Mobile and Ubiquitous Computing on Smartphones

Lecture 10b: Mobile Security and Mobile Software Vulnerabilities

Emmanuel Agu

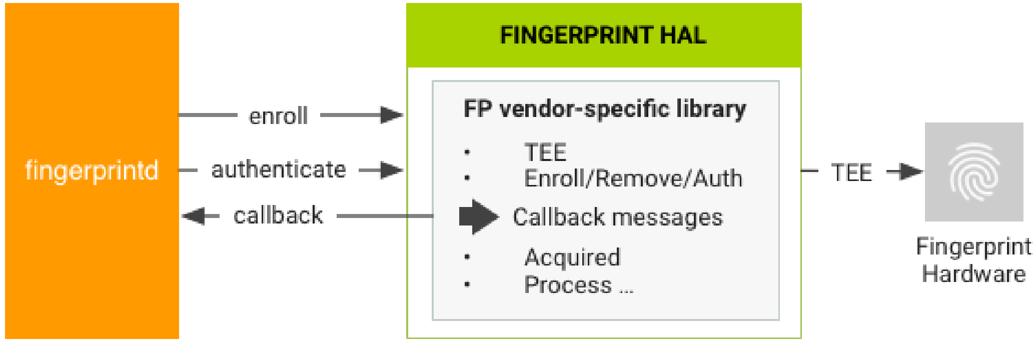
Authentication using Biometrics

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. Just be you. Cool!!

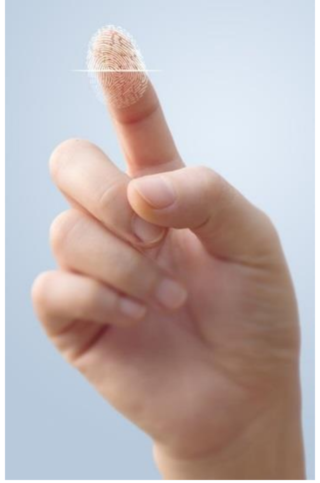
Android Biometric Authentication: Fingerprints

- **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 Aug 2017

Continuous Passive Authentication using Behavioral Biometrics

User Behavior as a Biometric

- User behaviors patterns 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 reliably, this could enable **passive authentication**

BehavioMetrics

Ref: Zhu *et al,* Mobile Behaviometrics: Models and Applications

- 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 verify a human's identity

