Authentication Using Pulse-Response Biometrics

Kasper B. Rasmussen[1] Marc Roeschlin[2]
Ivan Martinovic[1] Gene Tsudik[3]

[1]University of Oxford [2]ETH Zurich [3]UC Irvine

Clermont Ferrand, 2014

A Bit About Myself

Lecturer at University of Oxford.

Current Research Topics

- Security of Wireless Networks
- Protocol design
- Applied Cryptography
- Security of embedded systems
- Cyber-physical systems
- Oh yes—Biometrics.

Outline

UNIVERSITY OF OXFORD

1. Background on Biometrics
2. Pulse-Response
3. Security Applications
4. Experimental Results

Biometrics: A Definition

Biometrics

A means to identify individual human beings by their characteristics or traits.

Biometrics

Behavioral

Keystroke timing, speech pattern analysis, gait recognition and hand-writing

Physiological

Fingerprints, hand geometry, facial recognition, speech analysis and iris/retina scans

Biometrics

Unobtrusive

Keystroke timing, speech pattern analysis, gait recognition, hand-writing, facial recognition and speech analysis

Invasive

Fingerprints, hand geometry and iris/retina scans

Why a New Biometric?

- Some biometrics are “secure” but “hard to use”.
    - Fingerprints
    - Iris/Retina
- Others are “less secure” but “easy to use”.
    - Face recognition
    - Key-stroke dynamics

Biometric Design Goals

1. Universal: The biometric must be universally applicable, to the extent required by the application.

2. Unique: The biometric must be unique within the target population.

3. Permanent: The biometric must be consistent over the time period where it's used.

Biometric Design Goals ...cont.

4. Unobtrusive: An unobtrusive biometric is much more likely to be accepted.
5. Difficult to circumvent: Essential for a biometric in any security context.

...also, for completeness

Collectability, Acceptability and Cost Effectiveness

Biometrics in Security

Identification

Obtain the identity of a user.

vs.

Authentication

Confirm the identity of a user.

Biometrics in Security

Identification

Obtain the identity of a user.

vs.

Authentication

Confirm the identity of a user.

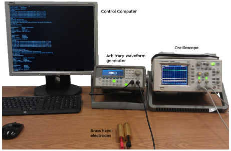
Continuous Authentication

Continuously confirm the identity of a user.

Pulse-Response Biometric

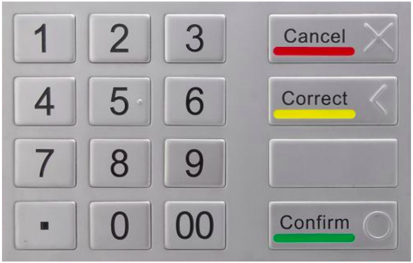
- Pulse signal applied to the palm of one hand.
- The biometric is captured by measuring the response in the user's hand.

