Future Authentication

Max Smith-Creasey
Security Research Specialist
Active Defence
Applied Research

Mechanisms for authentication

How we currently authenticate

- In this field the literature reveals **three** ways a user authenticates.

Something you know
- Passwords
- PINs
- Patterns
- Secret answers
- Pass phrase

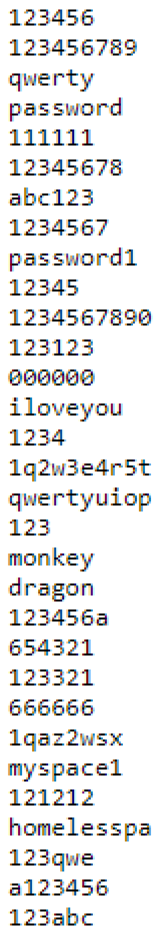
Something you have
- Pass-card
- Passport
- NFC card / key

Something you are
- Biometrics
  - Face
  - Iris
  - Fingerprint
  - Voice

- Traditionally authentication has favoured **something we know** and **something we have** to authenticate.

- New sensing and processing technologies has enabled authentication via **something we are**.

- Continuous sensor sampling can facilitate authenticating users **continuously**, allowing for **continuous authentication**.



```
123456
123456789
qwerty
password
111111
12345678
abc123
1234567
password1
12345
1234567890
123123
000000
iloveyou
1234
1q2w3e4r5t
qwertyuiop
123
monkey
dragon
123456a
654321
123321
666666
1qaz2wsx
myspace1
121212
homelesspa
123qwe
a123456
123abc
```

