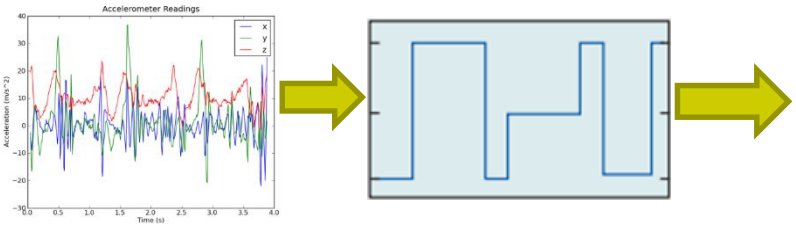
Calendar

Email

Lab results

2. Analyze

Machine Learning



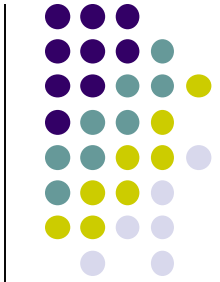
Regression, classification, etc

3. Inform

Mobile App

Hire Coach/Dr

Mymee.com (data-driven coaching)



Smartwatches + Wearables

Main Types of Wearables

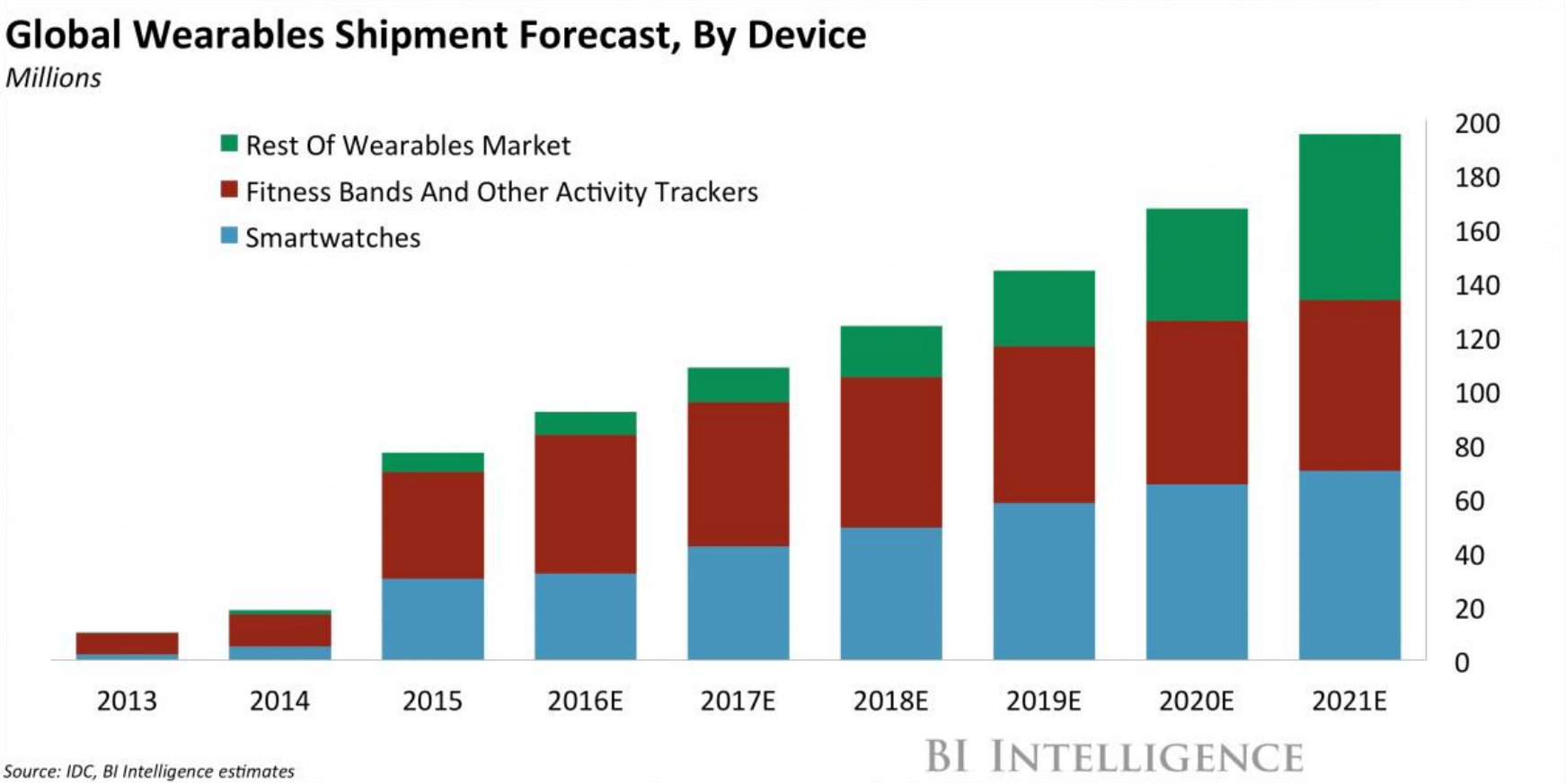
- **Activity/Fitness Trackers:**
  - physiological sensing (activity, step count, sleep duration and quality, heart rate, heart rate variability, blood pressure, etc)
  - E.g. Fitbit Charge 2
- **Smartwatches**
  - Some activity/fitness tracking
  - Also programmable: notifications, receive calls, interact/control smartphone
  - E.g. Apple watch, Samsung Gear

Fitbit Charge 2

Apple Watch

Samsung Gear 2 SmartWatch

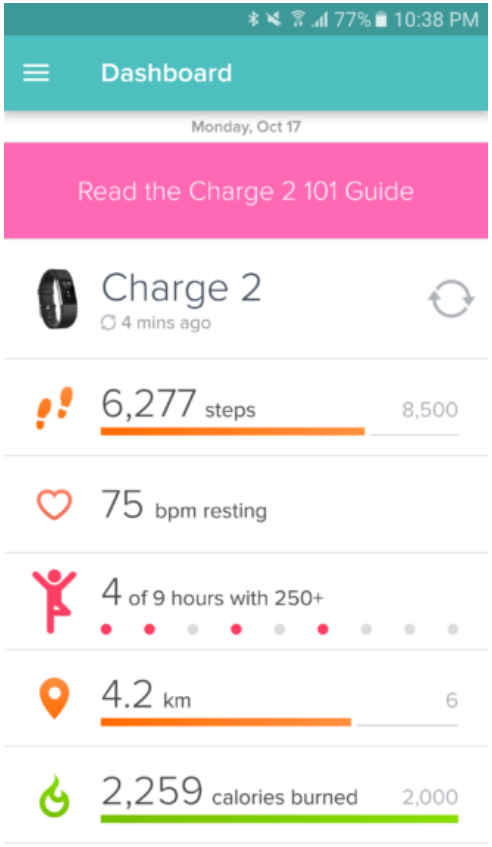
How Popular are Smartwatches/Wearables?



Wearables Example: Fitbit Charge 2

Fitbit Charge 2

synchronize

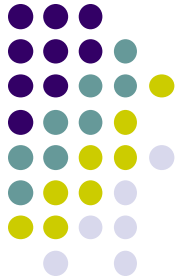


Smartphone companion app
(displays all variables tracked)

Example: Samsung Gear SmartWatch Uses

Image credits: Samsung

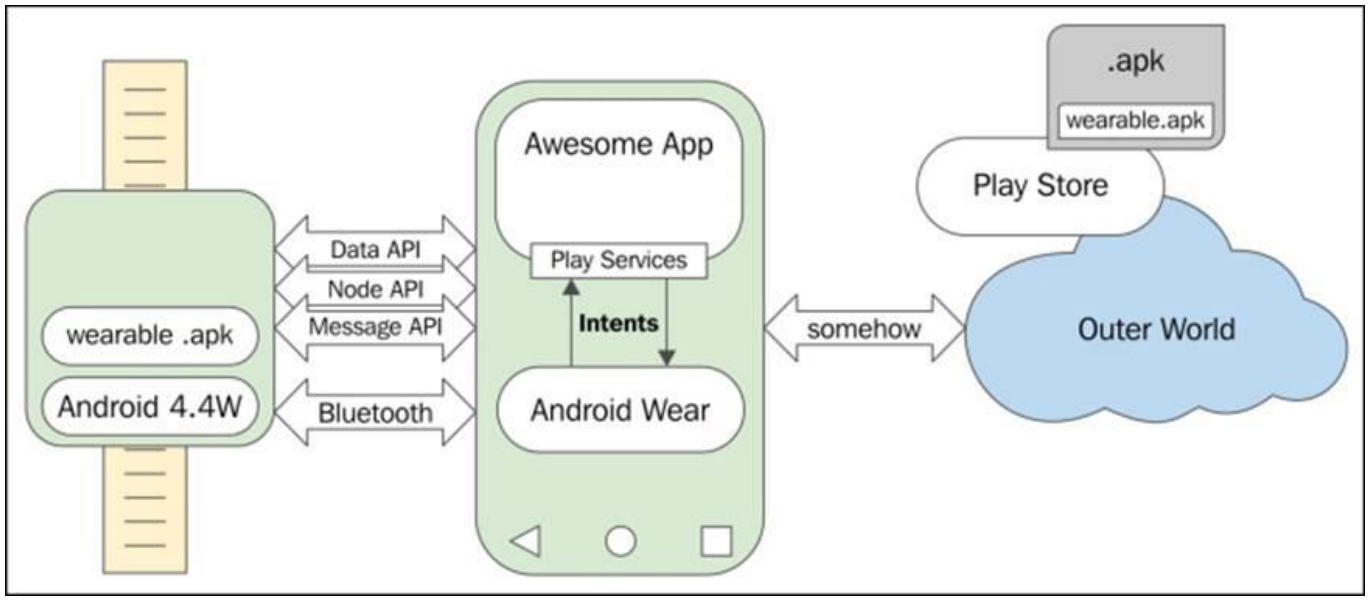
SmartPhone Vs Smartwatch



- Smartphone
  - pros:
    - More processing power, memory, sensors
    - More programming APIs
  - Cons:
    - Sometimes not carried (Left on table, in pocket, bag, briefcase, gym locker)
    - Smartphone on person ~50% of the time (Anind Dey *et al*, Ubicomp 2011)
    - Why? Sometimes inconvenient, impossible (e.g when swimming)
    - Consequence: Missed activity (steps, activity, etc), incomplete activity picture
- Smartwatch:
  - Lower processing power, memory, sensors, but always carried
  - Can sense physiological variables continuously

Programming Android Wearables

- Programmable using Android Wear (latest version is 2.8)
- Supported by Android Studio
- Needs to be connected to a smartphone (via Bluetooth)
- Architecture, 3 main APIs:
  - **Node API:** manages all connections/disconnections (E.g. wearables, smartwatches)
  - **Message API:** Used to send messages between wearable and smartphone
  - **Data API:** Used to synch data between app and smartwatch