User Safety

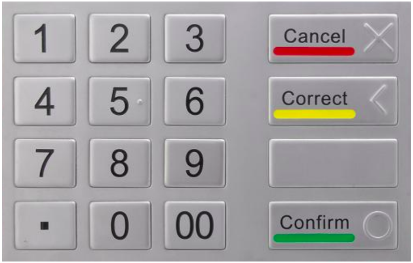


Voltage (V)	1	1.5
Max Current (mA)	0.1	500+
Exposure	100ns	∼500ms

Case 1: Hardening PIN Entry



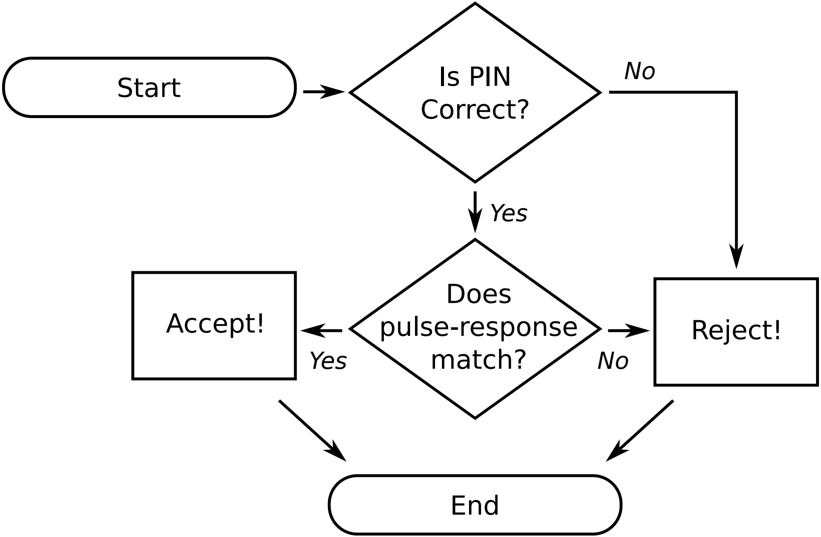
Case 1: Hardening PIN Entry



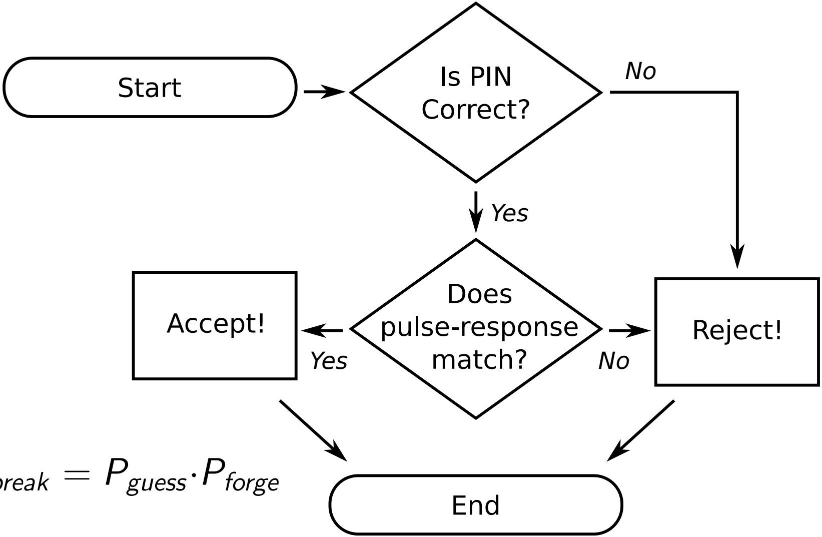
Biometric Properties

Universality, Uniqueness, Permanence, Unobtrusiveness, Circumvention Difficulty

ATM Decision Flowchart



ATM Decision Flowchart



$$P_{break} = P_{guess} \cdot P_{forge}$$

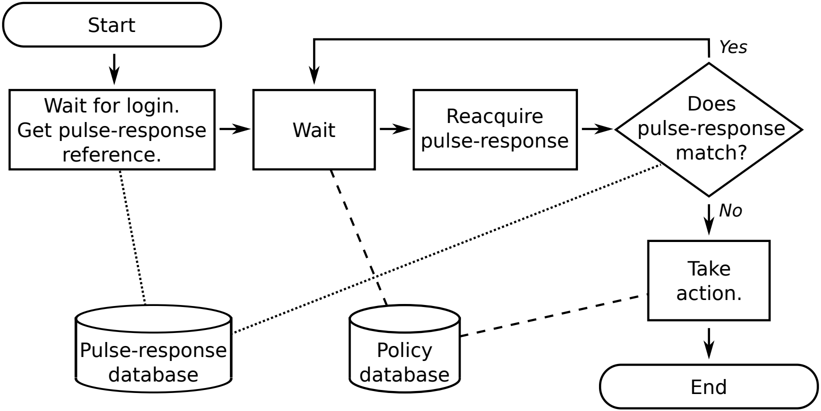
Case 2: Continuous Authentication

Case 2: Continuous Authentication

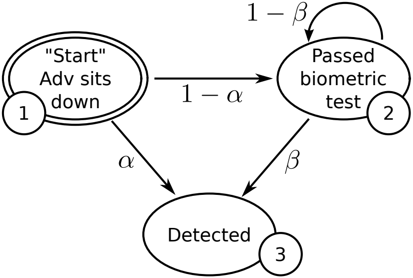
Biometric Properties

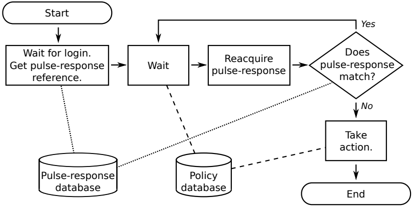
Universality, Uniqueness, Permanence, Unobtrusiveness, Circumvention Difficulty