Most common passwords according to UK's National Cyber Security Centre

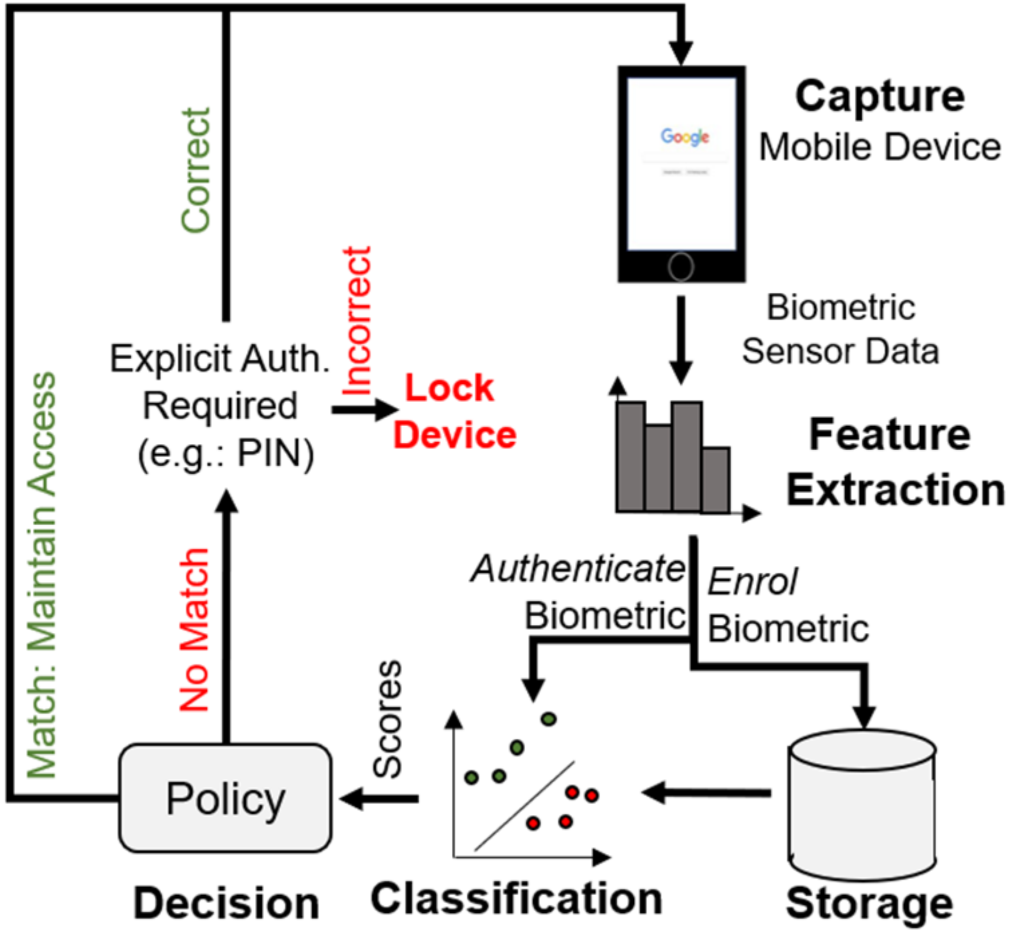
Future Authentication

Concept of continuous authentication

- Schemes that train **models** on **physiological** and/or **behavioural biometrics** such that future samples can be **continuously collected** and **assessed**.

- There five key modules that most schemes have:
  - **Capture** – to obtain sensor data
  - **Feature Extraction** – pre-processing
  - **Storage** – storage of templates or ML models
  - **Classification** – algorithms for comparing
  - **Decision** – engine to assess scores

- If score from user traits does not match known profile, device can **enforce policy in real-time**.

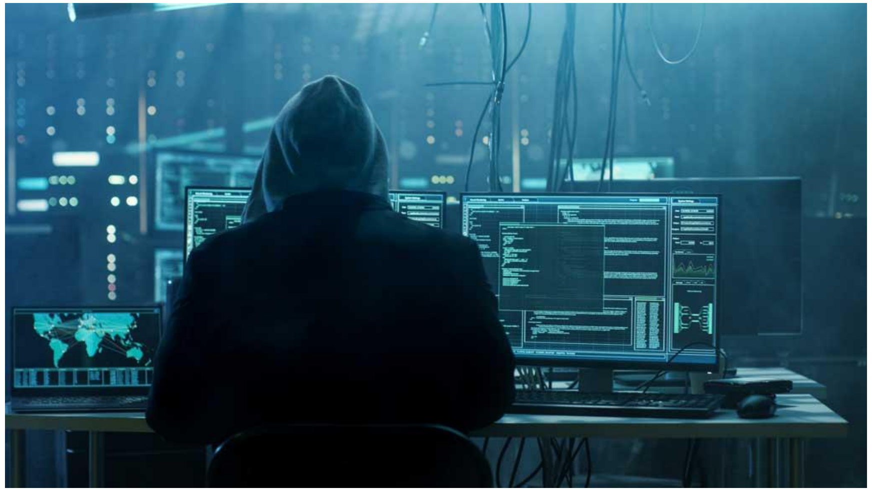


Motivations

Why investigate continuous authentication?

- Devices **lack protection when unlocked** with **traditional authentication** techniques.
  - Consequence of current authentication being **'one-shot'**.
  - Massive **business issue** of screens left unlocked.
  - **34% breaches** are via **internal actors** (Verizon, 2020).
- Plethora of **high quality sensors** on most user devices.
- Doesn't suffer from **poor password/PIN selection**.
- **Harder to attack**
  - No password/token to be observed/stolen
  - Behavioural biometrics especially hard to 'mimic'
  - Can use multiple biometrics.
- **Transparent** and **convenient**. Seen as more **secure**.
- Would be **used** by significant number of users.

Passwords can leave users fighting security for usability.



Systems left unlocked can be used by anybody…

Devices and Sensors

What’s the art of the possible with current devices/sensors?