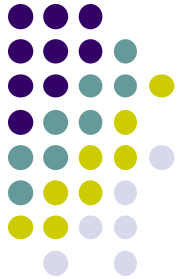


A bit outdated, but nice overview for Android Wear for kitkat Android 4.4W

Android Wear Evolution

https://en.wikipedia.org/wiki/Android_Wear

Android Wear Version	Android Smartphone Version	Release Date	Major New Features
4.4W1	4.4	June 2014	Initial release at Google I/O 2014
4.4W2	4.4	Oct 2014	GPS support, music playback
1.0	5.0.1	Dec 2014	Watch face API (face design) Sunlight & theater modes, battery stats
1.1	5.1.1	May 2015	WiFi, Drawable Emojis, Pattern Lock, swipe left, wrist gestures
1.3	5.1.1	Aug 2015	Interactive Watch Face, Google Translate
1.4	6.0.1	Feb 2016	Speaker support, send voice messages
1.5	6.0.1	June 2016	Restart watch, Android security patch
2.0	7.1.1	Feb 2017	UI revamp (material design, circular faces), watch keyboard, handwriting recognition, cellular support
2.8	8.0.0	Jan 2018	Glanceable notification, dark background support

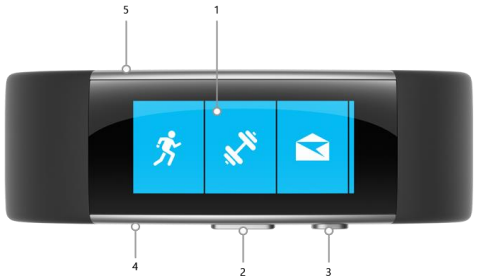


Physiological Sensing

Wearables for Physiological Sensing

- Some wearables measure more physiological signals
  - Cardiac rhythms (heartbeat), breathing, sweating, brain waves, gestures, muscular contractions, eye movements, etc
- Basis Health tracker: heart rate, skin temperature, sleep
- Microsoft Band 2: Heart rate, UltraViolet radiation, Skin conductance

Basis Health tracker



Microsoft Band 2

Empatica E4 WristBand

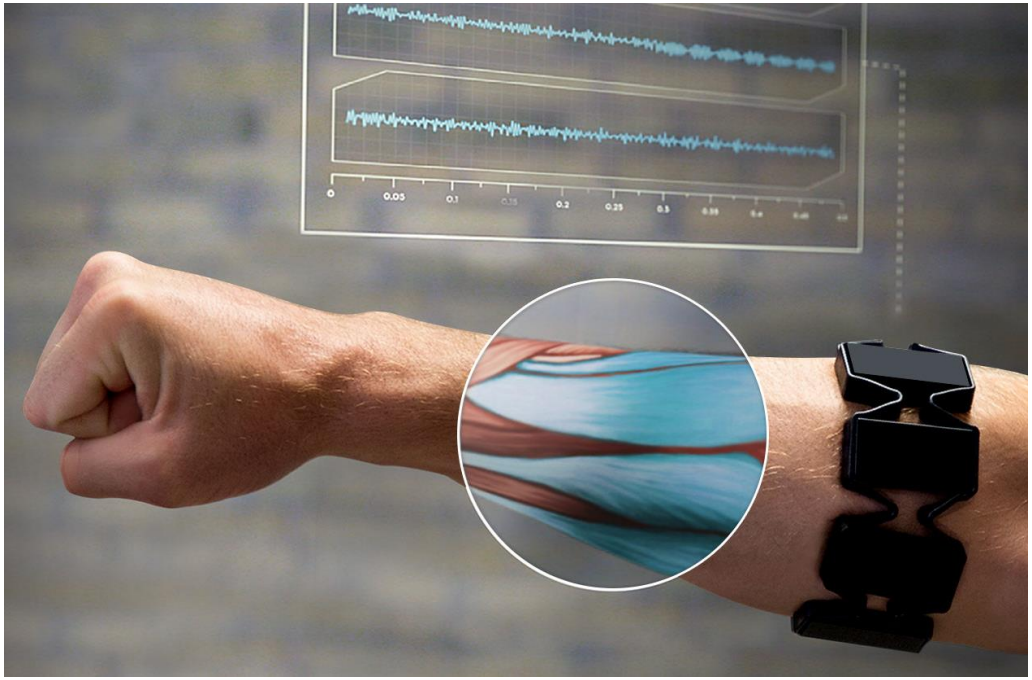
- Wristband measures physiological signals real time (PPG, EDA, accelerometer, infra-red temperature reader)

E4 wristband

Companion app

Myo Armband

- Measures muscle contraction (electromyography or EMG), to detect gestures



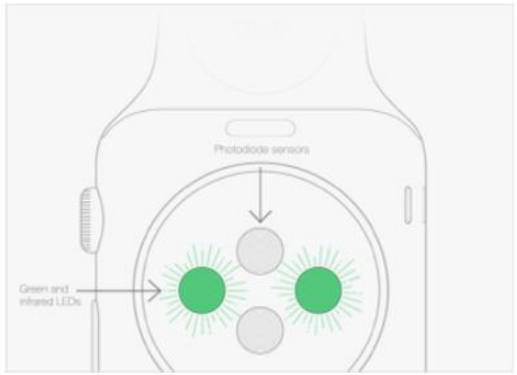
Photoplethysmography (PPG)

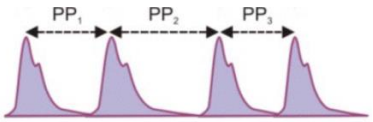
- **PPG:** Non-invasive technique for measuring blood volumes in blood vessels close to skin
- Now popular non-invasive method of extracting physiological measurements e.g. heart rate or oxygen saturation

Pulse Oximeter

Smartphone/Smartwatch PPG: Estimating HR

- **Principle:**
  - Blood absorbs green light
  - LED shines green light unto skin (back of wrist)
  - Blood pumping changes blood flow and hence absorption rhythmically
  - Photodiode measures rhythmic changes in green light absorption => HR





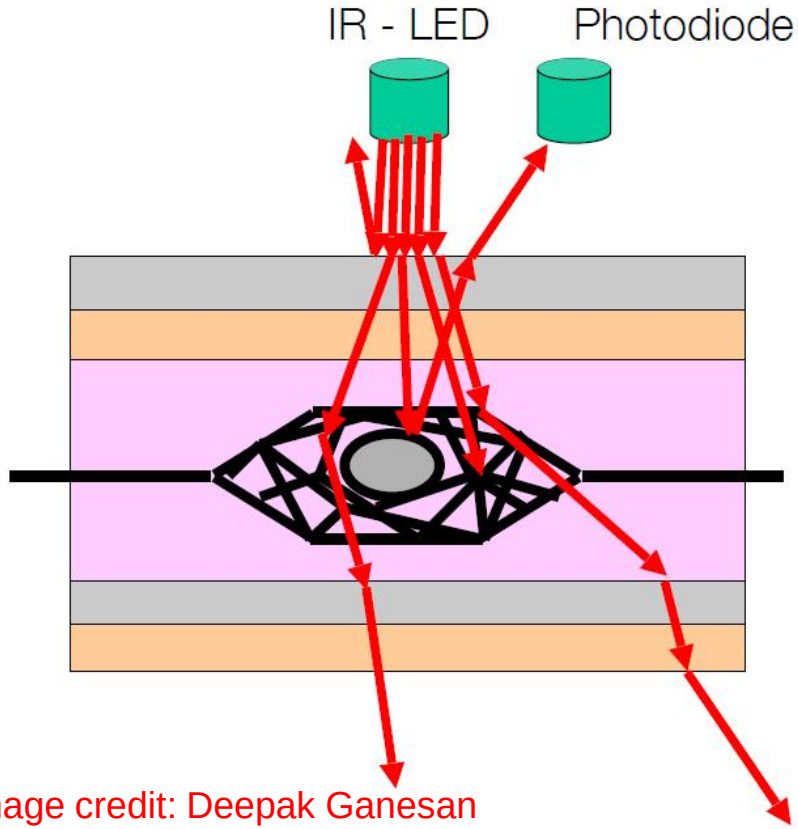
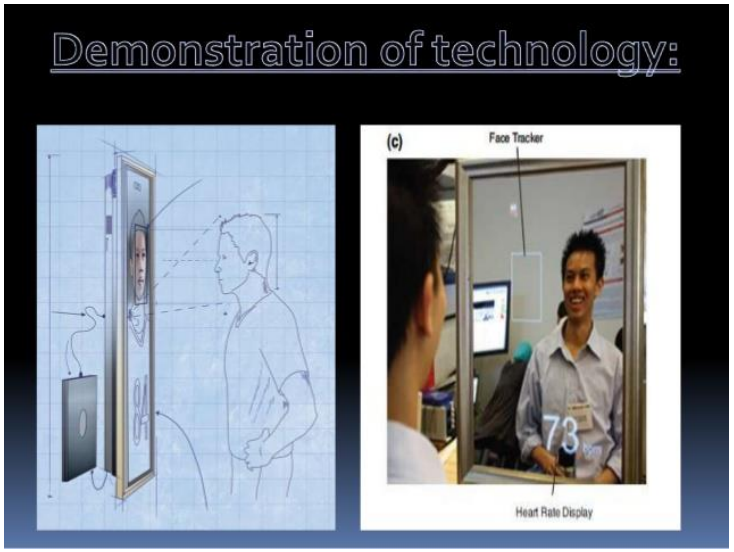


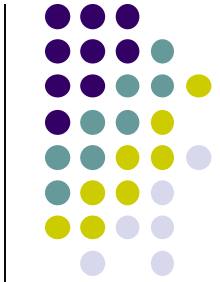
Image credit: Deepak Ganesan

Smartphone PPG: Heart Rate Detection

- Like smartwatch, use camera flash (emitter), camera as detector
- Place finger over smartphone's camera, shine light unto finger tip
- Heart pumps blood in and out of blood vessels on finger tip
  - Changes how much light is absorbed (especially green channel in RGB)
  - Causes rhythmic changes of reflected light
- **PPG also possible on other devices. E.g. Medical mirror**



MZ **Poh**, D McDuff, R Picard A medical **mirror** for non-contact health monitoring, ACM SIGGRAPH 2011



Energy Efficiency

Problem: Battery Power is Scarce!!