Cont. Auth. Decision Flowchart

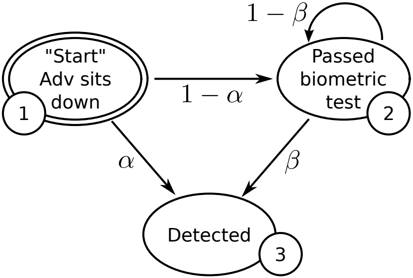


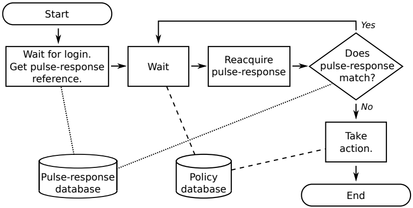
Cont. Auth. Security





Cont. Auth. Security





$$P = \begin{bmatrix} 0 & 1-\alpha & \alpha \\ 0 & 1-\beta & \beta \\ 0 & 0 & 1 \end{bmatrix}$$

Cont. Auth. Security

UNIVERSITY OF OXFORD

$$P = \begin{bmatrix} 0 & 1-\alpha & \alpha \\ 0 & 1-\beta & \beta \\ 0 & 0 & 1 \end{bmatrix}$$

Probabilities after i rounds, starting in state 1

$$\begin{aligned}[1,0,0]\cdot P^i = [0,& \\ &(1-\alpha)(1-\beta)^{i-1}, \\ &1-(1-\alpha)(1-\beta)^{i-1}]\end{aligned}$$

Probability of detection (state 3) for $i = 10$

$$\begin{aligned}1-(1-\alpha)(1-\beta)^{i-1} &= 1-(1-0.99)(1-0.3)^{10-1} \\ &= 1-0.01\cdot 0.7^9 \approx 99.96\%\end{aligned}$$

Cont. Auth. Security

$$P = \begin{bmatrix} 0 & 1-\alpha & \alpha \\ 0 & 1-\beta & \beta \\ 0 & 0 & 1 \end{bmatrix}$$

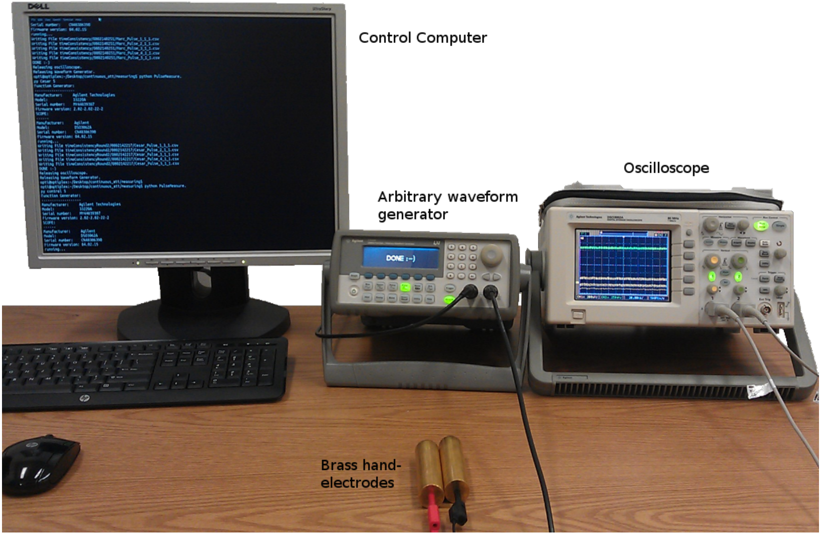
Probabilities after i rounds, starting in state 1

$$\begin{aligned}[1,0,0] \cdot P^i = [0,& \\ &(1-\alpha)(1-\beta)^{i-1}, \\ &1-(1-\alpha)(1-\beta)^{i-1}]\end{aligned}$$