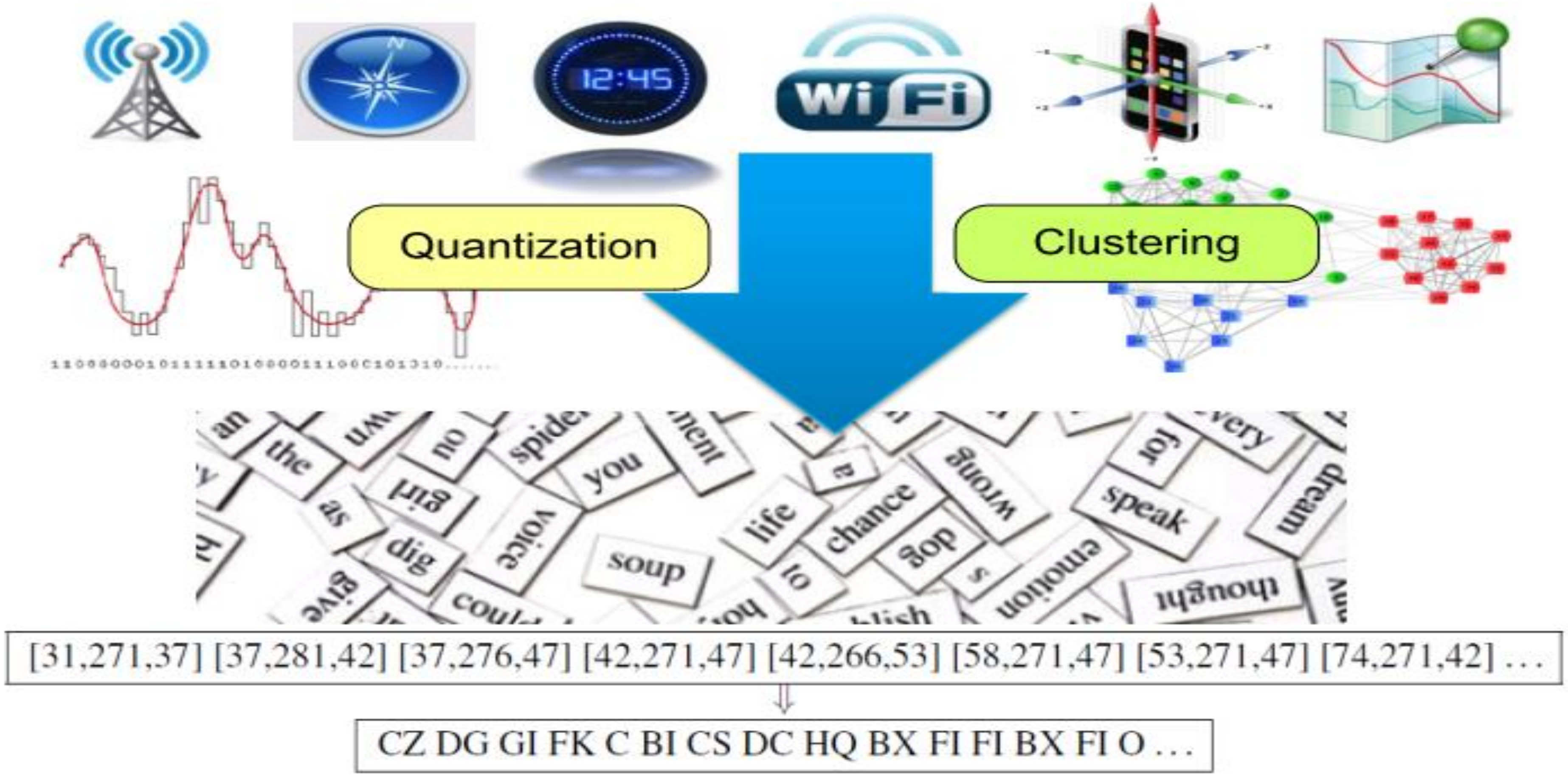
Mobile Sensing → BehavioMetrics

- Accelerometer
  - Activity & movement pattern, hand trembling, driving style
  - sleeping pattern
  - Activity level, steps per day, calories burned
- Motion sensors, WiFi, Bluetooth
  - Indoor position and trajectory.
- 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
  - User interactions, tasks .....

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

BehavioMetrics → Security

- Track smartphone user behavior using sensors
- Continuously extract and classify features from sensors = Detect contexts, 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 authentication schemes with different levels of authentication based on trust score



[31,271,37] [37,281,42] [37,276,47] [42,271,47] [42,266,53] [58,271,47] [53,271,47] [74,271,42] . . .

⇩

CZ DG GI FK C BI CS DC HQ BX FI FI BX FI O . . .

Continuous n-gram Model

- User activity at time *i* depends only on the last *n-1* activities
- Sequence of activities can be predicted by *n* consecutive activities in the past

$$P(l_i | l_{i-n+1}, l_{i-n+2}, \ldots, l_{i-1}) \quad \text{or} \quad P(l_i | l_{i-n+1}^{i-1})$$

- Maximum Likelihood Estimation from training data by counting:

$$P_{\text{MLE}}(l_i | l_{i-n+1}^{i-1}) = \frac{C(l_{i-n+1}, \ldots, l_{i-1}, l_i)}{C(l_{i-n+1}, \ldots, l_{i-1})}$$