- Battery energy is most constraining resource on mobile device
- Most resources (CPU, RAM, WiFi speed, etc) increasing exponentially *except* battery energy (ref. Starner, IEEE Pervasive Computing, Dec 2003)

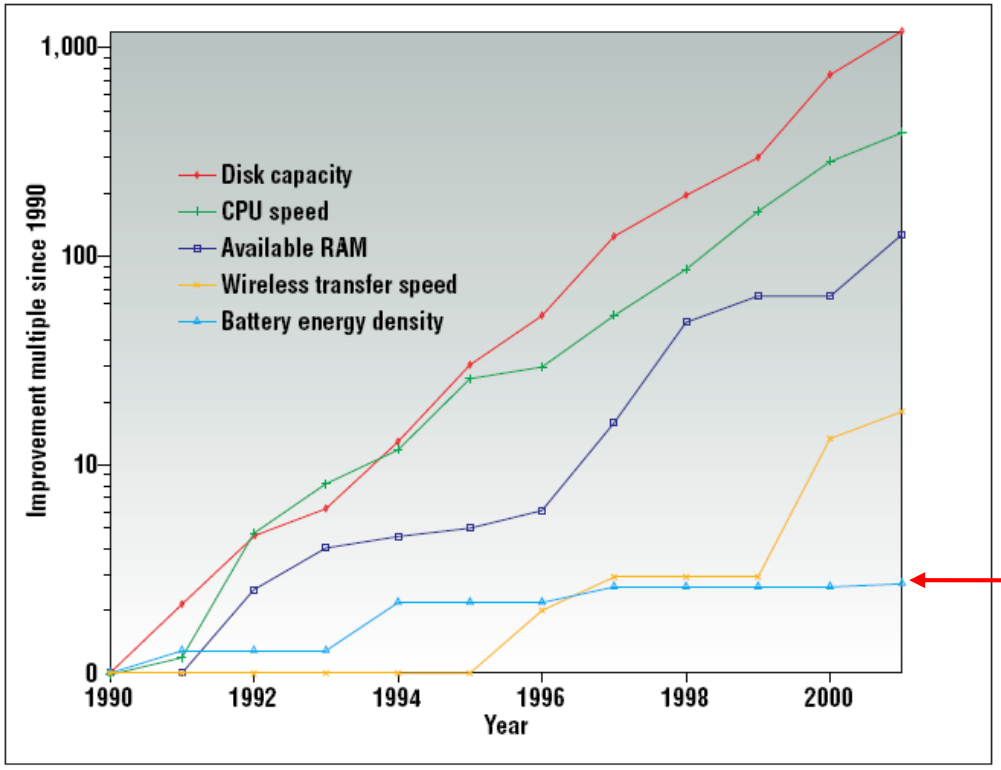
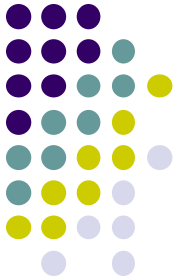


Figure 1. Improvements in laptop technology from 1990–2001.

Battery energy density barely increased

Android Doze

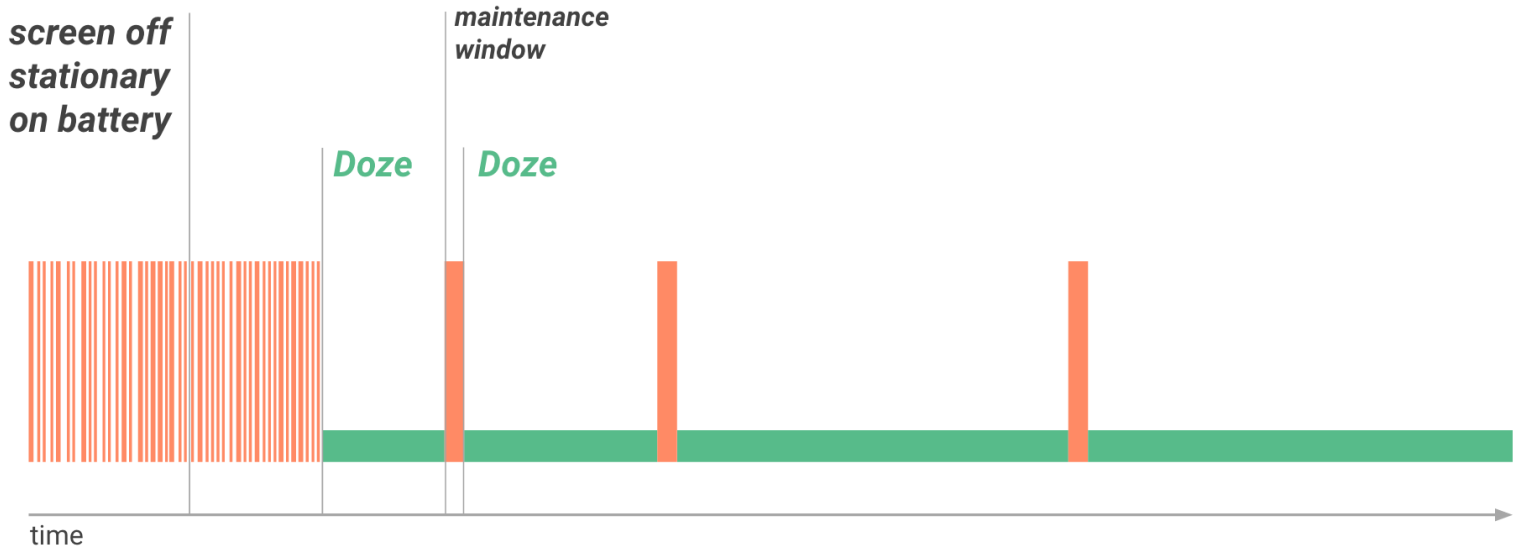
https://developer.android.com/training/monitoring-device-state/doze-standby.html



- Power-saving features introduced in Android 6.0
- Kicks in only when device is not connected to power source (e.g. charging)
- **Doze:** stops background CPU and network activity when **device is unused for long time**
- **App standby:** stops background network activity for apps that user has **not interacted with recently**

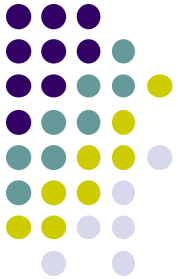
Doze

- System exits doze periodically to run pending jobs, alarms and allow network access (maintenance)
- Once user wakes device by moving it, turning on screen, or connecting a charger, system exits Doze and all apps return to normal activity

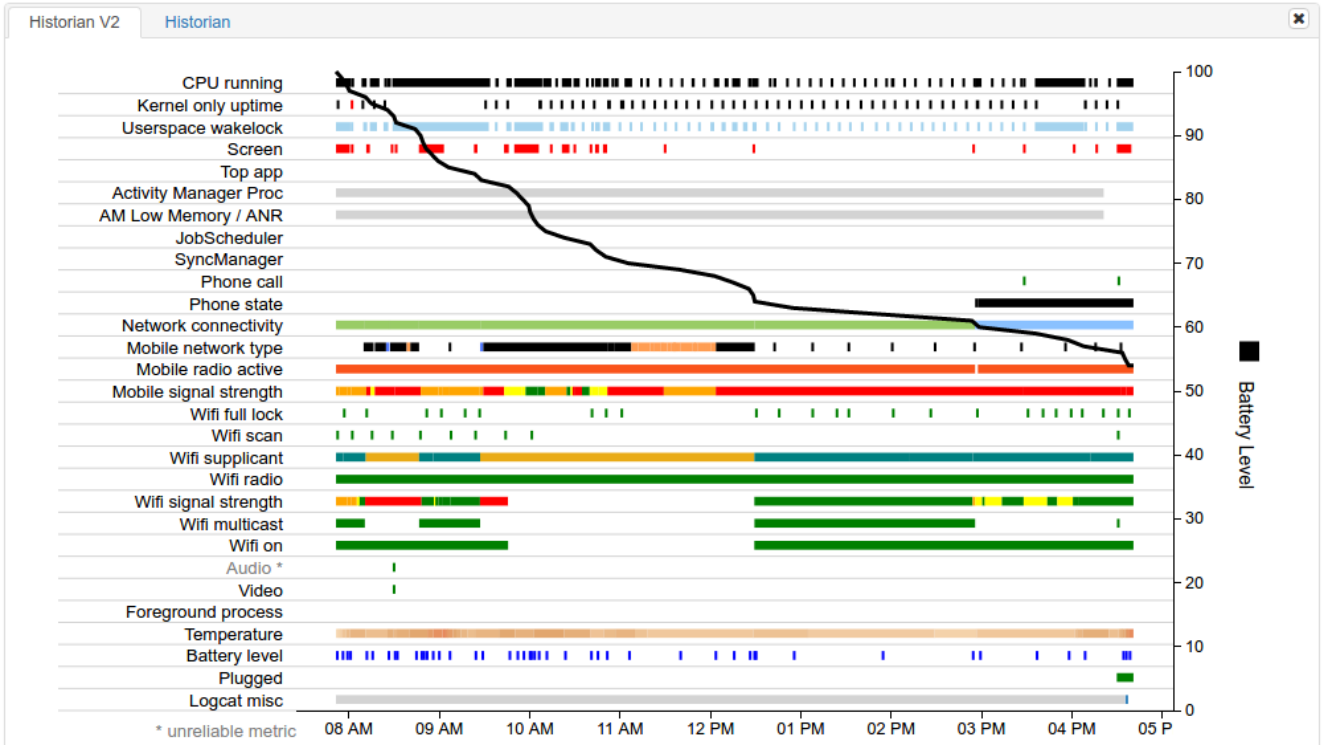


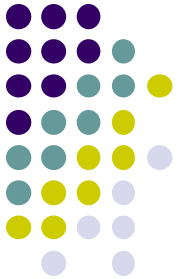
Battery Historian

https://developer.android.com/topic/performance/power/battery-historian.html



- Provides insight into device battery consumption
- Visualize, identify system events that cause high battery drain
- Also how your app's battery drain compares to other apps



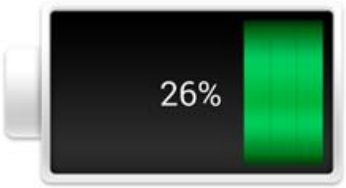


Sandra Helps You Learn: The More you Walk, the More Battery Your phone drains, *Ubicomp 2015*

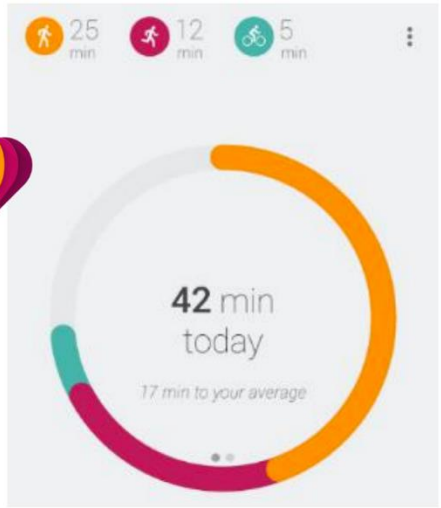
Problem: Continuous Sensing Applications Drain Battery Power

C Min *et al,* Sandra Helps You Learn: the More you Walk, the More Battery Your Phone Drains, in Proc Ubicomp '15

- CSAs (Continuous Sensing Apps) introduce new major factors governing phones' battery consumption
  - E.g. Activity Recognition, Pedometer, etc
- How? Persistent, mobility-dependent battery drain
  - Different user activities drain battery differently
  - E.g. battery drains more if user walks more



Google Fit:
activity tracking

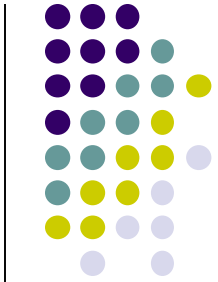


Moves:
activity/place tracking

Accupedo:
pedometer

Dieter:
pedometer

Sandra: Goal & Research Questions



- E.g. Battery at 26%. User's typical questions:
  - How long will phone last from now?
  - What should I do to keep my phone alive until I get home?