Probability of detection (state 3) for $i = 10$

After 50 rounds this grows to 99.99999997%

Experimental Setup



```
Serial number:    CN48306390
Firmware version: 04.02.15
running...
writing file timeConsistency/0002140251/Marc_Pulse_1_1_1.csv
writing file timeConsistency/0002140251/Marc_Pulse_2_1_1.csv
writing file timeConsistency/0002140251/Marc_Pulse_3_1_1.csv
writing file timeConsistency/0002140251/Marc_Pulse_4_1_1.csv
writing file timeConsistency/0002140251/Marc_Pulse_5_1_1.csv
DONE :-)
Releasing oscilloscope.
Releasing Waveform Generator.
opti@optiplex:~/Desktop/continuous_att/measuring$ python PulseMeasure.
py Cesar 5
Function Generator:
-------------------
Manufacturer:     Agilent Technologies
Model:            33220A
Serial number:    MY44039387
Firmware version: 2.02-2.02-22-2
SCOPE:
------
Manufacturer:     Agilent
Model:            DSO3062A
Serial number:    CN48306390
Firmware version: 04.02.15
running...
writing file timeConsistencyRound2/0002142217/Cesar_Pulse_1_1_1.csv
writing file timeConsistencyRound2/0002142217/Cesar_Pulse_2_1_1.csv
writing file timeConsistencyRound2/0002142217/Cesar_Pulse_3_1_1.csv
writing file timeConsistencyRound2/0002142217/Cesar_Pulse_4_1_1.csv
writing file timeConsistencyRound2/0002142217/Cesar_Pulse_5_1_1.csv
DONE :-)
Releasing oscilloscope.
Releasing Waveform Generator.
opti@optiplex:~/Desktop/continuous_att/measuring$
opti@optiplex:~/Desktop/continuous_att/measuring$ python PulseMeasure.
py control 5
Function Generator:
-------------------
Manufacturer:     Agilent Technologies
Model:            33220A
Serial number:    MY44039387
Firmware version: 2.02-2.02-22-2
SCOPE:
------
Manufacturer:     Agilent
Model:            DSO3062A
Serial number:    CN48306390
Firmware version: 04.02.15
running...
```

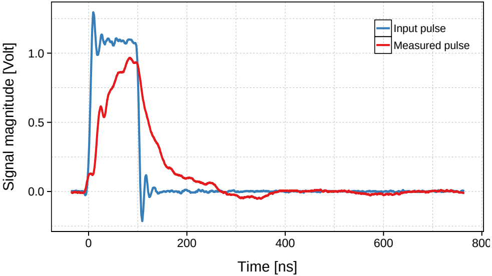
Control Computer

Arbitrary waveform generator

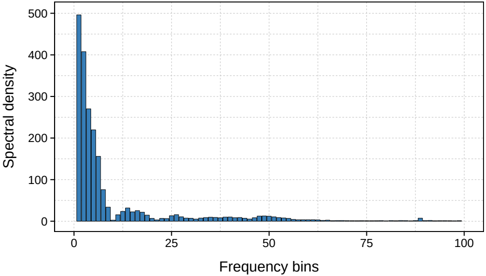
Oscilloscope

Brass hand-electrodes

Signals

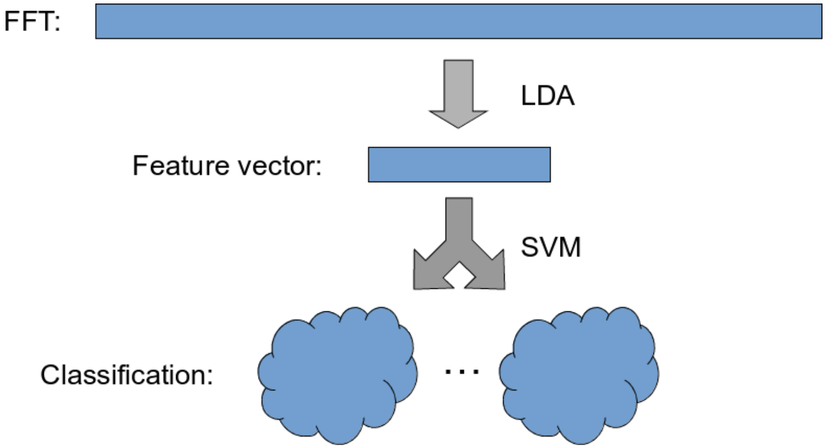


Input pulse
Measured pulse
Signal magnitude [Volt]
1.0
0.5
0.0
0
200
400
600
800
Time [ns]



