Mobile Active Authentication via Linguistic Modalities

Rachel Greenstadt, Moshe Kam, Patrick Juola, Patrick Brennan, Lex Fridman

Smart Card Alliance Conference
DARPA Active Authentication
Oct 29, 2014

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).

Outline

- **Overview**
- Tracking Application
- Mobile Dataset
- Dataset Analysis

Active Authentication Performer Overview and Status

Drexel University

PERFORMER OVERVIEW AND STATUS

BIOMETRIC: Stylometry (how people use language when they write) augmented by author classification and verification. Data fusion using stylometry, eye tracking, and other methods.

Key Objectives

Our objective is to develop an authentication modality that infers the identity of the user of a mobile device (cell phone) by analyzing the style and dynamics of his or her interactions with that device.

- Gather a **large data set** of text produced by routine mobile device use for development and testing of the modality.
- Develop modalities based on **eye-tracking** and other low-level interactions with the device.
- **Adapt stylometric techniques** for the authentication problem to validate the identity of writers by analyzing the style of their writing.
  - Investigated **authorship attribution** using higher level linguistic sensors based on Myers-Briggs Personality Type, Handedness, and Gender. These sensors use character bigrams and common words for features, and centroid-based 1-nearest-neighbor leave-one-out validation for classification.
- Integrate known Human-Computer Interaction (HCI) modalities with a **fusion algorithm** and test. We will integrate known and novel low-level modalities (including eye-tracking with a fusion algorithm and test on the data set. We will determine where and when our modalities provide value added over known modalities and where and how known modalities can mitigate the technical and security risks.
- Harden our approach against **active adversaries** that might circumvent it or spoof users

Status

- ✓ Prototype data collection Android application written.
- ✓ Algorithm development in progress.
- ✓ Drexel IRB study approval acquired.
- ✓ Phase 1 results demonstrate stylometry promising in Desktop case
- ○ Phase 2 study underway for 200 subjects.

MOBILE ACTIVE AUTHENTICATION VIA LINGUISTIC AND OTHER MODALITIES

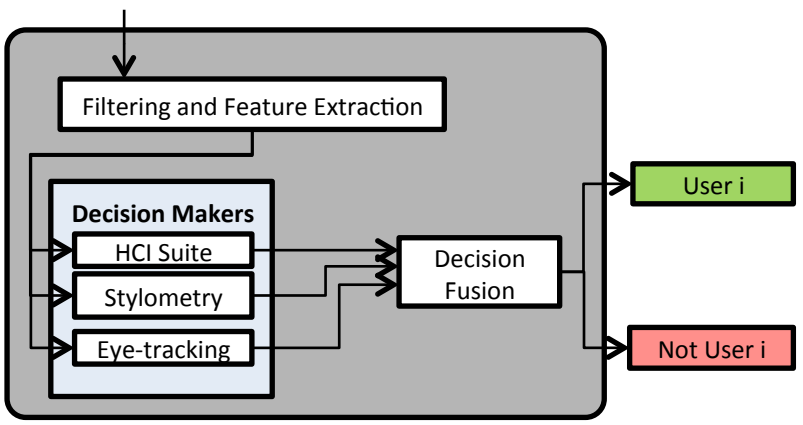
FAR/FRR Performance (on current subset of subjects)

Stylometry: **0.22 / 0.30**

GPS location: **0.15 / 0.23**

Application usage: **0.24 / 0.16**

Fused sensor: **0.11 / 0.15**



Team Members

Principal Investigator: Rachel Greenstadt, Drexel University, Philadelphia, PA

- Moshe Kam (Co-PI), Drexel University, Philadelphia, PA
- Alex Fridman (Researcher), Drexel University, Philadelphia, PA
- Ariel Stolerman (Researcher), Drexel University, Philadelphia, PA
- Jesse Kuehn (Researcher), Drexel University, Philadelphia, PA
- Patrick Juola (Researcher), Juola and Associates, Pittsburgh, PA
- Patrick Brennan (Researcher) , Juola and Associates, Pittsburgh, PA
- John Noecker, Jr. (Researcher) , Juola and Associates, Pittsburgh, PA
- Michael Ryan (Researcher) , Juola and Associates, Pittsburgh, PA