- Users currently informed on well-known factors draining battery faster
  - E.g. frequent app use, long calls, GPS, brighter screen, weak cell signal

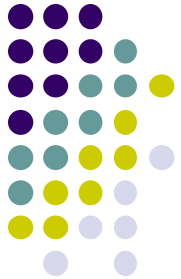
Sandra: Goal & Research Questions

- Users currently don't accurately include CSAs in their mental model of battery drain
  - CSA energy drain sometimes counter-intuitive
  - E.g. CSA drain is **continuous** but users think drain only during activity (e.g. walking)
  - Battery drain depends on activities performed by user

- Paper makes 2 specific contributions about energy drain of CSAs

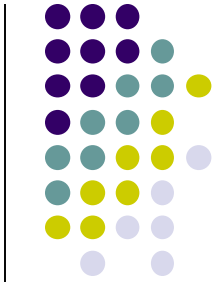
  1. **Quantifies CSA battery impact:** Nonlinear battery drains of CSAs
  2. Investigates/corrects **user's incorrect perceptions** of CSAs' battery behaviors

Sandra: Goal & Research Questions



- **Battery information advisor (Sandra):**
  - Helps users make connection between battery drain (including CSAs) and their activities
  - Forecasts battery drain under different **future** mobility conditions
    - E.g. (stationary, walking, transport) + (indoor, outdoor)
  - Maintains a history of **past** battery use under different mobility conditions

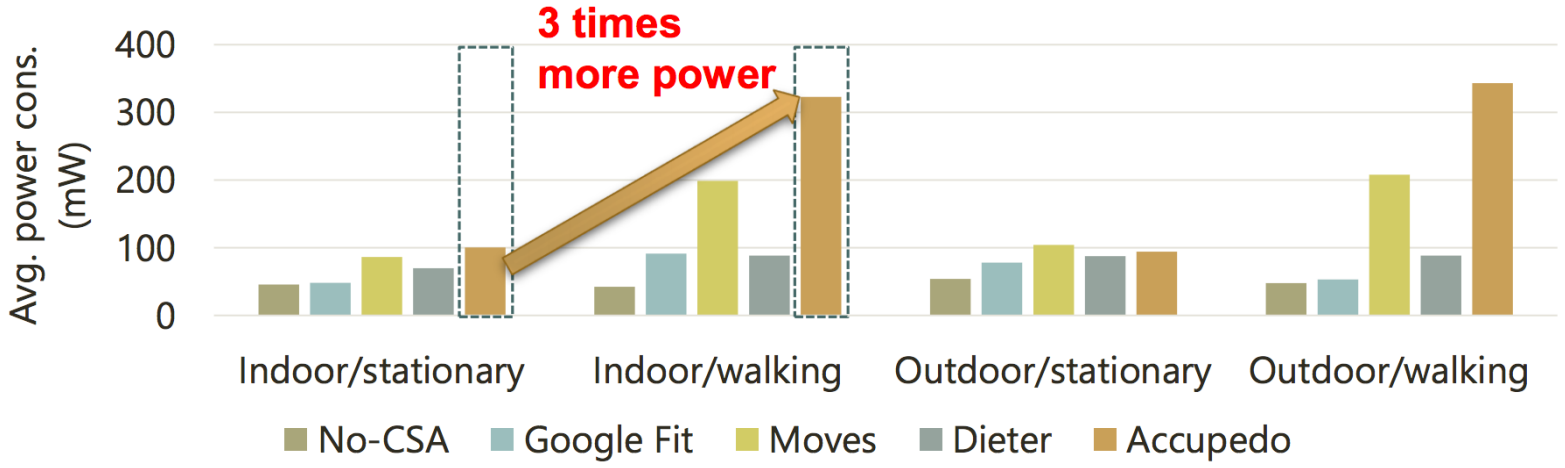
First Step: Measure Battery Consumption of 4 CSAs



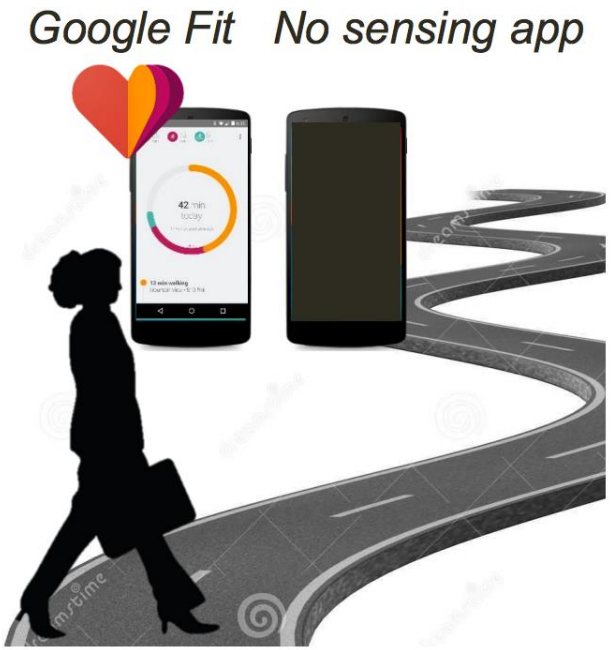
- **Google Fit:**
  - Tracks user activity continuously (walking, cycling, riding, etc)
- **Moves:**
  - Tracks user activity (walking, cycling, running), places visited and generates a storyline
- **Dieter:**
  - Fitness tracking app in Korea
- **Accupedo:**
  - Pedometer app

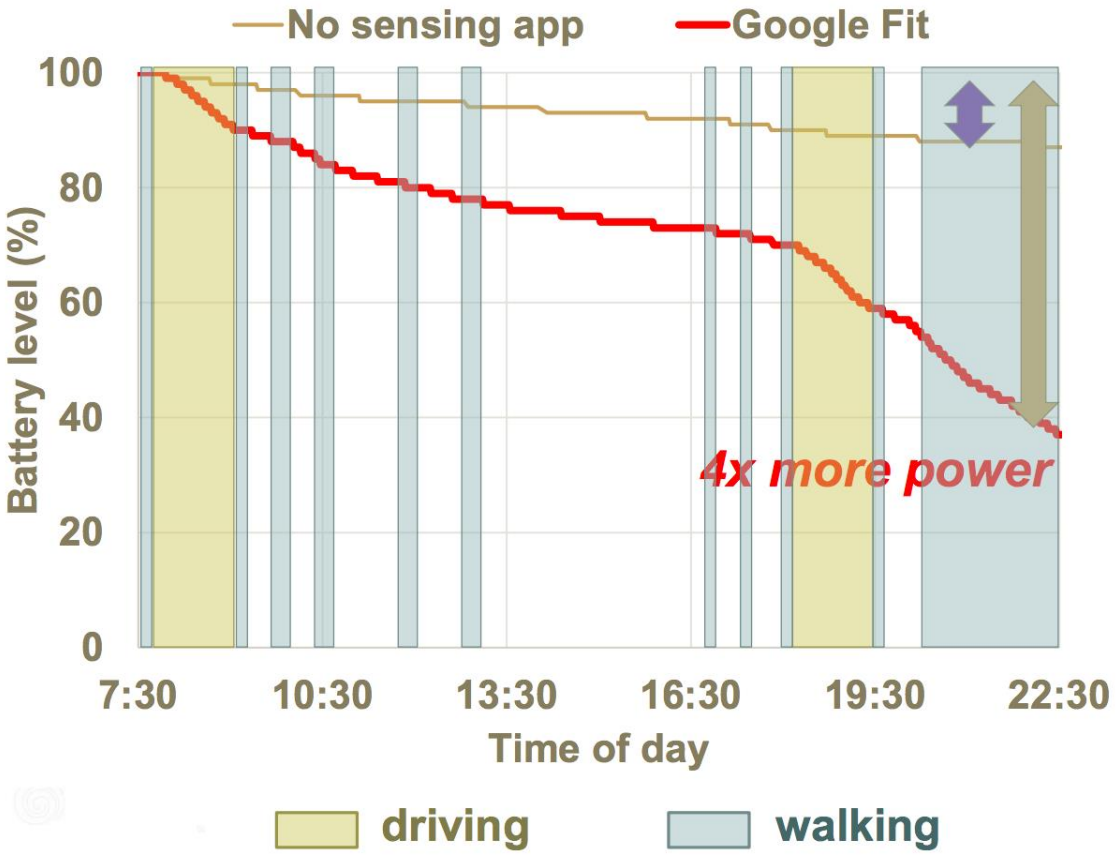
Energy Consumed by CSAs under different mobility conditions

- CSAs drain extra stand-by power
- Average increase in battery drain: 171% vs No-CSA
- Drains 3x more energy when user is walking vs stationary



Day-long Battery Drain under real Life Mobility

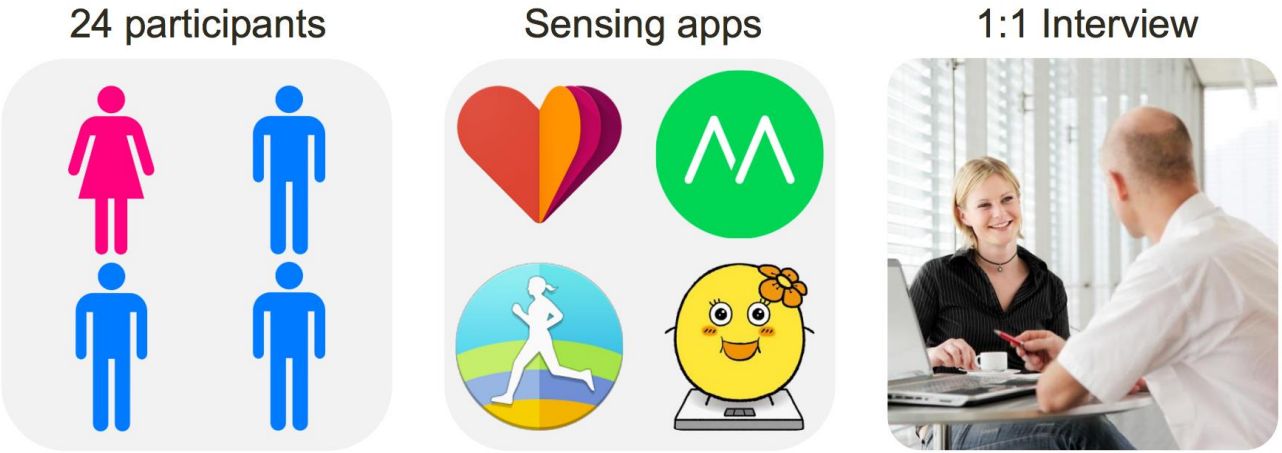




Also steeper battery drain when user is walking

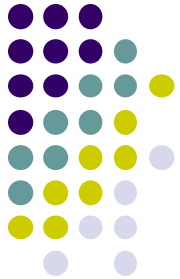
Users may focus on only battery drain caused by their foreground interactions

Next: Investigate User perceptions of CSAs' Battery Consumption



- Interviewed 24 subjects to understand factors influencing phone's battery life
- Questions included:
  - Do you feel concerned about phone's battery life?
  - Have you suspected that CSAs reduce battery life?