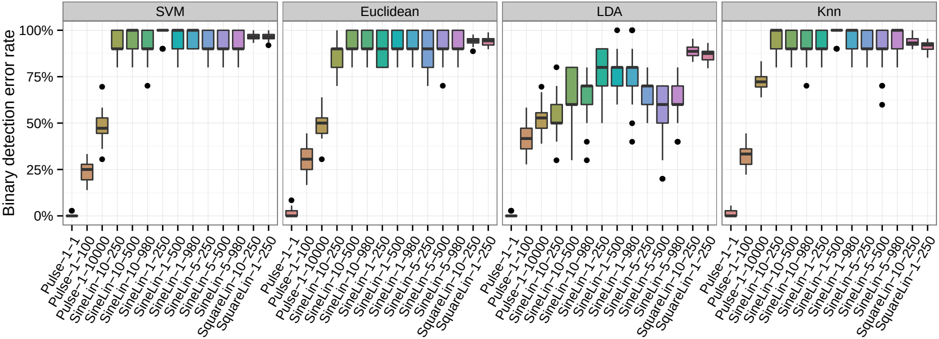
Spectral density
500
400
300
200
100
0
0
25
50
75
100
Frequency bins

Classification

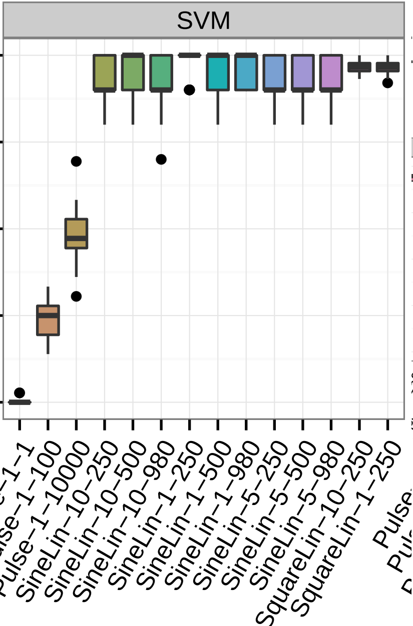


Selecting the Classifier

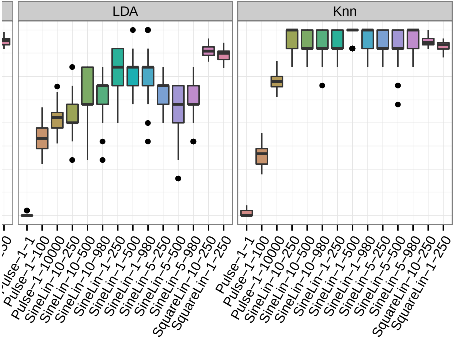
Support Vector Machine, Euclidean Distance, Latent Dirichlet Allocation, K-Nearest Neighbor



