CONTINUOUS AUTHENTICATION OF MOBILE USERS: FUSION OF FACE AND INERTIAL MEASUREMENT UNIT DATA

David Crouse¹, Hu Han¹, Deepak Chandra², Brandon Barbello², and Anil K. Jain¹

¹Michigan State University
²Google, Inc.
Outline

• Background
• Proposed approach
  • Face uprightness correction
  • COTS and component based face matching
  • Confidence function
  • Prototype system on Android
• Experimental results
• Summary
Background

1973 - Motorola DynaTAC Prototype
First mobile phone

1992 – Motorola 3200
First mobile digital phone

1993 – IBM Simon
First smartphone

1999 – Kyocera VP-210
First camera phone

2007 – Apple iPhone
First iOS phone

2008 – HTC Dream
First Android phone

2011 – Samsung Galaxy Nexus
Introduced Face Unlock

2013 – LG Nexus 5
Used for data collection

2013 – iPhone 5S
TouchID

2014 – iPhone 6
Apple Pay

www.businessinsider.com/complete-visual-history-of-cell-phones-2011-5?op=1
wikipedia.com
Background

- **Security concerns**
  - Mobile devices contain personal information, such as e-mail, photos & videos, and financial information
  - 67% of users do not password protect their devices [1]
  - Many users are using too simple passwords, such as ‘1234’, ‘0000’, ‘2580’, ‘1111’, etc. [2]

Users believe it is too complicated to enter a password/PIN!

Background

- Computer passwords were originally intended for mainframes/desktop computers
  - Desktops are stationary and the user is constantly engaged while logged in
- Mobile phones adopted the paradigm
  - Mobile devices are small and easy to steal while unlocked
- Complexity requirements make passwords hard to remember
  - This produces a stigma against password use, they are just “a hassle”

We need a security solution built around mobile!
Proposed Approach

- **Unobtrusive** continuous authentication using face
  - **Unobtrusive:** uncooperative subjects; unconstrained sensing, no change to user workflow
  - **Continuous:** verify user identity periodically
Face Uprightness Correction

1. Device Locked
2. Log in to Device
3. Update Enrollment
4. Wait
5. Capture Images
6. Apply Uprightness Correction
7. Match Faces
   - Above Threshold: Update and Check Confidence
   - Below Threshold: Repeat from Step 1
Face Uprightness Correction

(a) Face images without orientation correction

(b) Images with automatic orientation correction

- IMU is used to correct for device rotation
- Correction uses temporal interpolation
Face Uprightness Correction
COTS and Component-Based Face Matching
COTS and Component-Based Face Matching

- COTS matchers
  - PittPatt SDK in client-server mode
  - Qualcomm SDK in smartphone-only mode
- Component-based matcher (Person-Specific) [1]

Confidence Function

1. Device Locked
2. Log in to Device
3. Update Enrollment
4. Wait
5. Capture Images
6. Apply Uprightness Correction
7. Match Faces
8. Update and Check Confidence

Above Threshold

Below Threshold
Confidence Function

- Initial confidence value in user’s identity = 1.0; decays over time
- If confidence < T (0.6 in our trials), lock the phone
- Raise confidence if the genuine face is recognized; lower the confidence for impostor face
Prototype System on Android

- Android has 81% market share [1]
- Google Nexus 5 smartphone
- Uprightness correction was performed on the device GPU
- Both client-server mode (ICB paper) and smartphone-only mode (ongoing work) have been implemented

Experimental Results

- Face verification
  - Using customized application, we collected images of 10 subjects for 1-6 weeks
  - 250,000 images in 3,600 sessions were collected
  - Roughly 50% of these images contained a face

(a) Full faces
(b) Partial faces
(c) No faces
Experimental Results

- Face verification (in client-server mode)
Experimental Results

- Face verification (in smartphone-only mode)
Experimental Results

- Face verification examples

False reject by COTS, correct accept by our system

False accept by COTS, correct reject by our system
Experimental Results

- User testing
  - 24 subjects used an Android device equipped with the system for multiple sessions
  - For 3 to 5 sessions, subjects operated the device for up to 15 minutes or until they were logged out
  - For an additional 3 to 5 sessions, subjects operated the device for 1 minute, then handed the device to an impostor

![Bar chart showing user testing results](chart.png)
Experimental Results

• Genuine user
Experimental Results

- Impostor user

```csharp
[Graph showing score vs image group with genuine and impostor categories]
```
Summary

- We have presented a robust continuous authentication system for mobile devices.
- Fusion of camera with the device’s IMU allows for enhanced face matching performance.
- Experiments show significant reduction in the time impostors have access to a device while maintaining usability for genuine users.
YOU ARE YOUR SMARTPHONE’S PASSWORD!

Questions?

I have the same password on my luggage!