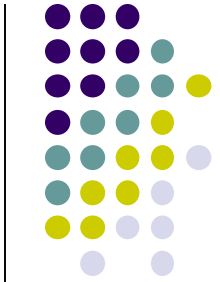
Findings: Investigate User perceptions of CSAs' Battery Consumption



- Subjects
  - Already knew well-known sources of battery drain (display, GPS, network, voice calls, etc)
  - Felt battery drain should be minimal when phone is not in use
  - Were very concerned about battery life. E.g. kept multiple chargers in office, home, car, bedside, etc
  - Had limited, sometimes inaccurate understanding of details of CSA battery drain
  - Disliked temporarily interrupting CSAs to save battery life.
    - E.g. Users kill battery hungry apps, but killing step counter misses steps, 10,000 step goals

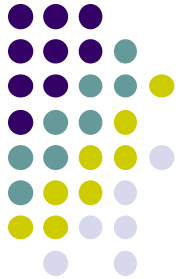
Sandra Battery Advisor Design

- Sandra interfaces that forecasts expected standby times for a commonly occurring mobility conditions
  - E.g. Walking indoors/outdoors, commuting outdoors, etc

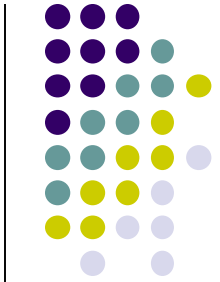


Mobile Security Issues

Introduction

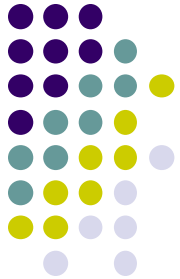


- So many cool mobile apps
- Access to web, personal information, social media, etc
- Security problems (not previously envisaged) have resulted
- Examples:
  - Malicious apps can steal your private information (credit card information, etc)
  - Smartphone sensors can leak sensitive information
  - Malware can lock your phone till you pay some money (ransomeware)
- Need deeper understanding of mobile security



Android Security Model

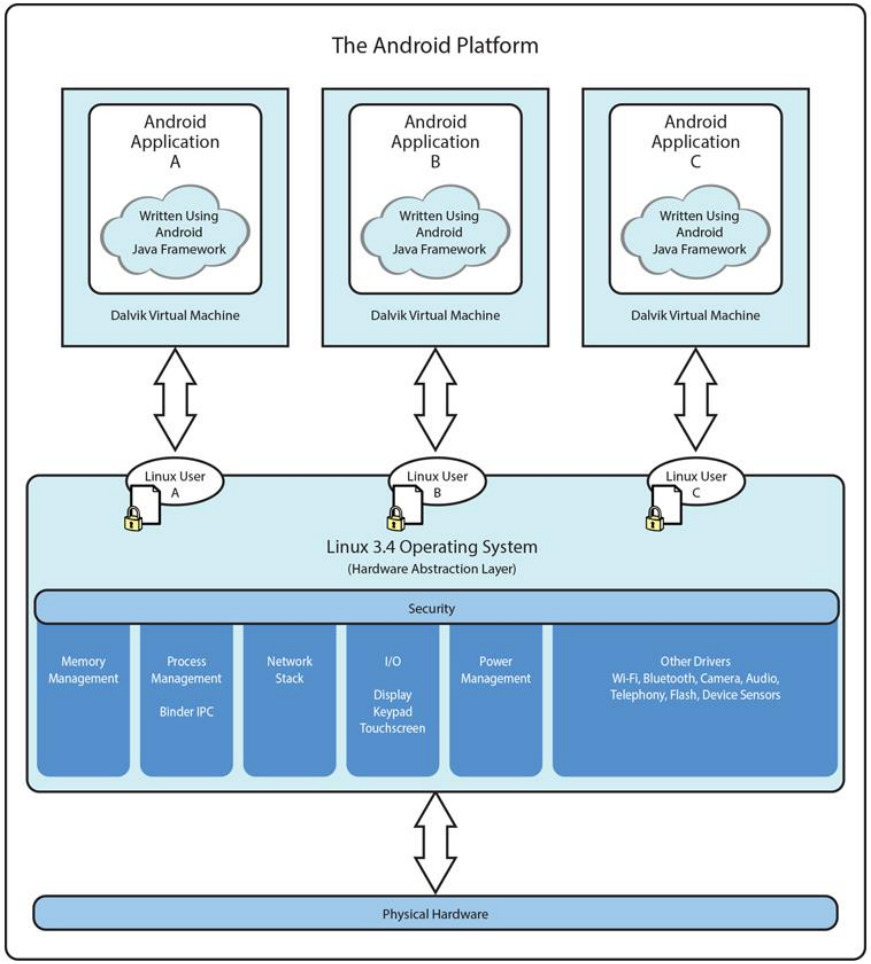
Android Security



- Security goals are to
  - Protect user data, system resources (hardware, software)
  - Provide application isolation

- **Foundations of Android Security**
  1. **Application Isolation:**
     - Application sandboxing: App 1 cannot interact directly with app 2
     - Secure inter-process communication

  2. **Permission Requirement:**
     - System-built and user-defined permissions
     - Application signing

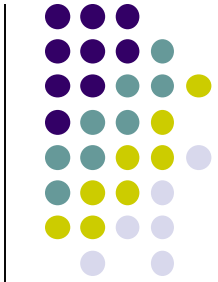


Recall: Android Software Framework

- Each Android app runs in its own security sandbox (VM, minimizes complete system crashes)
- Android OS multi-user Linux system
- Each app is a different user (assigned unique Linux ID)
- Access control: only process with the app's user ID can access its files
- Apps talk to each other only via intents, IPC or ContentProviders

Ref: Introduction to Android Programming, Annuzzi, Darcey & Conder

Android Encryption



- Encryption encodes data so that unauthorized party cannot read it

- **Full-disk encryption:** Android 5.0+ provides full filesystem encryption
  - All user data can be encrypted in the kernel
  - User password needed to access files, even to boot device

- **File-based encryption:** Android 7.0+ allows specific files to be encrypted and unlocked independently

iPhone vs Android Encryption

- In earlier Androids, encryption was up to user
- iPhones encrypt automatically: almost all encrypted

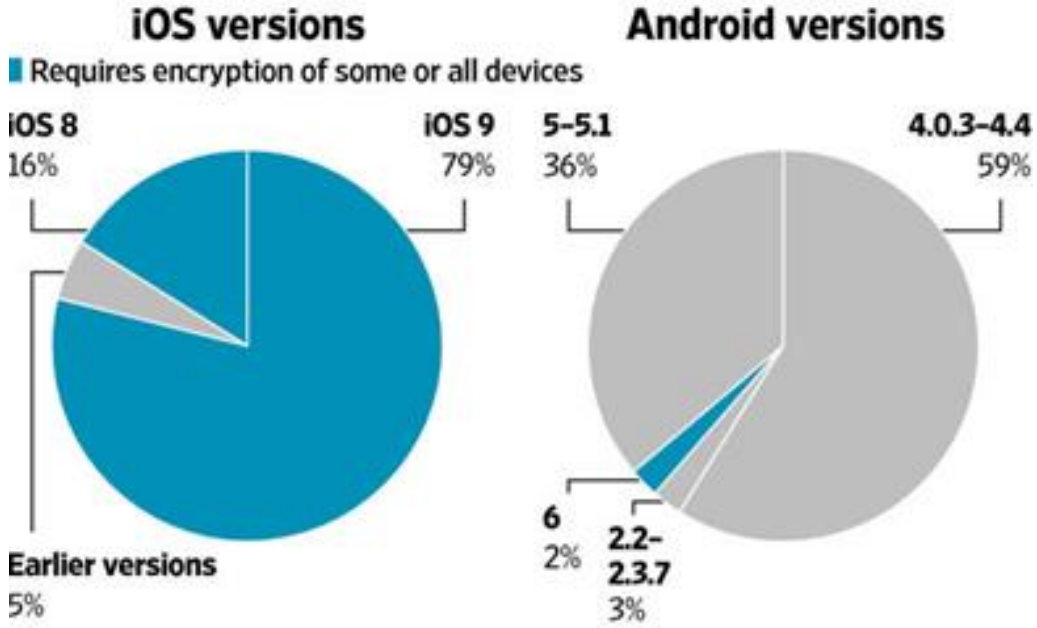
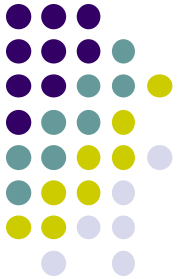


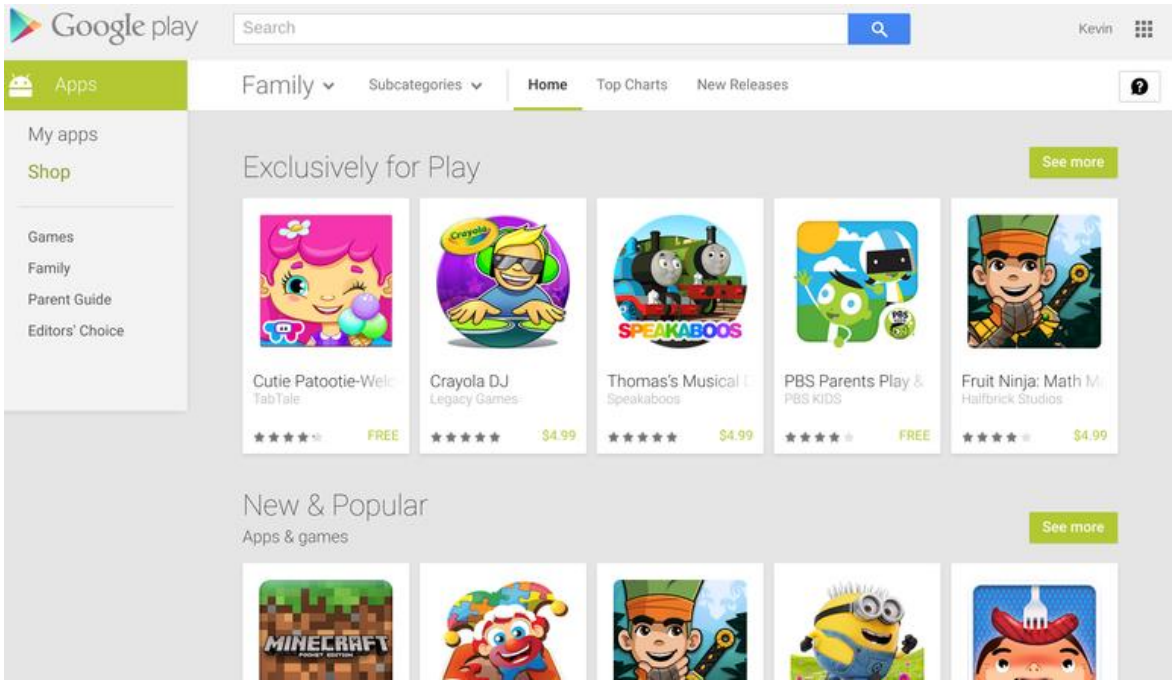
Image credit: wall street journal

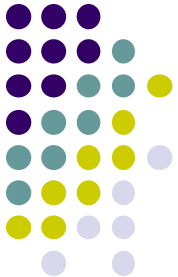


App Markets

App Markets & Distribution

- Major OS vendors manage their own markets for “certified” apps
  - Android: the Google Play Store
  - iOS: the App Store is the sole source of apps