Approach

- Linguistic Modeling
  - Identification based on writing (Stylometry)
  - Personality ID using writing
- Other modalities
  - Application usage
  - Web browsing behavior
  - GPS location
  - Eye movements as users interact with device
- Fusion
  - Fusion of modalities to characterize contribution of each individual modality

Outline

- Overview
- **Tracking Application**
- Mobile Dataset
- Dataset Analysis

Tracking Application:
Successes and Challenges

- Data collected successfully:
  - Keystrokes
  - SMS
  - GPS
  - Images
  - Web history
  - Application usage
  - Gyroscope
- Challenges encountered:
  - Touch tracking
  - Eye tracking
- Personality tests
  - A demographic survey.
  - Myers-Briggs Type Inventory (MBTI)
  - Learning Styles Inventory
  - Multiple Intelligences Developmental Assessment Scales (MIDAS)
  - Rosenberg Self-Esteem Scale
  - NEO Personality Inventory (NEO-PI)
  - HEXECO

Tracked Behavioral Biometrics (Part 1)

Application usage:

2013-05-20 (From) 2013-05-20 (To) Today

Application	Duration	Clicks
VirtualBox	28 min 23 sec	5
explorer	15 min 20 sec	15
AP01Main	5 min 32 sec	4
notepad	4 min 16 sec	6
welcome	1 min 8 sec	2
wmplayer	1 min 3 sec	1
Skype	50 sec	6
Total Applications used:	**57 min 43 sec**	**17**

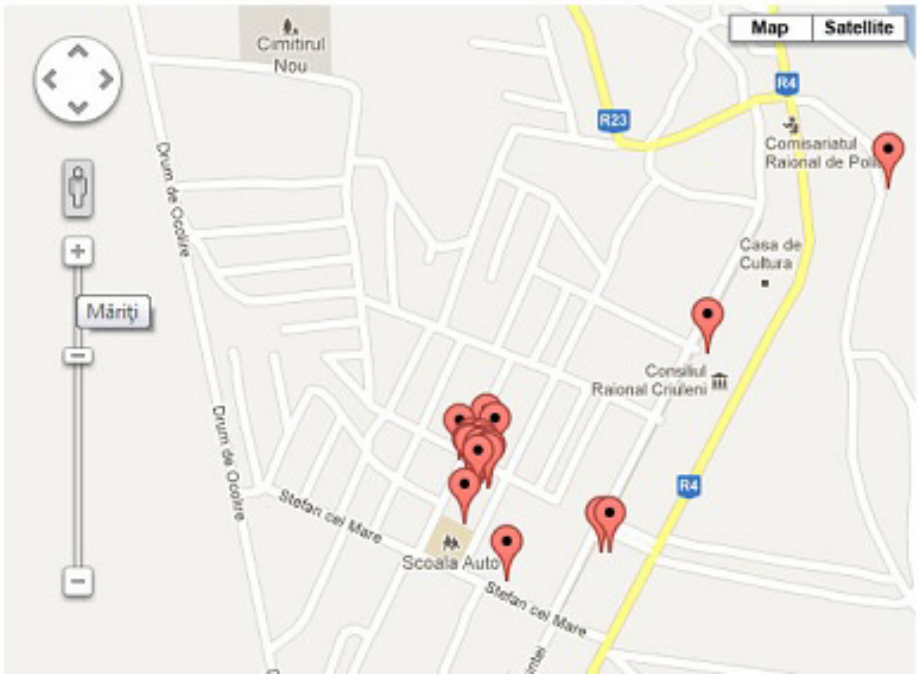
Web history:

2013-03-21 (From) 2013-03-21 (To) -- Other --

Рейтинг посещаемых сайтов	Запросы в строке поиска
2 google.ru 13 min 20 sec	1 timedoctor
2 bing.com 4 sec	1 youtube
1 kidlogger.net 4 min 34 sec	
1 facebook.com 10 min 25 sec	
1 odnoklassniki.ru 5 min 25 sec	
1 flashgames.ru 5 min	
1 chrome 10 sec	
Total Visits: 9	Total Search Queries: 2
Total Sites: 7	

GPS Location:

Total points: 83



Tracked Behavioral Biometrics (Part 2)

Conversations (SMS, Skype)

2011-08-25 From

2011-08-25 To

Yesterday

in_call

- 2. Incoming call: 18885599600 Jary Lu
- 1. Incoming call: 18884166603 Mum

out_call

- 3. New call: 18885599600 Jary Lu
- 1. New call: 18884166603 Mum
- 1. New call: 18884269937 Loly

Skype

Contact	Общение
Tesline Service	29
Colin	15
Unknown contact	3
Cirlig Alina	2
Pedersen & Partners	1
Patrak	1
Total messages	**51**

Gyroscope

Outline

- Overview
- Tracking Application
- **Mobile Dataset**
- Dataset Analysis

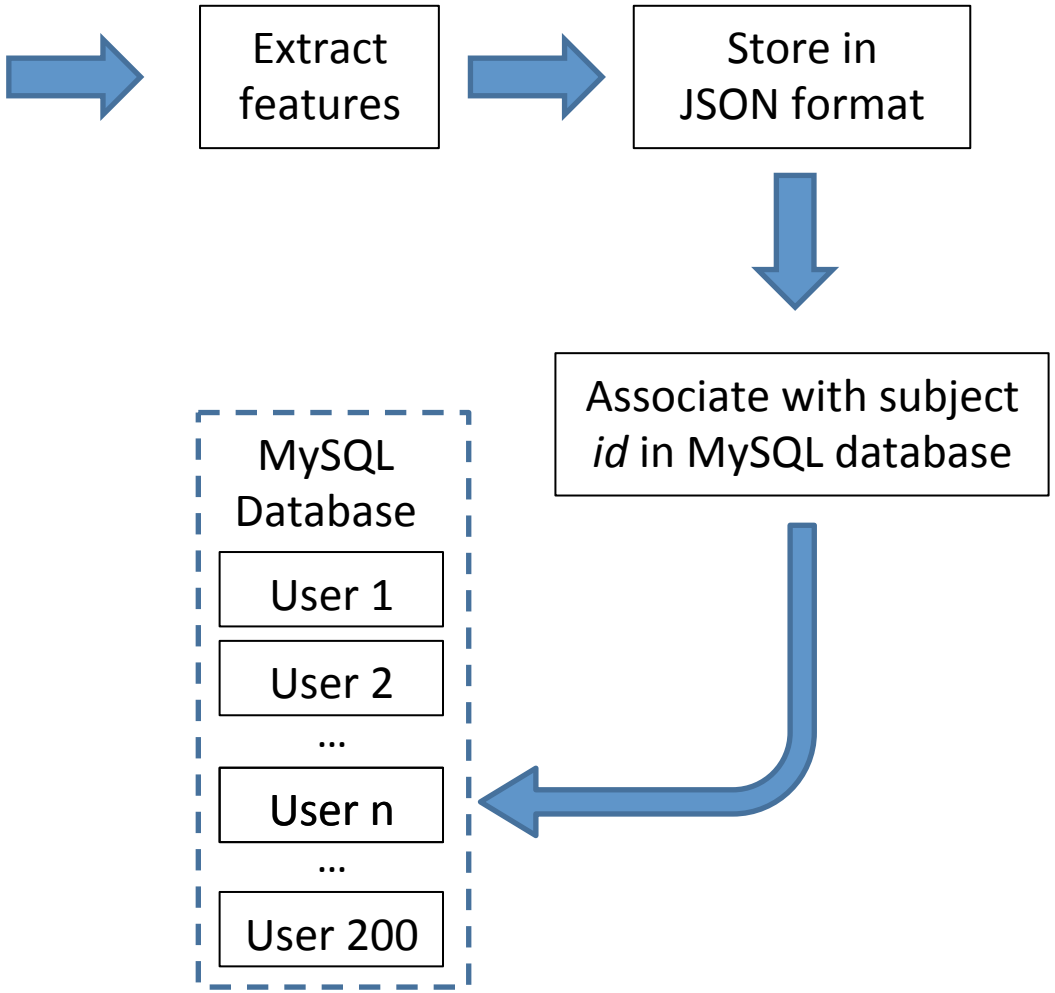
Mobile Dataset

- This section will show:
  - How tracked data is processed and organized.
  - Statistics on the collected data.
  - Statistics on the personality tests.

Processing Tracked Data

Raw data from KidLogger app

15:30	Messages
14:45	com.android.browser otdrdant
14:45	HTC Sense
14:45	Search Query: mordant
14:37	http://m.cookingchanneltv.com
14:37	com.android.browser an dan noodle recipe
14:37	http://m.cookingchanneltv.com/recipes/ching-he-huang/chings-midnight-d
14:36	https://www.ets.org
14:36	http://www.foodnetwork.com/recipes/alton-brown/dan-dan-noodles-recipe.
14:36	Search Query: dan dan noodle recipe
14:36	https://www.ets.org/gre
14:36	com.android.browser an dan noodle
14:36	https://www.ets.org/gre/revised_general/scores/understand/
14:35	Internet
14:33	Messages
14:32	Gallery
14:32	Messages
08:39	HTC Sense
08:39	system Logging started by system
08:39	in_call: 8622216000 Tania Maheshwari
08:38	Phone
01:32	Location