- MLE assign zero probability to unseen n-grams

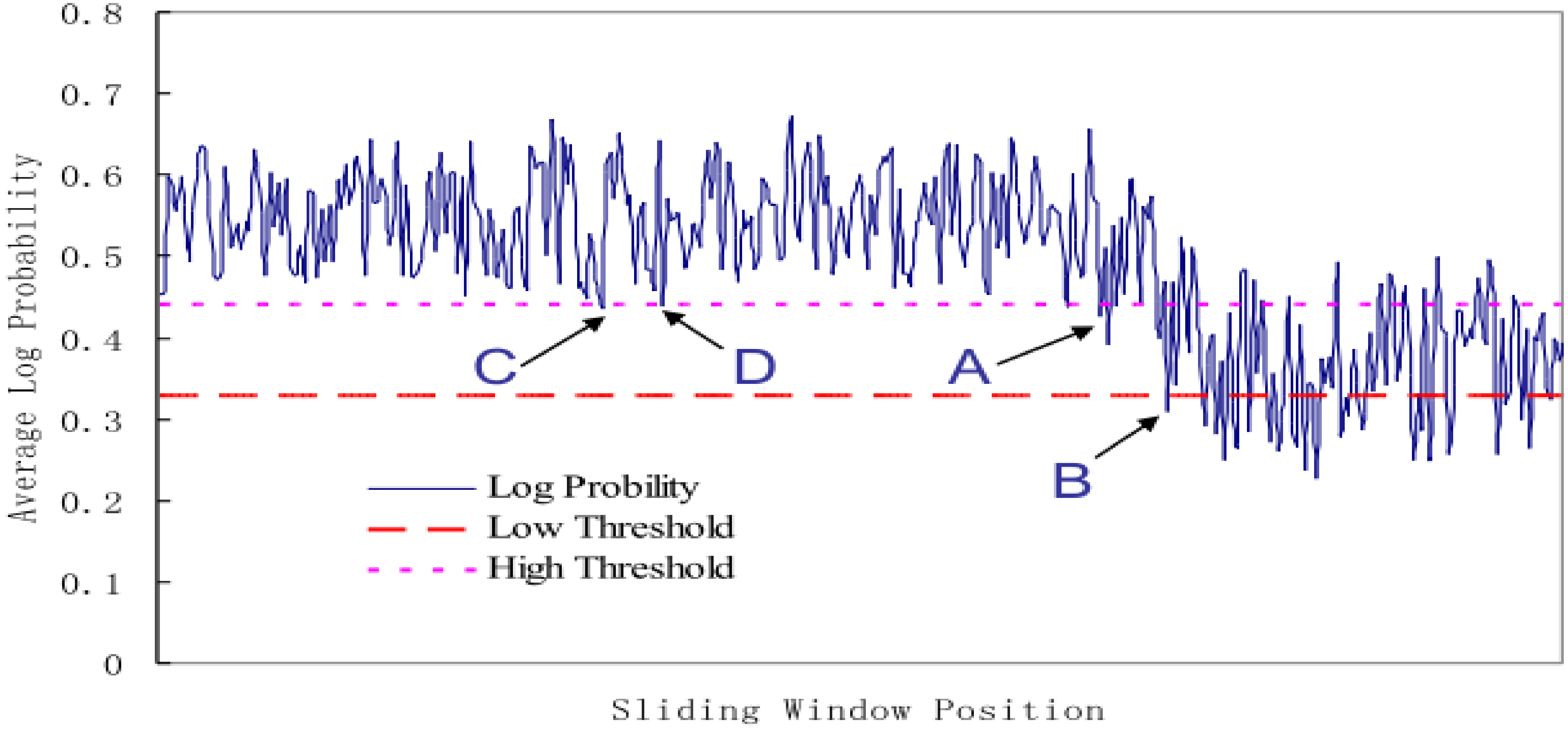
Classification

- Build *M* BehavioMetrics models P_0, P_1, P_2, … , P_{M-1}
  - Genders, age groups, occupations
  - Behaviors, activities, actions
  - Health and mental status

- Classification problem formulated as

$$\hat{u} = \operatorname*{argmax}_{m} P(L, m) = \operatorname*{argmax}_{m} \sum_{i=1}^{N} \log P_m(l_i | l_{i-n+1}^{i-1})$$

Anomaly Detection Threshold



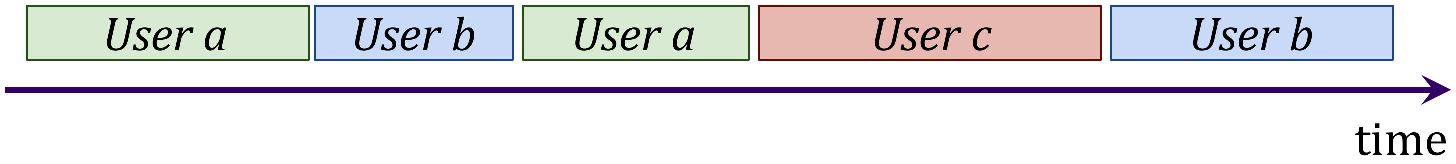
Behavioral Biometrics Issues:
Shared Devices

BehavioMetric Issues: Multi-Person Use

- Many mobile devices are shared by multiple people
  - Classifier trained using person A’s data cannot detect Person B

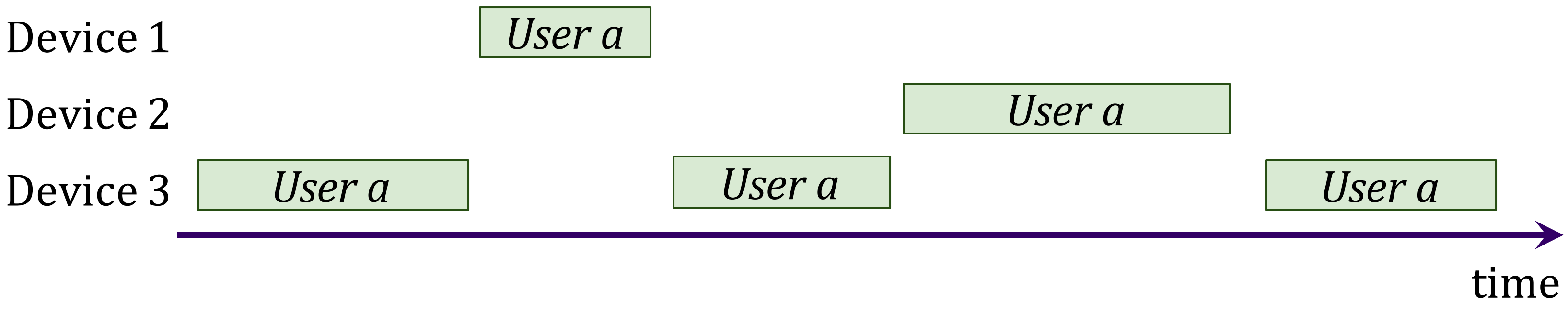
- **Question:** How to distinguish when person A vs person B using the shared device

- How to segment the activities on a single device to those of multiple users?



BehavioMetric Issues: Multi-Device Use

- 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
  - **E.g.** Use Classifier trained on smartphone to recognize user on smartwatch
- How to match user’s activity segments on different devices?