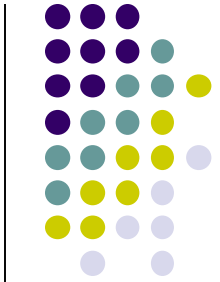


App Market Scanning

- Google Play app scanning: Google Play Protect
- Antivirus system scans Google Play for threats, malware
- New “peer grouping system:
  - similar apps (e.g. all calculators) are grouped on app market.
  - If one app requests more permissions than similar apps, human takes a look

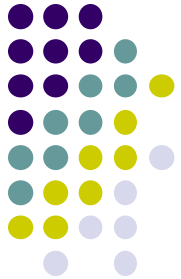
- Apple App Store
  - Highly regulated
  - All applications are reviewed by human
  - iOS devices can only obtain apps through here, unless jailbreaked

- Many malware developers target third-party markets
  - Weaker/no restrictions or analysis capabilities



Malware Evolution

Threat Types: Malware, Grayware & Personal Spyware

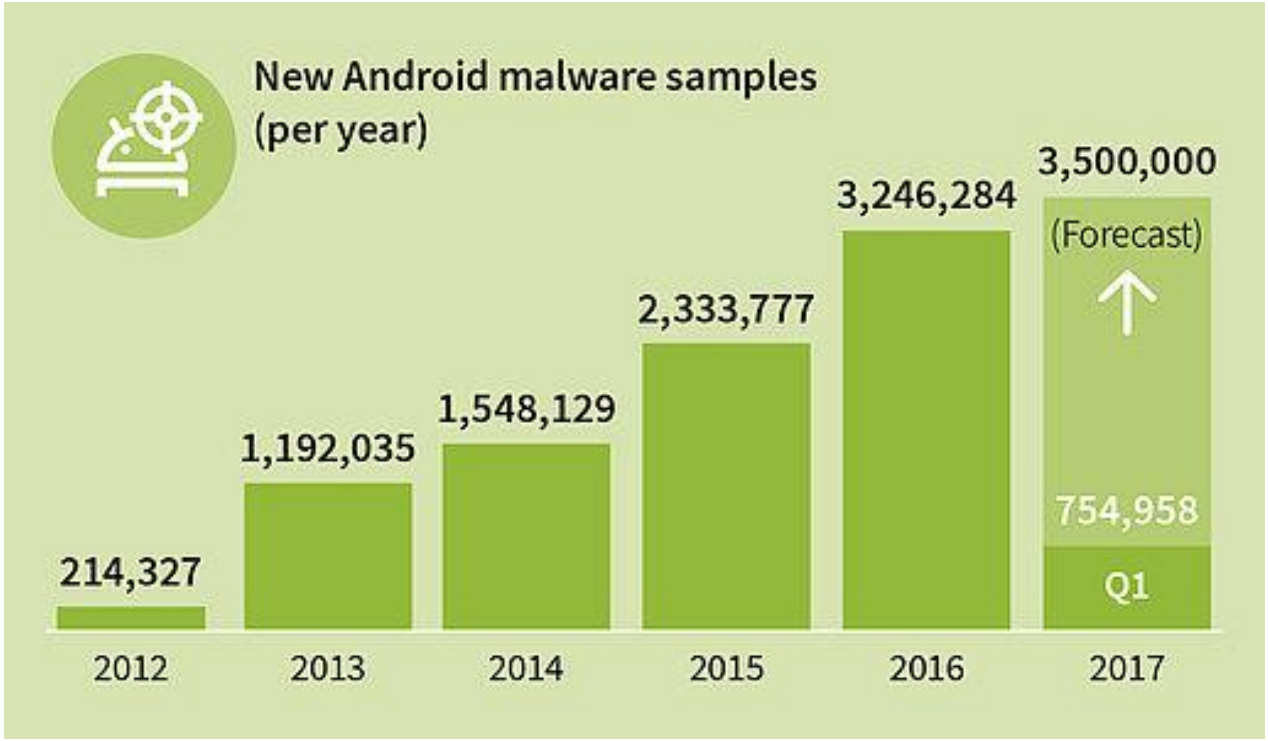


- **Malware:**
  - Gains access to a mobile device in order to steal data, damage device, or annoying the user, etc. **Malicious!!**

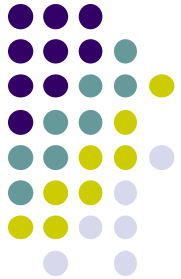
- **Personal Spyware:**
  - Collects user's personal information over of time
  - Sends information to app **installer** instead of author
  - E.g. spouse may install personal spyware to get info

- **Grayware:**
  - Collect data on user, but with no intention to harm user
  - E.g. for marketing ,user profiling by a company

Growth of Android Malware



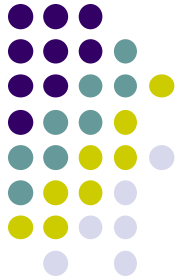
Ref: Bochum, Author: Christian Lueg8,400 new Android malware samples every day
https://www.gdatasoftware.com/blog/2017/04/29712-8-400-new-android-malware-samples-every-day



Mobile Malware Survey (*Felt et al*)

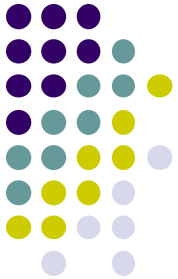
Mobile Malware Study?

A survey of mobile malware in the wild Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steve Hanna, and David Wagner in Proc SPSM 2011



- First major mobile malware study in 2011 by Andrienne Porter Felt *et al*
  - Previously, studies mostly focused on PC malware
- Analyzed 46 malwares that spread Jan. 2009 – June 2011
  - 18 – Android
  - 4 – iOS
  - 24 – Symbian (discontinued)
- Analyzed information in databases collected by:
  - information in databases maintained by anti-virus companies
    - E.g., Symantec, F-Secure, Fortiguard, Lookout, and Panda Security
  - Mentions of malware in news sources
- Did not analyze spyware and grayware

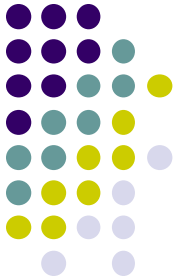
Categorized Apps based on Behaviors



- **Novelty and amusement:** Minor damage. E.g.
  - Change user's wallpaper

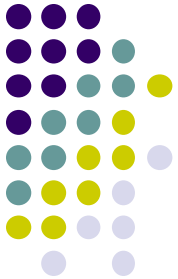
- **Selling user information:**
  - Personal information obtained via API calls
    - User's location, contacts, download + browser history/preferences
  - Information can be sold for advertisement
    - $1.90 to $9.50 per user per month

Categorized Apps based on Behaviors



- **Stealing user credentials:**
  - People use smartphones for shopping, banking, e-mail, and other activities that require passwords and payment information
  - Malwares can log keys typed by user (keylogging), scan their documents for username + password
- In 2008, black market price of:
  - Bank account credentials: $10 to $1, 000,
  - Credit card numbers: $.10 to $25,
  - E-mail account passwords: $4 to $30

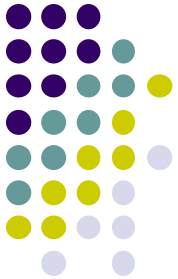
Categorized Apps based on Behaviors



- **Make premium-rate calls and SMS:**
  - Premium rate texts to specific numbers are expensive
  - Malware sends SMS to these numbers set up by attacker
  - Cell carrier (e.g. sprint) bills users
  - Attacker makes money

- **SMS spam:**
  - Used for commercial advertising and phishing
  - Sending spam email is illegal in most countries
  - Attacker uses malware app on user's phone to send SPAM email
  - Harder to track down senders

Categorized Apps based on Behaviors



- **Search Engine Optimization (SEO):**
  - Malware makes HTTP requests for specific pages to increase its ranking (e.g. on Google)
  - Increases popularity of requested websites

- **Ransomeware**
  - Possess device, e.g. lock screen till money is paid
  - *Kenzero* – Japanese virus included in pornographic games distributed on the P2P network
    - Asked for Name, Address, Company Name for “registration” of software
    - Asked **5800 Yen** (~$60) to delete information from website (Paper information is wrong)
    - About 661 out of 5510 infections actually paid (12%)

Ransomware

Ransomware: Type of malware that prevents or limits users from accessing their system, by locking smartphone's screen or by locking the users' files till a ransom is paid

Source: Lookout Top Threats
https://www.lookout.com/resources/top-threats/scarepakage

Source: MalwareBytes "State of Malware Report" 2017
https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf

Categorization of Malware Behaviors

Exfiltrates user information	28
Premium calls or SMS	24
Sends SMS advertisement spam	8
Novelty and amusement	6
Exfiltrates user credentials	4
Search engine optimization	1
Ransom	1

Table 1: We classify 46 pieces of malware by behavior. Some samples exhibit more than one behavior, and every piece of malware exhibits at least one.