Laptop/Desktop Computers

- General Behaviour – times/files/programs accessed
- Camera – Face recognition
- Keyboard – keystroke dynamics
- Mouse – Mouse movements
- Wifi – Trusted hotspots
- Bluetooth – Trusted local devices
- Microphone – Voice biometrics

Smartphones

General Behaviour – times/files/apps

- GPS – trusted locations
- Camera – Face recognition
- Touchscreen – touch dynamics
- Wifi – Trusted hotspots
- Movements – Gait recognition
- Bluetooth – Trusted local devices
- Microphone – Voice biometrics

Virtual Reality Headsets

- General Behaviour – times/files/programs accessed
- Accelerometer/Gyroscope – gait, other movements
- Microphone – voice recognition

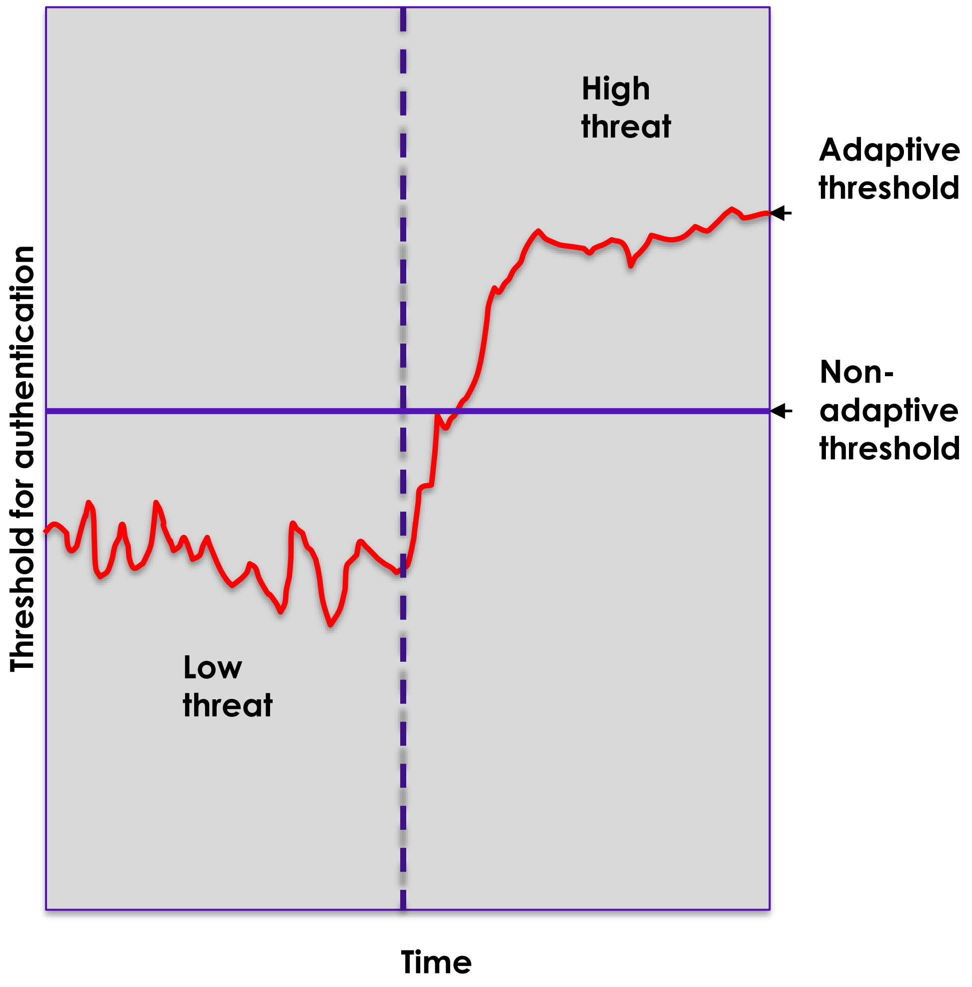
Smartwatches

- General Usage – activity times, etc.
- Accelerometer/Gyroscope – gait, other movements
- Microphone – voice recognition
- ECG/photoplethysmography – cardiovascular indicators

Policies

What policies/decisions could continuous auth facilitate?