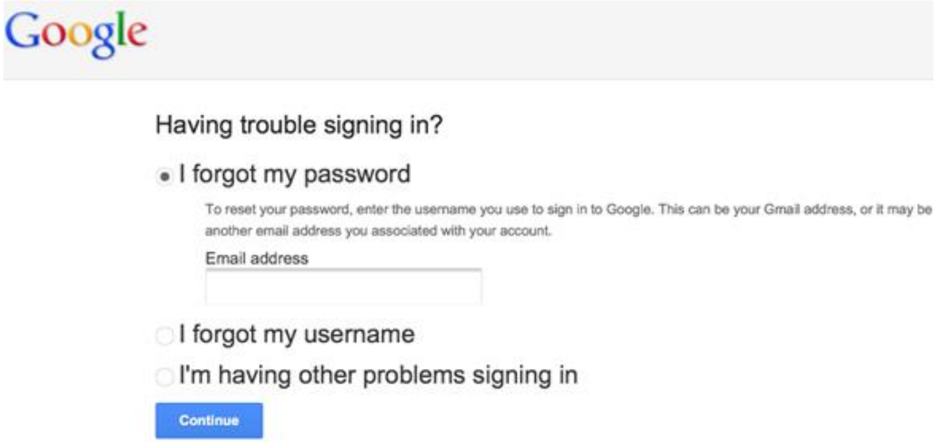


ActivPass

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!!)



Having trouble signing in?

● I forgot my password

To reset your password, enter the username you use to sign in to Google. This can be your Gmail address, or it may be another email address you associated with your account.

Email address

○ I forgot my username

○ I'm having other problems signing in

ActivPass

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

- Unique human biometrics being explored
- **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: calls, SMS, contacts, etc
- **Advantage of biometrics:** simple, no need to remember anything

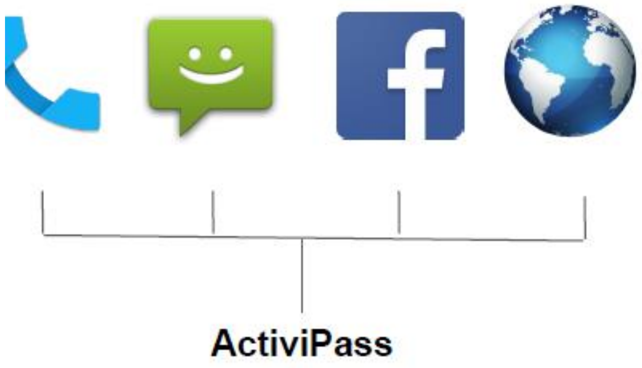
ActivPass Vision

- **Observation:** rare events are easy to remember, hard to guess
  - E.g. A website user visited this morning that they rarely visits
    - 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 to confirm rare (outlier) 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



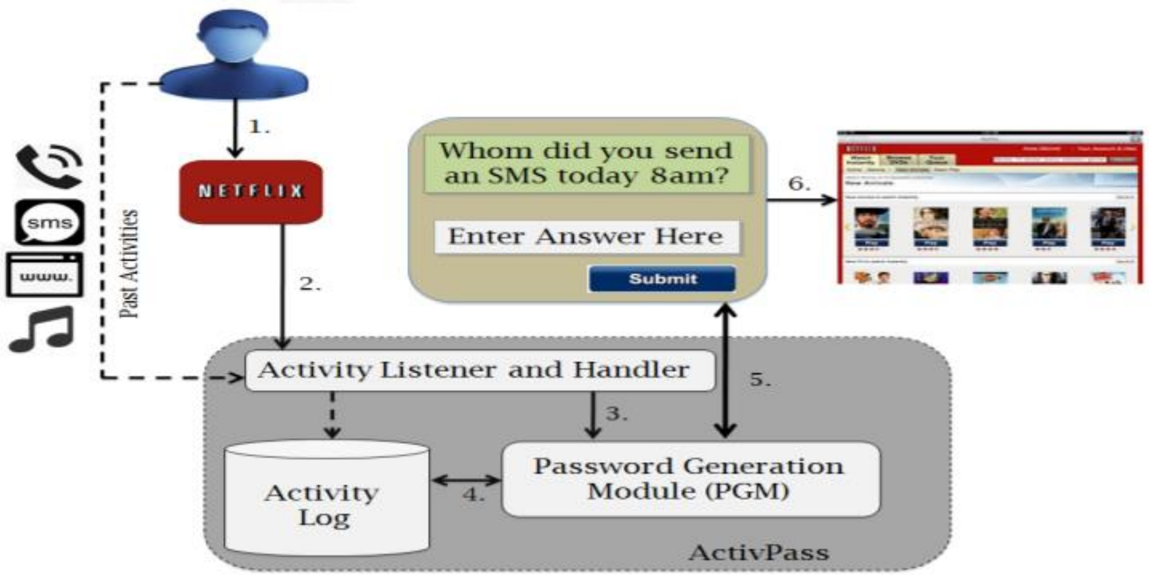
ActivPass Envisioned Usage Scenarios

- Replace password hints with Activity questions when password lost
- Combine with regular password (soft authentication mechanism)
- Prevent password sharing.
  - E.g. Bob pays for Netflix, shares his login details with Alice