Malware Detection based on Permissions

- Does malware request more permissions?
- Analyzed permissions of 11 Android malwares

- **Findings: Yes!**
  - 8 of 11 malware request SMS permission (73%)
    - Only 4% of non-malicious apps ask for this
  - Malware 6.18 dangerous permissions
    - 3.46 for Non-malicious apps
  - Dangerous permissions: requests for personal info (e.g. contacts), etc

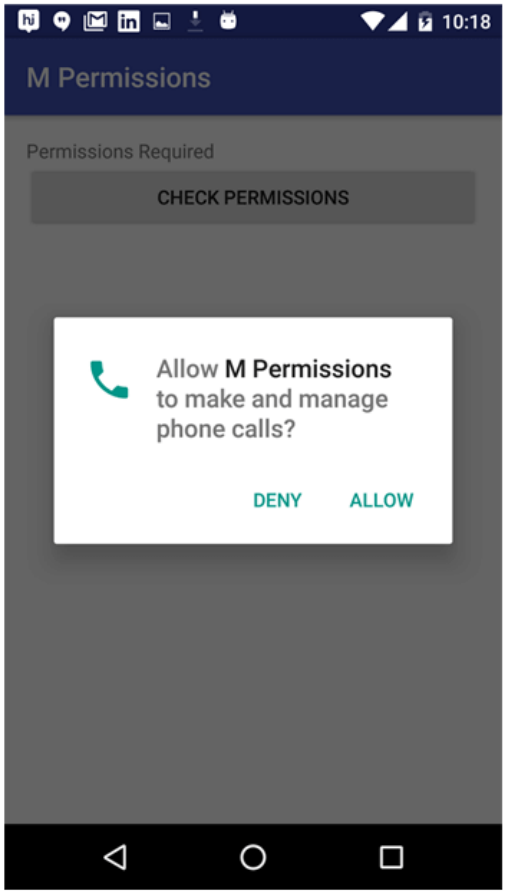
Number of Dangerous permissions	Number of non-malicious applications		Number of malicious applications
0	75	(8%)	-
1	154	(16%)	1
2	182	(19%)	1
3	152	(16%)	-
4	140	(15%)	2
5	82	(9%)	1
6	65	(7%)	-
7	28	(3%)	2
8	19	(2%)	1
9	21	(2%)	1
10	10	(1%)	1
11	6	(0.6%)	1
12	7	(0.7%)	-
13	4	(0.4%)	-
14	4	(0.4%)	-
15	2	(0.2%)	-
16	1	(0.1%)	-
17	1	(0.1%)	-
18	-		-
19	-		-
20	1	(0.1%)	-
21	-		-
22	-		-
23	1	(0.1%)	-
24	-		-
25	-		-
26	1	(0.1%)	-

Table 2: The number of "Dangerous" Android permissions requested by 11 pieces of malware and 956 non-malicious applications [28].

Run-Time Permissions Changed in Marshmallow (Android 6.0)

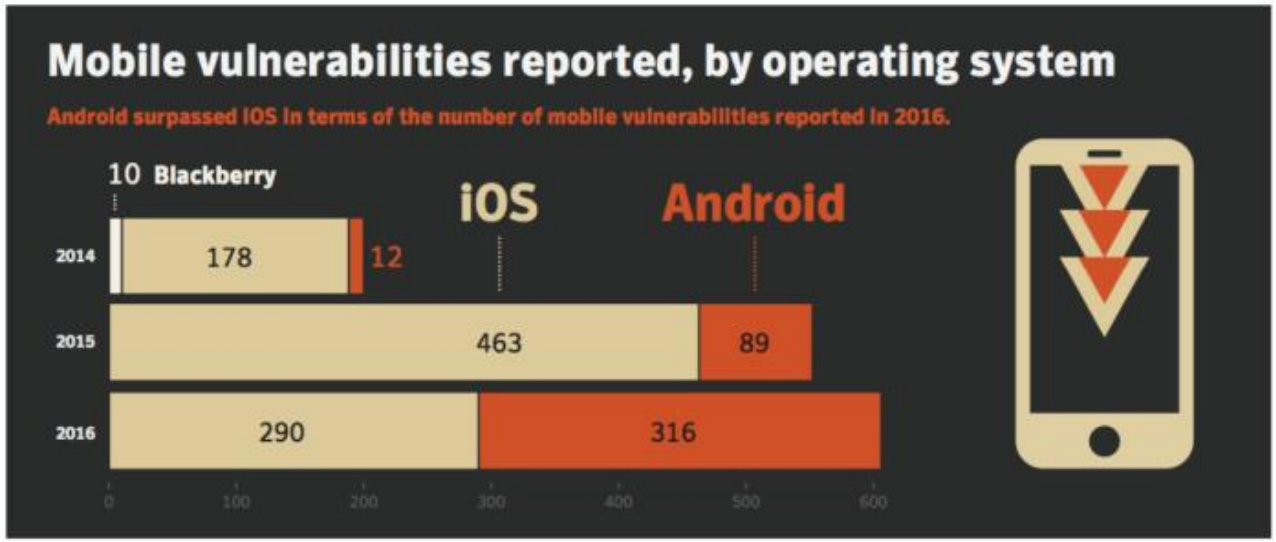
- "Normal" permissions don't require user consent
  - Normal permissions can do very little to harm app
  - E.g. change timezone
  - Automatically granted
  - Can be used freely by ad networks

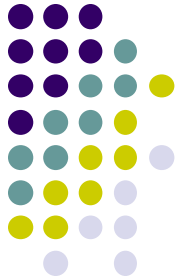
- Run-time permissions required for "more dangerous" access
- **Dangerous?** contacts, etc



iOS Malware Review

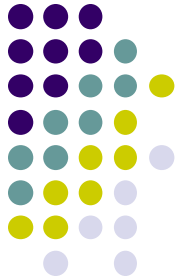
- iOS generally fewer vulnerabilities (even till date)
  - All 4 pieces of Apple malware were spread through jailbroken devices;
  - not found on App Store
  - Human review more effective but slow!!?





Authentication using Biometrics

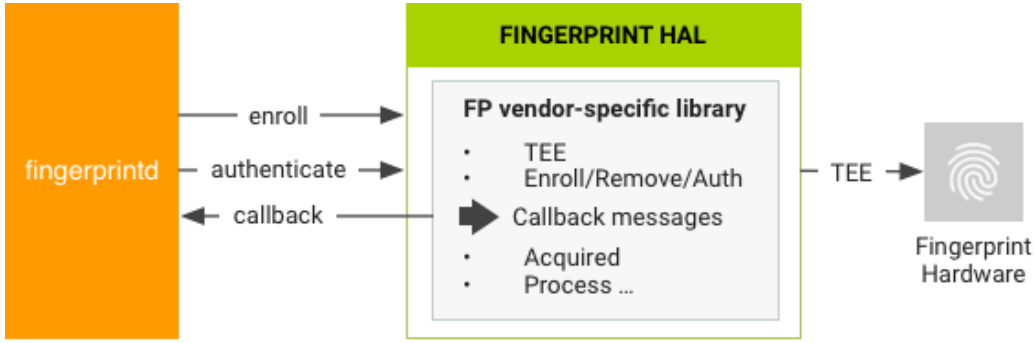
Biometrics



- Passwords tough to remember, manage
- Many users have simple passwords (e.g. 1234) or do not change passwords
- Biometrics are unique physiological attributes of each person
  - Fingerprint, voice, face
- Can be used to replace passwords
  - No need to remember anything. Cool!!

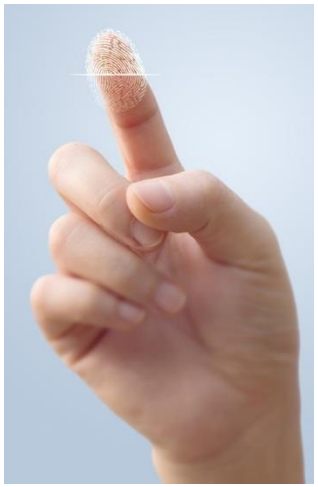
Android Biometric Authentication: Fingerprints

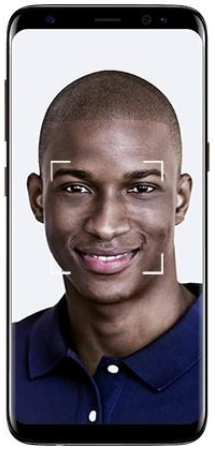
- **Fingerprint:** On devices with fingerprint sensor, users can enroll multiple fingerprints for unlocking device



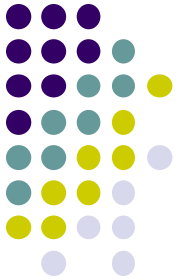
Samsung Pass: More Biometrics

- **Samsung pass:** Fingerprint + Iris scan + facial recognition

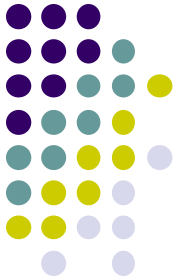


- Probably ok to use for facebook, social media
- Spanish bank BBVA's mobile app uses biometrics to allow login without username + password
- Bank of America: pilot testing iris authentication since August



Continuous Passive Authentication using Behavioral Biometrics



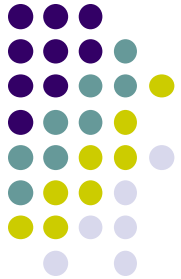
User Behavior as a Biometric

- User (micro-)behaviors are unique personal features. E.g
  - Each person's daily location pattern (home, work, places, times)
  - Walk pattern
  - Phone tilt pattern

- **General idea:** Continuously authenticate user as long as they behave like themselves

- If we can measure user behavior at very fine granularity, this could enable **passive authentication**

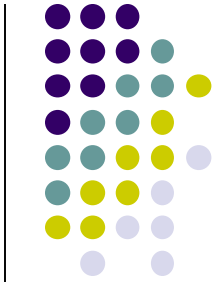
BehavioMetrics



- Derived from Behavioral Biometrics
  - Behavioral: the way a human subject behaves
  - Biometrics: technologies and methods that measure and analyzes biological characteristics of the human body
    - Fingerprints, eye retina, voice patterns

- BehavioMetrics:
  - Measurable behavior to recognize or to verify identity of a human subject or subject's certain behaviors

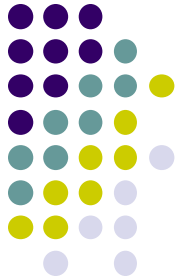
Mobile Sensing → BehavioMetrics



- Accelerometer
  - activity, motion, hand trembling, driving style
  - sleeping pattern
  - inferred activity level, steps made per day, estimated calorie burned
- Motion sensors, WiFi, Bluetooth
  - accurate indoor position and trace.
- GPS
  - outdoor location, geo-trace, commuting pattern
- Microphone, camera
  - From background noise: activity, type of location.
  - From voice: stress level, emotion
  - Video/audio: additional contexts
- Keyboard, taps, swipes
  - Specific tasks, user interactions, …