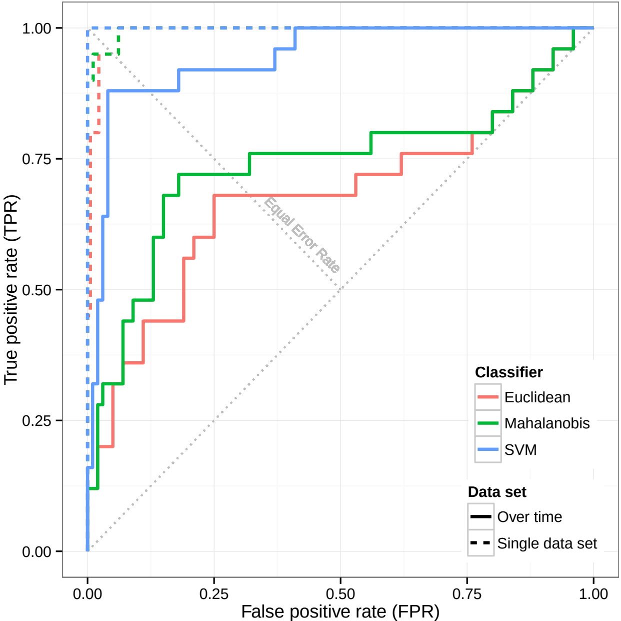
Selecting the Classifier



uclidean Distance,
K-Nearest Neighbor



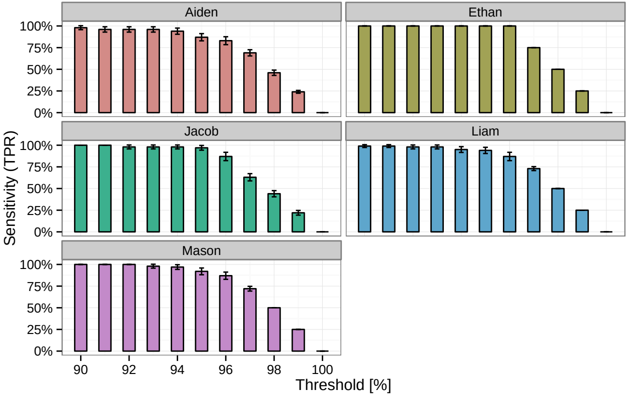
ROC Curves


1.00
0.75
0.50
0.25
0.00
True positive rate (TPR)
0.00
0.25
0.50
0.75
1.00
False positive rate (FPR)
Equal Error Rate
Classifier
Euclidean
Mahalanobis
SVM
Data set
Over time
Single data set