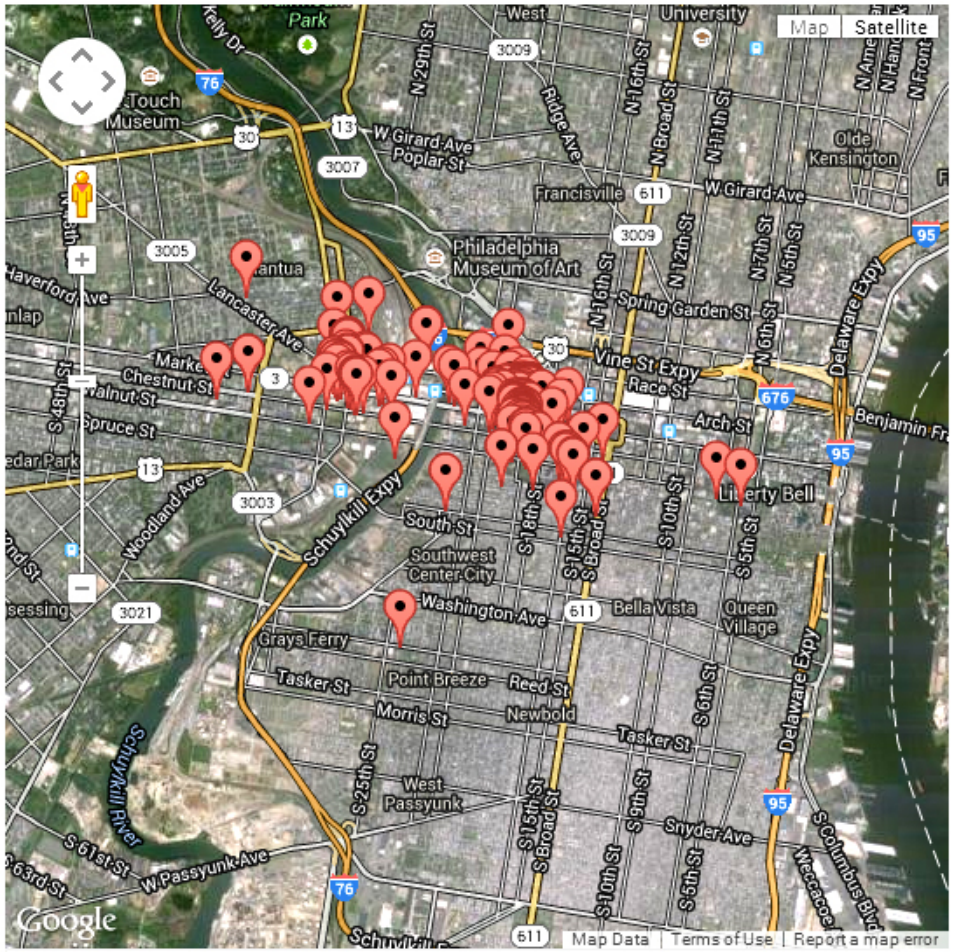
Status of Data Collection

- **174** subjects enrolled with more than 2 weeks of data already collected for each.
- **113** subjects with more than 30 days worth of data.
- **26** subjects scheduled to be enrolled in study.

The following slides provide some statistics and preliminary analysis on the data collected from the 174 subjects already enrolled.

Statistics on Data Collected: GPS Locations

Average locations sampled: ***19 locations*** *per user per day*



14:44:00	GPS POINT(39.95440021,-75.1864592)
14:57:00	GPS POINT(39.9566352,-75.1896297)
15:49:00	GPS POINT(39.9566352,-75.1896297)
17:41:00	GPS POINT(39.95450597,-75.18622069)
17:50:00	GPS POINT(39.95551214,-75.18950851)
18:05:00	GPS POINT(39.9575157,-75.1818912)
18:15:00	GPS POINT(39.95505982,-75.19033025)
18:26:00	GPS POINT(39.9575157,-75.1818912)
18:35:00	GPS POINT(39.95488319,-75.19033078)
19:05:00	GPS POINT(39.9575157,-75.1818912)
19:42:00	GPS POINT(39.95499943,-75.19071759)
20:14:00	GPS POINT(39.9575157,-75.1818912)
20:27:00	GPS POINT(39.95521819,-75.19089456)
20:47:00	GPS POINT(39.95235461,-75.17560776)
20:59:00	GPS POINT(39.95176584,-75.1730081)
21:15:00	GPS POINT(39.9503479,-75.184907)