How ActivPass Works

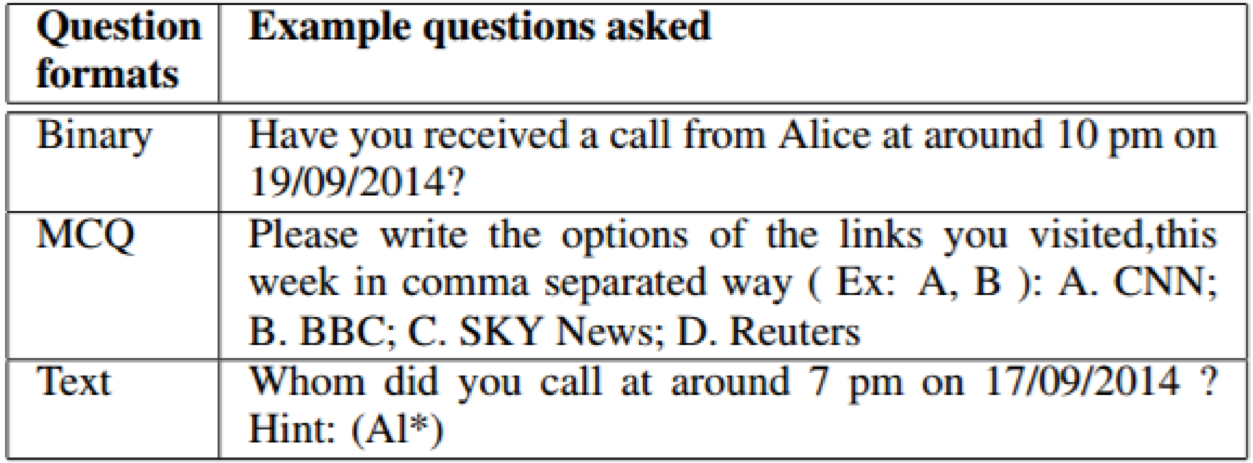
- Activity Listener runs in background, logs
  - Calls, SMS, web pages visited, etc

- 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!


1.
NETFLIX
sms
www.
Past Activities
2.
Whom did you send an SMS today 8am?
Enter Answer Here
Submit
6.
5.
Activity Listener and Handler
3.
Activity Log
4.
Password Generation Module (PGM)
ActivPass

ActivPass Vision

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

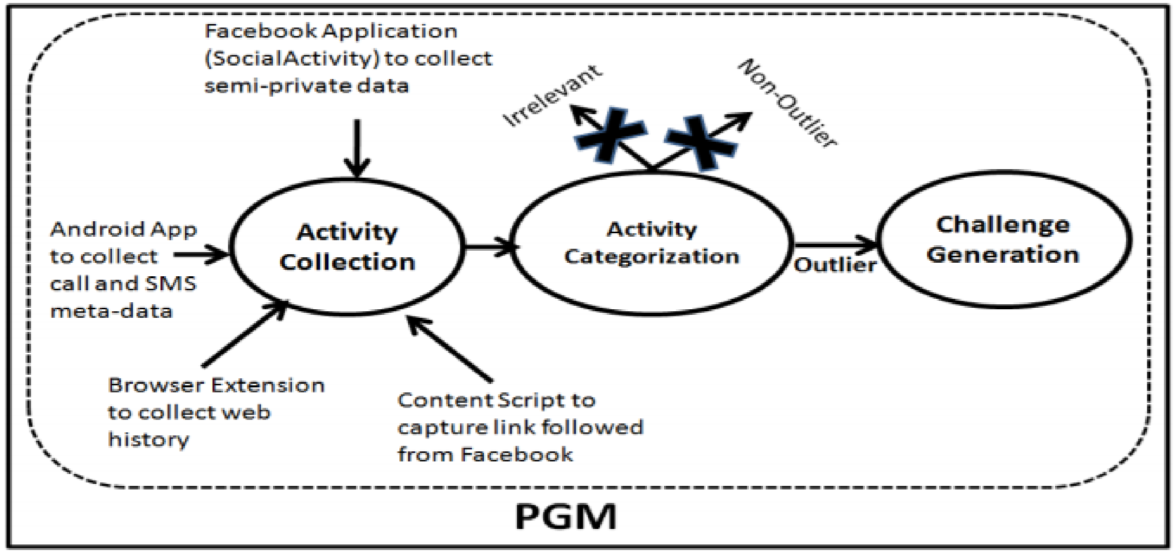


Question formats	Example questions asked
Binary	Have you received a call from Alice at around 10 pm on 19/09/2014?
MCQ	Please write the options of the links you visited,this week in comma separated way (Ex: A, B): A. CNN; B. BBC; C. SKY News; D. Reuters
Text	Whom did you call at around 7 pm on 17/09/2014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