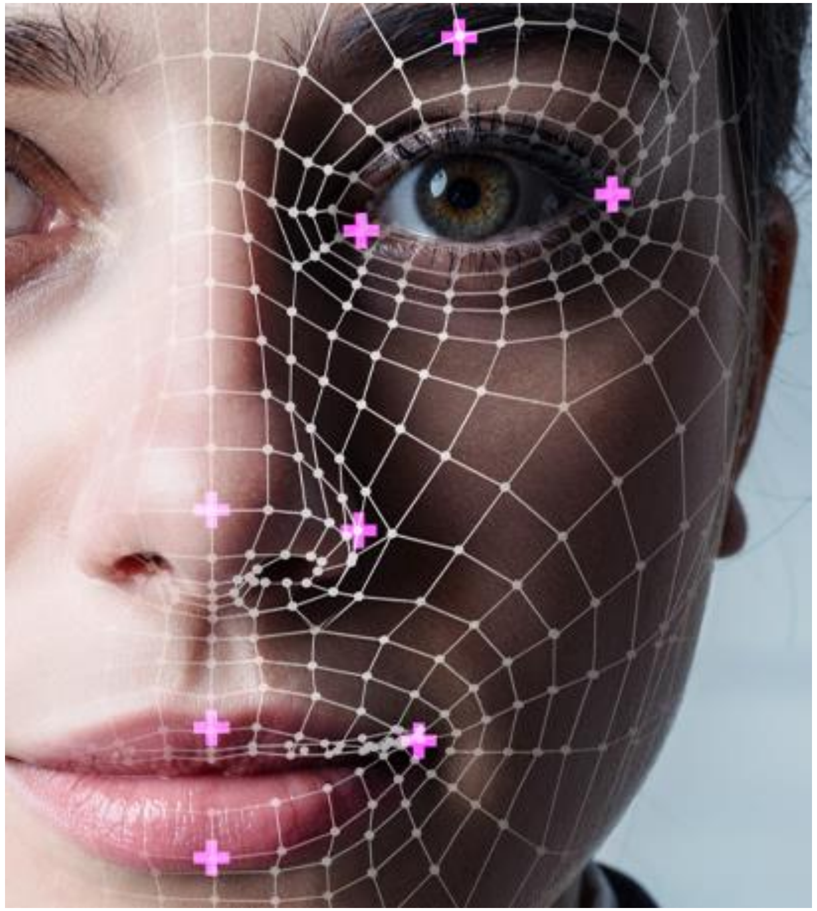
- This form of authentication is **very flexible**.
- It can be used as **sole**, **second factor**, or **back up factor**.
- Security can be **increased/decreased** with thresholds.
- Policies can be highly flexible if biometrics don’t match, e.g.:
  - Completely **lock device**.
  - Revoke **access** to *certain* resources.
  - **Flag the system** to an admin.
  - **Require explicit re-authentication** (e.g.: PIN).
- Custom **grace periods** could be set.
- Can react if **threat** on network, **requiring more biometrics or higher thresholds**



Challenges

What are some challenges facing continuous authentication?

- **Spoof detection**
  - It's well known that faces/fingerprints have been spoofed in the past.
  - How can we **protect continuous auth** from spoof attacks?
- **Demographic bias**
  - Many studies in continuous auth field are **small**.
  - Models could lead to bias in systems.
  - How can this be mitigated for different types of data?
- **Security/Usability/Privacy**
  - What is **optimal compromise** between security, usability and privacy?



Conclusions

- Continuous authentication is a future authentication **hot topic** for both **research** and **industry** on all devices.

- Overcomes **issues** with existing authentication techniques and **builds security layer on top**.

- Helps address emerging problems facing businesses such as **insider attacks** and need for **passwordless authentication**

- Promising and **upcoming field**, but still **challenges faced**.