21:29:00	GPS POINT(39.95172833,-75.17324544)
21:39:00	GPS POINT(39.94955917,-75.17199491)
21:59:00	GPS POINT(39.94805772,-75.17130214)
22:12:00	GPS POINT(39.9532691,-75.1717448)
22:33:00	GPS POINT(39.95194468,-75.17238505)
22:46:00	GPS POINT(39.9532691,-75.1717448)
23:09:00	GPS POINT(39.95453424,-75.17283532)
23:24:00	GPS POINT(39.9532691,-75.1717448)

Statistics on Data Collected

- Average GPS locations:
  19 locations per user per day
- Average SMS/Chat messages:
  28 messages per user per day
- Average websites visited:
  14 websites per user per day
- Average apps (duplicates included) launched:
  79 apps launched per user per day

Outline

- Overview
- Tracking Application
- Mobile Dataset
- **Dataset Analysis**

Preliminary Results for Partial Mobile Dataset

- **Dataset:** 174
- **Duration:** 2-4 weeks of data for each
- Performance cross validation parameters:
  - Training set size: 60%
  - Fusion characterization set size: 20%
  - Testing set size: 20%
- Time to authenticate: 10 minutes
- Performance *(still being analyzed)*
  - FAR/FRR for GPS location: 0.06 / 0.08
  - FAR/FRR for application usage: 0.12 / 0.19
  - FAR/FRR for fused sensor: 0.06 / 0.06
  - *Eye tracking and full stylometric analysis pending.*