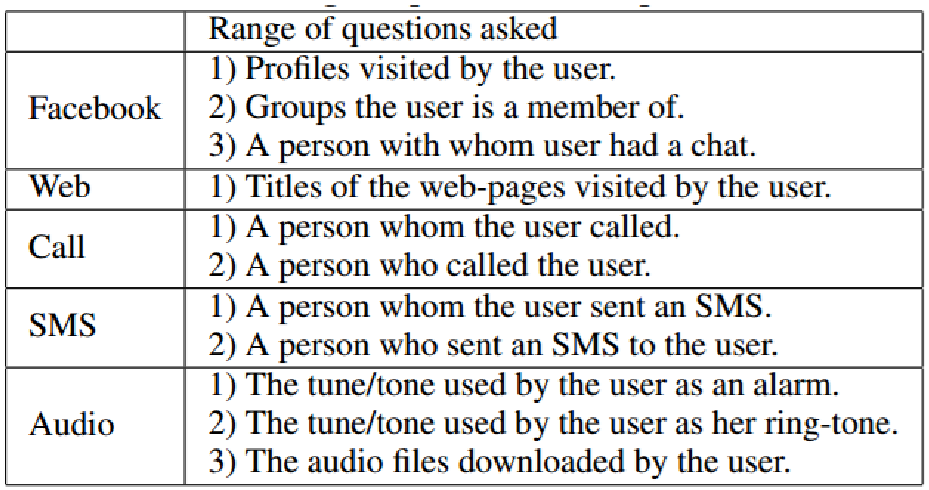
- Paper investigated ActivPass utility by conducting user studies

How ActivPass Works

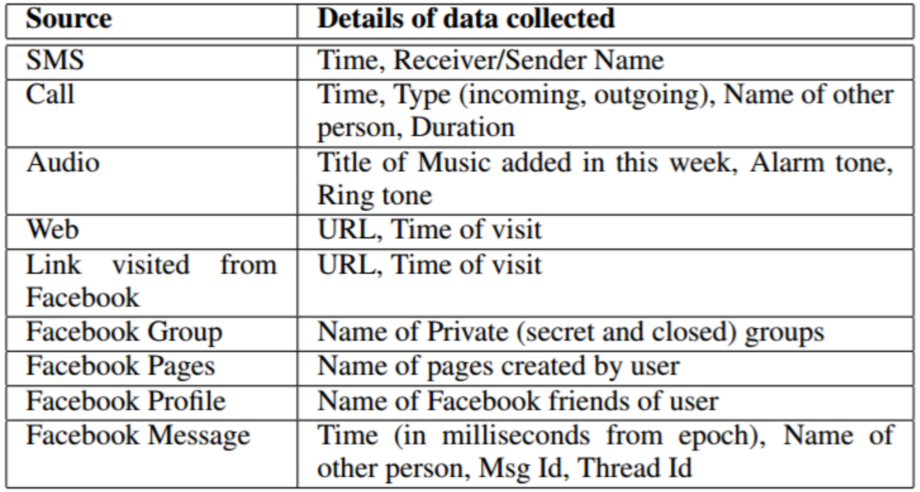
- Periodically retrieves logs in order to classify them using **Activity Categorization Module**
  - Tries to find outliers in the data. E.g. Frequently visited pages vs rarely visited web pages


Facebook Application (SocialActivity) to collect semi-private data
Irrelevant
Non-Outlier
Android App to collect call and SMS meta-data
Activity Collection
Activity Categorization
Outlier
Challenge Generation
Browser Extension to collect web history
Content Script to capture link followed from Facebook
PGM

ActivPass: Types of Questions Asked Vs Data Logged



	Range of questions asked
Facebook	1) Profiles visited by the user. 2) Groups the user is a member of. 3) A person with whom user had a chat.
Web	1) Titles of the web-pages visited by the user.
Call	1) A person whom the user called. 2) A person who called the user.
SMS	1) A person whom the user sent an SMS. 2) A person who sent an SMS to the user.
Audio	1) The tune/tone used by the user as an alarm. 2) The tune/tone used by the user as her ring-tone. 3) The audio files downloaded by the user.



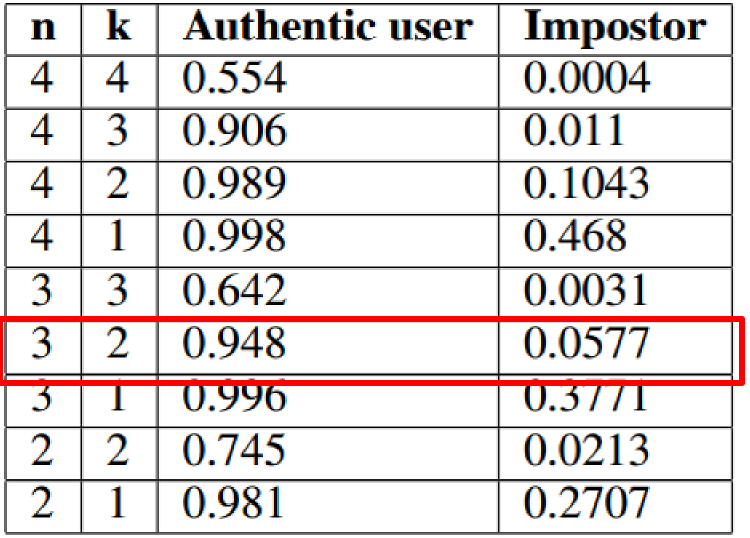
Source	**Details of data collected**
SMS	Time, Receiver/Sender Name
Call	Time, Type (incoming, outgoing), Name of other person, Duration
Audio	Title of Music added in this week, Alarm tone, Ring tone
Web	URL, Time of visit
Link visited from Facebook	URL, Time of visit
Facebook Group	Name of Private (secret and closed) groups
Facebook Pages	Name of pages created by user
Facebook Profile	Name of Facebook friends of user
Facebook Message	Time (in milliseconds from epoch), Name of other person, Msg Id, Thread Id