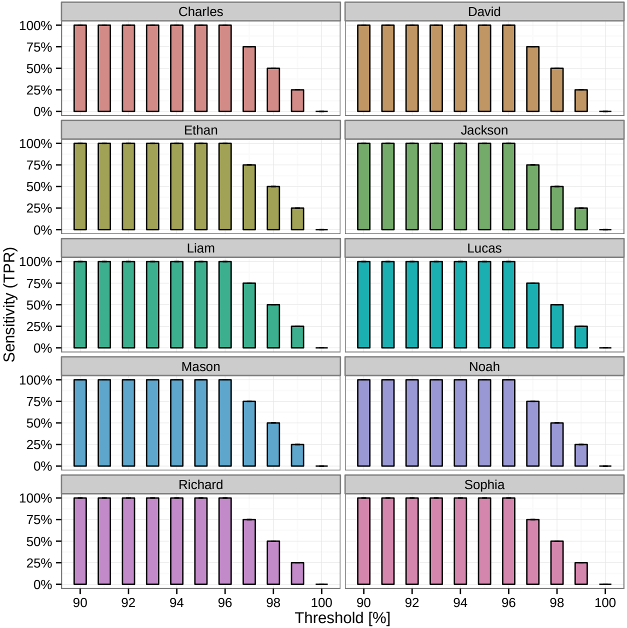
Authentication Classifier

UNIVERSITY OF OXFORD

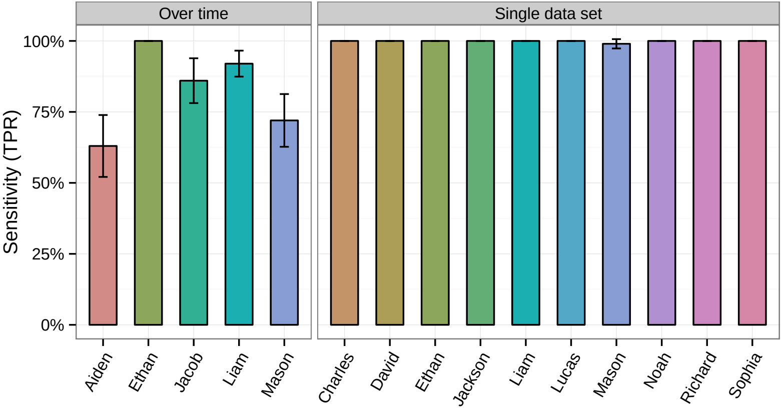
Over Time



Auth: Single Session



Identification Classifier



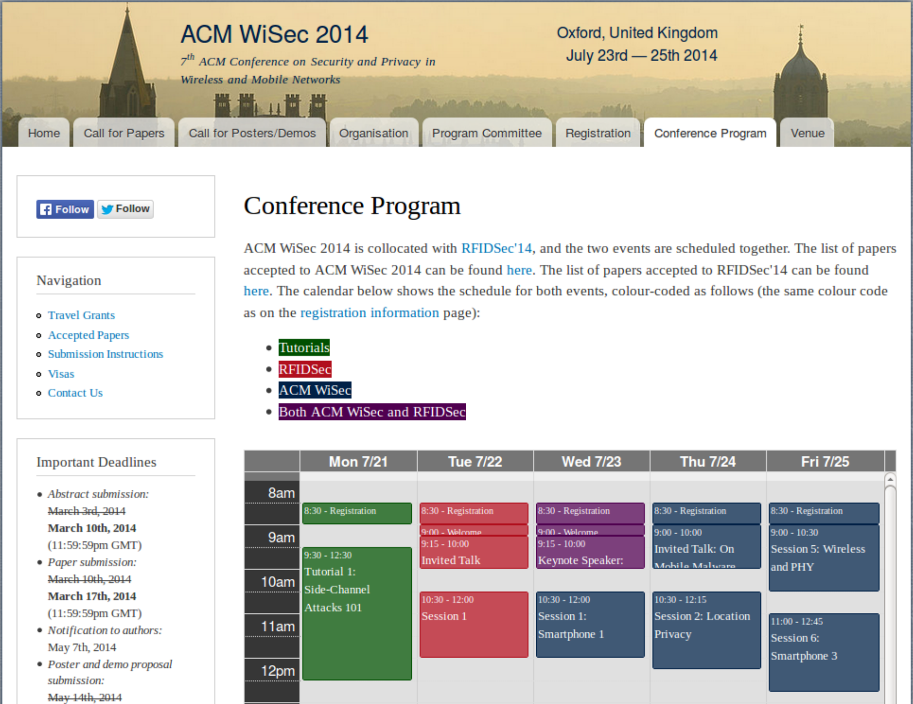
Future Work

Prototype

- Build PIN entry prototype.
- Gather experience on acquisition time, etc.
- Gather more data.

Acquisition Signal

- Higher bandwidth
- No signal
- Effects of stress, blood sugar levels, etc.
- Assess impersonation strategies.



ACM WiSec 2014

7th ACM Conference on Security and Privacy in Wireless and Mobile Networks

Oxford, United Kingdom
July 23rd — 25th 2014

Navigation

- Travel Grants
- Accepted Papers
- Submission Instructions
- Visas
- Contact Us

Important Deadlines

- *Abstract submission:* ~~March 3rd, 2014~~ **March 10th, 2014** (11:59:59pm GMT)
- *Paper submission:* ~~March 10th, 2014~~ **March 17th, 2014** (11:59:59pm GMT)
- *Notification to authors:* May 7th, 2014
- *Poster and demo proposal submission:* ~~May 14th, 2014~~

Conference Program

ACM WiSec 2014 is collocated with RFIDSec'14, and the two events are scheduled together. The list of papers accepted to ACM WiSec 2014 can be found here. The list of papers accepted to RFIDSec'14 can be found here. The calendar below shows the schedule for both events, colour-coded as follows (the same colour code as on the registration information page):

- Tutorials
- RFIDSec
- ACM WiSec
- Both ACM WiSec and RFIDSec

	Mon 7/21	Tue 7/22	Wed 7/23	Thu 7/24	Fri 7/25
8am	8:30 - Registration	8:30 - Registration	8:30 - Registration	8:30 - Registration	8:30 - Registration
9am	9:30 - 12:30 Tutorial 1: Side-Channel Attacks 101	9:00 - Welcome 9:15 - 10:00 Invited Talk	9:00 - Welcome 9:15 - 10:00 Keynote Speaker:	9:00 - 10:00 Invited Talk: On Mobile Malware	9:00 - 10:30 Session 5: Wireless and PHY
10am		10:30 - 12:00 Session 1	10:30 - 12:00 Session 1: Smartphone 1	10:30 - 12:15 Session 2: Location Privacy	
11am					11:00 - 12:45 Session 6: Smartphone 3
12pm					

Conclusion

- A new biometric based on Pulse-Response.
- Two simple application scenarios for Pulse-Response integration.
- Very promising results. Very high degree of uniqueness and good stability over time.

Conclusion – Questions?

- A new biometric based on Pulse-Response.
- Two simple application scenarios for Pulse-Response integration.
- Very promising results. Very high degree of uniqueness and good stability over time.

Thank you for your attention.
Questions?
`kasper.rasmussen@cs.ox.ac.uk`