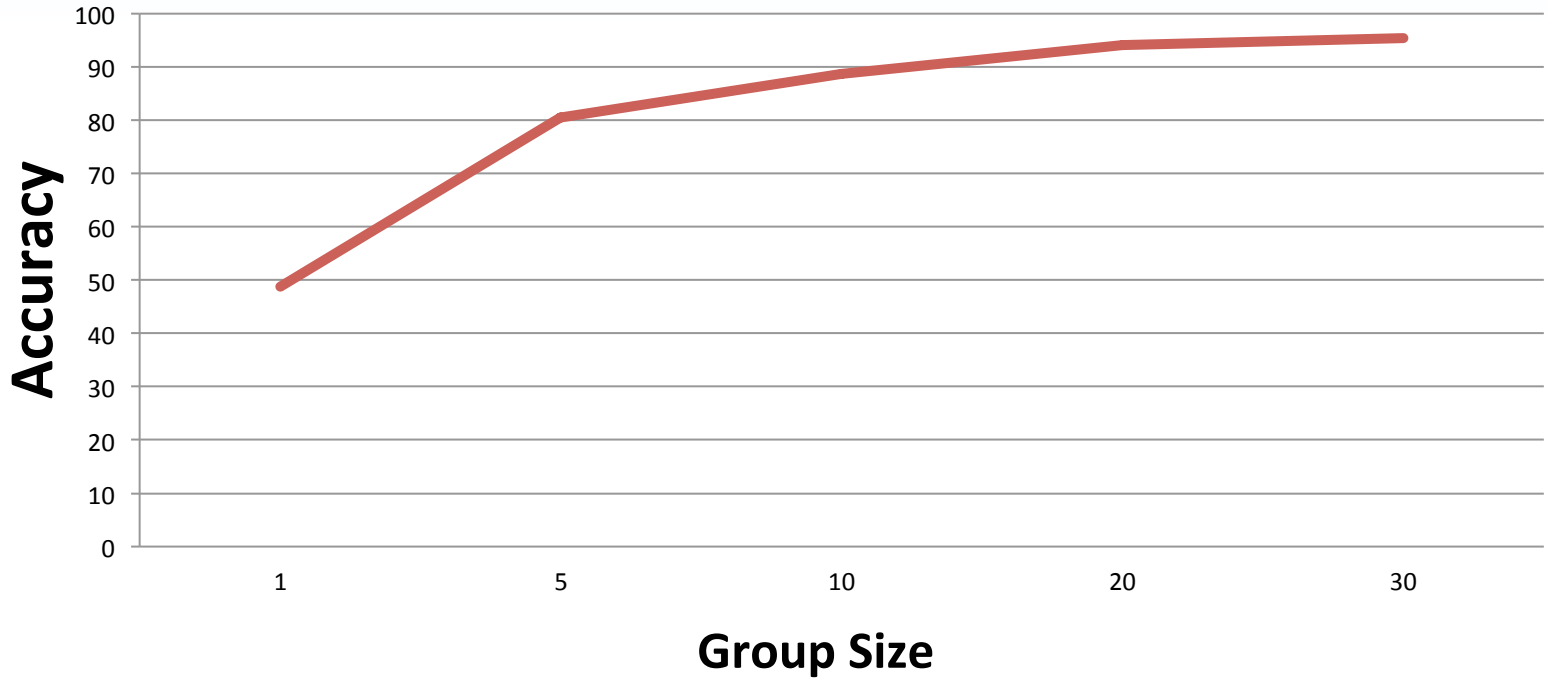
Mobile Twitter Corpus

- Collected feeds from 249 users
- Filter data to contain only tweets from **mobile** sources (Android, iPhone, Blackberry, etc.)
- Average 567 mobile tweets per user
- Scraped using the Twitter API

Stylometry on Microtext Data

- Microtext documents
  - Tweets, SMS Messages, short emails etc.
- Randomly arrange authors
- Break them into groups of 15
- Group these tweets by 1, 5, 10, 20, 30
- Features: Writeprints Feature Set

Results: Microtext Corpus



Group Size	Accuracy (TP)	FP Rate
1	48.75200667	0.071284884
5	80.55229667	0.021704068
10	88.72031667	0.012703128
20	94.13021333	0.006378687
30	95.34706	0.005006918