ActivPass: Evaluation

- Over 50 volunteers given 20 questions:
  - Avg. recall rate: 86.3% ± 9.5 (user)
  - Avg guessability: 14.6% ± 5.7 (attacker)

- Devised Bayesian estimate of challenge given *n* questions where *k* are required

- Tested on 15 volunteers
  - Authenticates correct user 95%
  - Authenticates imposter 5.5% of the time (guessability)



n	k	Authentic user	Impostor
4	4	0.554	0.0004
4	3	0.906	0.011
4	2	0.989	0.1043
4	1	0.998	0.468
3	3	0.642	0.0031
3	2	0.948	0.0577
3	1	0.996	0.3771
2	2	0.745	0.0213
2	1	0.981	0.2707

Optimal *n, k*

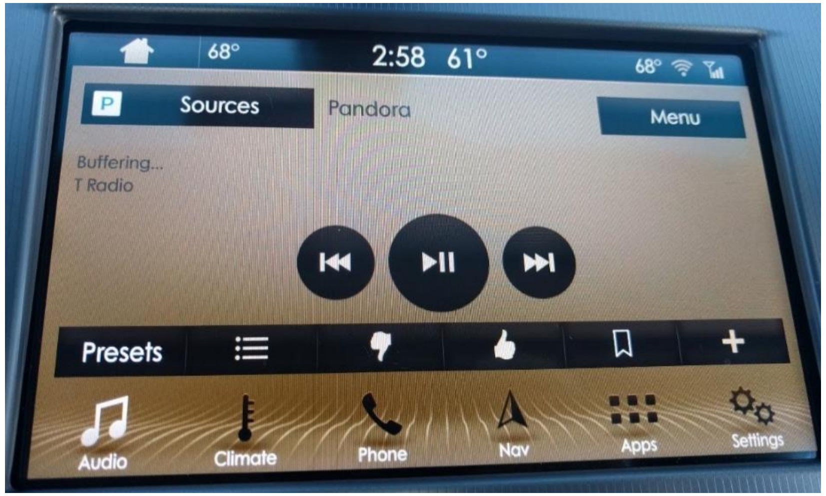
Maximize

Minimize

Smartphones + IoT Security Risks

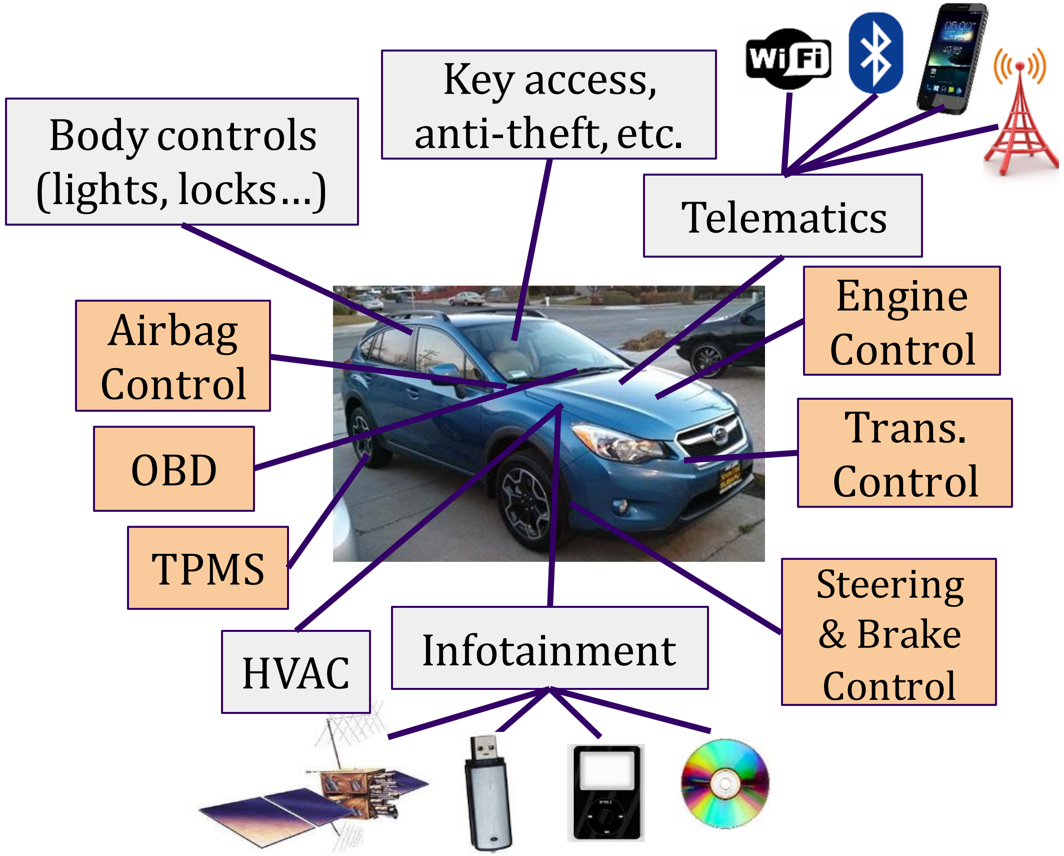
Cars + Smartphones → ?