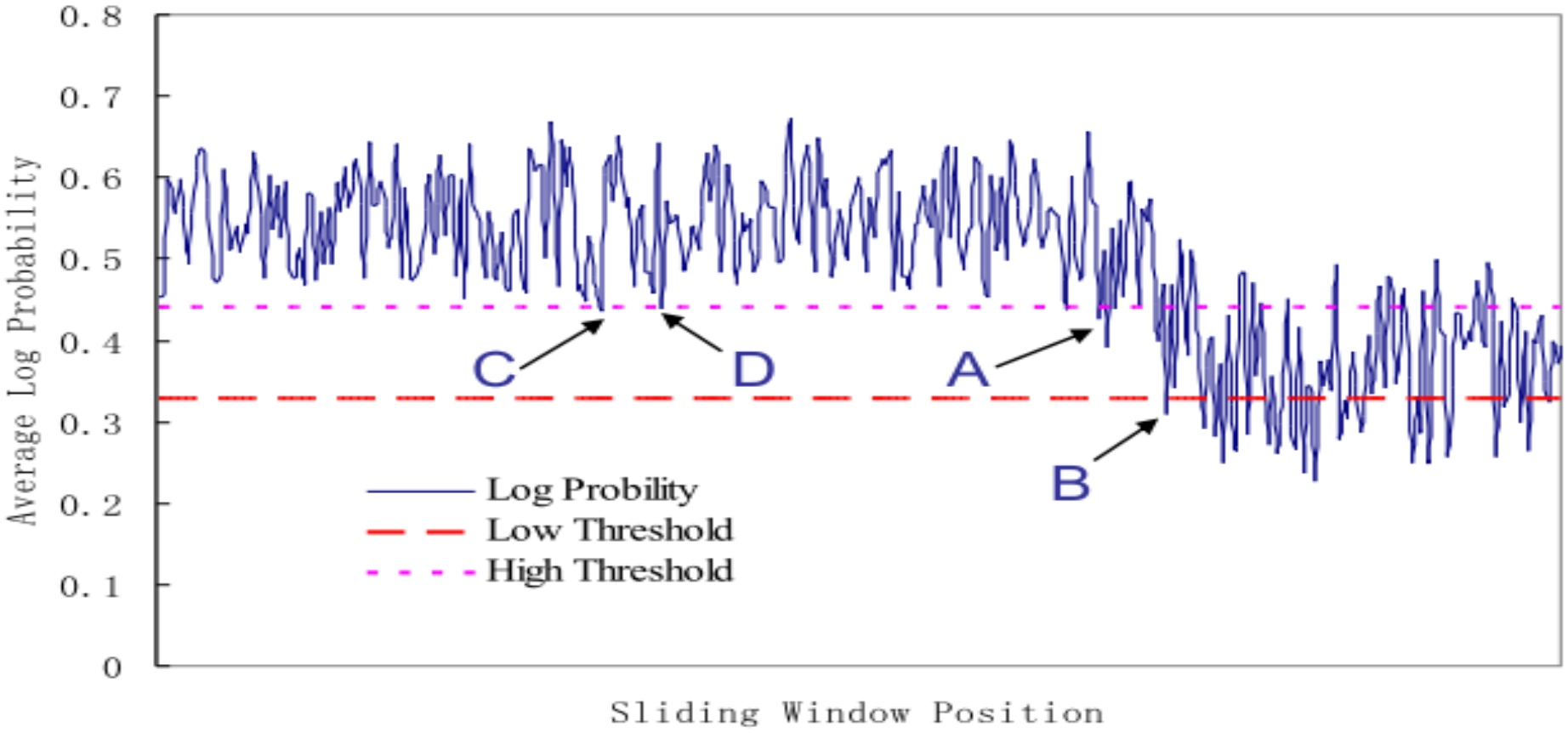
- *Network Factors*
- *Personal Factors*
- *Behavioral Factors*
- *Application Factors*

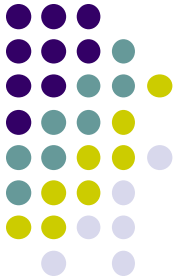
BehavioMetrics → Security



- Track smartphone user behavior using sensors
- Continuously extract and classify sensory traces + context = personal behavior features (pattern classification)
- Generate unique pattern for each user
- **Trust score:** How similar is today's behavior to user's typical behavior
- Trigger various authentication schemes when certain applications are launched

Anomaly Detection Threshold



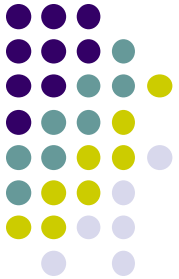


Behavioral Biometrics Issues: Shared Devices

Multi-Person and -Device Use

- Many mobile devices are shared by multiple people
  - Classifier trained using person A's data cannot detect Person B
  - **Question:** How to distinguish different people's data (segment) on same device

- Many people have multiple mobile devices
  - Classifier trained on device 1 (e.g. smartphone) may not detect behavior on device 2 (e.g. smartwatch)
  - **Question:** How to match same user's session on multiple devices

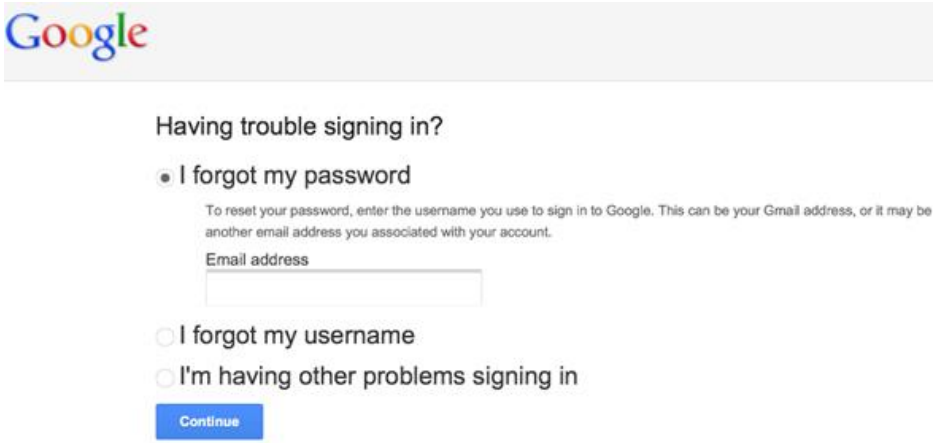


ActivPass

ActivPass

S. Dandapat, S Pradhan, B Mitra, R Choudhury and N Ganguly, ActivPass: Your Daily Activity is Your Password, in Proc CHI 2015

- Passwords are mostly secure, simple to use but have issues:
  - Simple passwords (e.g. 1234): easy to crack
  - Secure passwords hard to remember (e.g. $emime)$@(*$@)9)
  - Remembering passwords for different websites even more challenging
  - Many people use same password on different websites (dangerous!!)

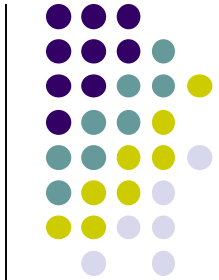


ActivPass

S. Dandapat, S Pradhan, B Mitra, R Choudhury and N Ganguly, ActivPass: Your Daily Activity is Your Password, in Proc CHI 2015

- **Explicit biometrics:** user actively makes input
  - E.g. finger print, face print, retina scan, etc
- **Implicit biometrics:** works passively, user does nothing explicit to be authenticated.
  - E.g. unique way of walk, typing, swiping on screen, locations visited daily
- **This paper:** smartphone soft sensors as biometrics: Specifically unique calls, SMS, contacts, etc
- **Advantage of biometrics:** simple, no need to remember anything

ActivPass Vision



- **Observation:** rare events are easy to remember, hard to guess
  - E.g. Website visited this morning that user rarely visits. E.g
  - User went to CNN.com today for the first time in 2 years!
  - Got call from friend I haven't spoken to in 5 years for first time today

- **Idea:** Authenticate user by quizzing them about user's outlier (rare) activities
  - What is caller's name from first call you received today?
  - Which news site did you not visit today? (CNN, CBS, BBC, Slashdot)?

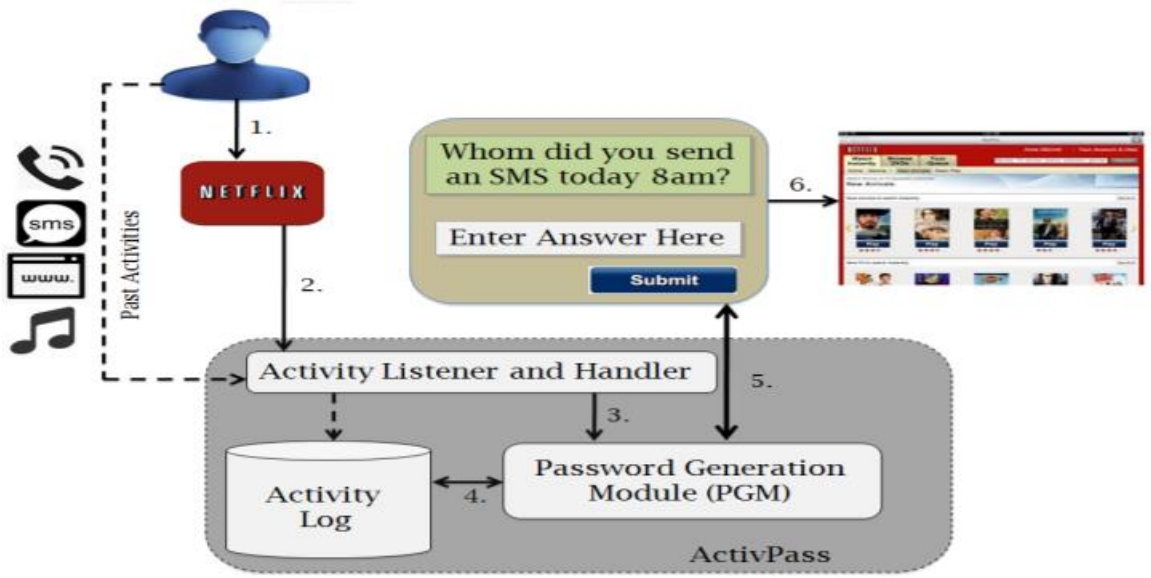
ActivPass Vision

- Authentication questions based on outlier (rare) activities generated from:
  - Call logs
  - SMS logs
  - Facebook activities
  - Browser history

How ActivPass Works

- Activity Listener runs in background, logs
  - Calls, SMS, web pages visited, etc

- When user launches an app:
  - Password Generation Module (PGM) creates *n* password questions based on logged data
  - If user can answer *k* of password questions correctly, app is launched!



ActivPass Vision

- User can customize
  - Number of questions asked, what fraction must be answered correctly
  - Question format
  - Activity permissions

Question formats	Example questions asked
Binary	Have you received a call from Alice at around 10 pm on 19/09/2014?
MCQ	Please write the options of the links you visited,this week in comma separated way (Ex: A, B): A. CNN; B. BBC; C. SKY News; D. Reuters
Text	Whom did you call at around 7 pm on 17/09/2014 ? Hint: (Al*)

- Paper investigates ActivPass utility by conducting user studies

References

- Deepak Ganesan, Behavioral Health Sensing, Course Notes Fall 2015
- Melania Swan, The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery,
- BBC, Quantified Self – The Tech-based Route to Better Life
- NY Times, The Data-Driven Life
- The Ultimate Guide to The Quantified Self

  http://www.slideshare.net/ramykhuffash/the-ultimate-quide-to-the-quantified-self