Results 2: Stylometry on Microtext

- Twitter Corpus
  - Accuracy: 55.7%
  - Chance: .4%
- P1 Active Authentication Corpus, By-User
  - 80 character chunks
    - Accuracy: 40.8%
    - Chance: 1.25%
  - 60 character chunks
    - Accuracy: 33.8%
    - Chance: 1.25%
  - 40 character chunks
    - Accuracy: 25.6%
    - Chance: 1.25%

Singaporean English SMS Corpus

- We have acquired an SMS corpus from Singapore
- The language was English
- We cleaned up all messages with less than 50 characters
- There were 202 authors with an average of 90 tweets per author
- Best performing method had a result of 47.94% accuracy (9273 / 19342)
  - Chance is .495%

Stylometry Verification on P2 Mobile Data

- Verification is an open-class, one-to-one detection method
  - Attribution is closed-class one-to-many
  - Essentially, verification asks “is this user person x, yes or no?”
- Using LOO we sequestered a portion of the data, then using the rest of the data we built a distractor set and generated a threshold for each user
- Time to authenticate: 1 minute of keystrokes
- FAR: 0.22
- FRR: 0.30

Twitter MBTI Corpus

- We have generated a tweet corpus for each Myers-Briggs personality type. (16 types in total)
- The language was English
- There were 234 authors with an average of 1500 tweets per author
- Best performing method had a result of 20.88%
  - Base accuracy is 6.25%
- Single-category classification average accuracy was 59.8%

P1 Personality Results

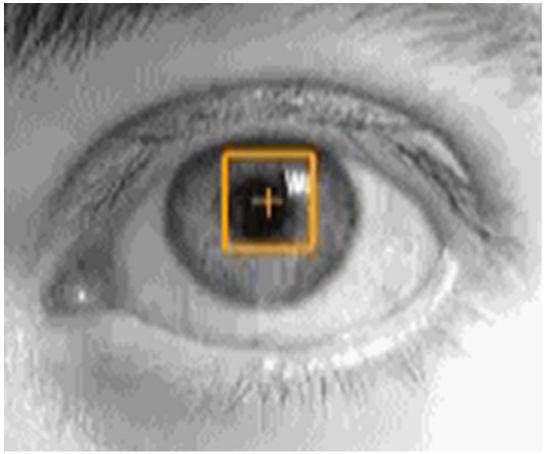
- P1 Active Authentication Corpus, MIDAS Categories
  - 80 character chunks
    - Accuracy: 42.2%
    - Chance: 11.1%
- P1 Active Authentication Corpus, MBTI
  - 200 character chunks
    - Accuracy: 68.92%
    - Chance: 50%
- P1 Active Authentication Corpus, Self Esteem
  - 80 character chunks
    - Accuracy: 49.01%
    - Chance: 20%
- P1 Active Authentication Corpus, Learning Styles
  - 80 character chunks
    - Accuracy: 48.51%
    - Chance: 14.29%

P2 Personality Results

- P2 Active Authentication Corpus, MBTI
  - Individual Messages
    - E/I
      - Accuracy: 89.38%
      - Chance: 50%
    - N/S
      - Accuracy:83.23%
      - Chance: 50%
    - T/F
      - Accuracy: 94.26%
      - Chance: 50%
    - J/P
      - Not enough data for analysis

Eye-Tracking

- **Features**
  - **Fixations:** We look at things by fixating on them (holding it relatively still for 200-600 ms)
  - **Saccades:** Between fixations our gaze jumps (called saccades). These last 30-120 ms.
  - **Scanpath:** A sequence of saccade, fixation, saccade.



©Evangelos Skodras and Nikos Fakotakis

- **Required algorithm characteristics:**
  - Does not require calibration
  - Robust to low-light conditions
  - Robust to occlusions
- **Our implementation:**
  - OpenCV
  - C++

Preliminary Results

- **Dataset:** 60 subjects
- **Duration:** 10 minutes of active use.
- **Training** on 6 minutes, **characterization** on 2 minutes, and **testing** on 2 minutes

- Performance:
  - **Eye tracking**
    - FAR/FRR: 0.28 / 0.22
  - **Eye tracking fused with Gyroscope**
    - error rate: 0.14 / 0.17