- Many new vehicles come equipped with smartphone integration / capabilities in the infotainment system (Android Auto!)



Smartphones that Drive

- If a mobile app gets access to a vehicle's infotainment system, is it possible to get access to (or even to control) driving functionality?



Smart Vehicle Risks

- Many of the risks and considerations that we discussed in this course can be applied to smart vehicles and smartphone interactions

- However, many more risks come into play because of the other functionality that a car has compared to a smartphone

Secure Mobile Software Development Modules

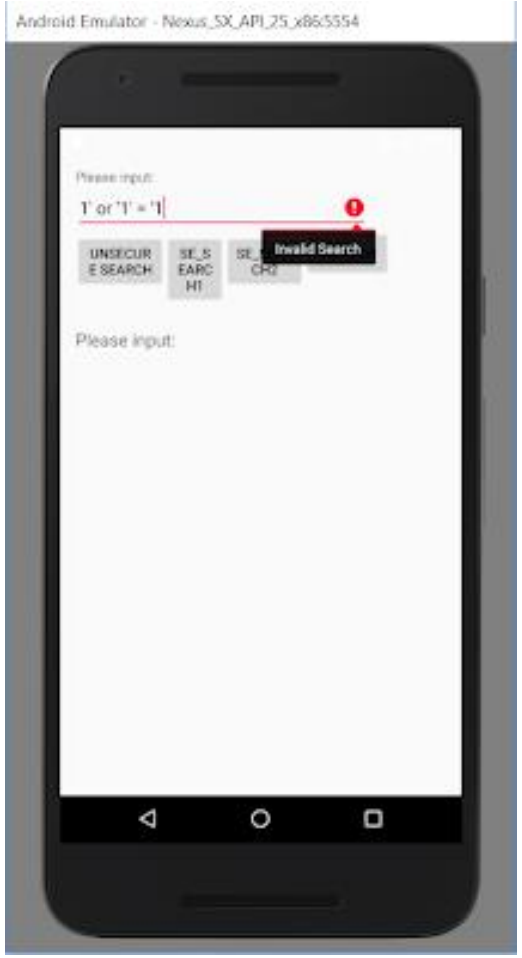
Introduction

- Many Android smartphones compromised because users download malicious software disguised as legitimate apps
- Malware vulnerabilities can lead to:
  - Stolen credit card numbers, financial loss
  - Stealing user's contacts, confidential information
- Frequently, unsafe programming practices by software developers expose vulnerabilities and back doors that hackers/malware can exploit
- Examples:
  - Attacker can send invalid input to your app, causing confidential information leakage

Secure Mobile Software Development (SMSD)

- **Goal:** Teach mobile (Android) developers about backdoors, reduce vulnerabilities in shipped code

- SMSD:
  - Hands-on, engaging labs to teach concepts, principles
  - Android plug-in: Highlights, alerts Android coder about vulnerabilities in their code
  - Quite useful



Android Emulator - Nexus_5X_API_25_x86:5554

Please input:

1' or '1' = '1

Invalid Search

Please input:

SMSD: 8 Modules

- Focussed more on teaching you about the modules
- M0: Getting started
- M1: Data sanitization for input validation
- M2: Data sanitization for output encoding
- M3: SQL injections
- M4: Data protection
- M5: Secure inter-process communication (IPC)
- M6: Secure mobile databases
- M7: Unintended data leakage
- M8: Access control

- https://sites.google.com/view/projectsmsd/home

Open Source SMSD API Plugin for Android Studio IDE

- Plugin you can use to scan your Android projects for vulnerabilities

- M0. Getting Started with SpotBugs for Android Static Code Analysis
- M1. Potential SQL Injection Vulnerability Detecting with SpotBugs
- M2. Data Sanitization for output encoding Vulnerability Detecting with SpotBugs
- **M3. Intent Interception and Spoofing Vulnerability Detecting with SpotBugs**
- **M4 InterAppSender Access Control Vulnerability Detecting with SpotBugs**

M7 & M8 Overview

- M7: Blah
- Unintended Data Leakage
  - Understand fundamental concepts of unintended data leakages from the clipboard
  - Understand defenses against these unintended data leakages
- M8: Inter-App Secure IPC vulnerabilities
  - Malicious app can exploit security loophole in Broadcast Receivers to intercept valuable information