Hold & Sign: A Novel Behavioral Biometrics for Smartphone User Authentication

Attaullah Buriro[1], Bruno Crispo[2], Filippo Del Frari[1]
Konrad Wrona[3]

[1]University of Trento

[2]DistriNet - KULeuven

[3]NCIA - NATO

{attaullah.buriro, filippo.delfrari}@unitn.it
bruno.crispo@cs.kuleuven.be

November 15, 2017

NATO Communications and Information Agency
Agence OTAN d'information et de communication

KU LEUVEN

UNIVERSITY OF TRENTO - Italy

Handwritten Biometric Recognition

- Process of identifying the author of a given text.
  - Handwritten signature is a specific instance.

Barack Obama

Handwritten Biometric Recognition

- Process of identifying the author of a given text.
  - Handwritten signature is a specific instance.
- **Wide social and legal acceptance in daily life.**
  - Witness intentions (signing a contract)
  - indicate physical presence (signing in for work)

Barack Obama

Handwritten Biometric Recognition

- In static systems, scanned image is processed and compared with the stored image to authenticate.

[1] http://www.sutisoft.com/sutisign/

Handwritten Biometric Recognition

- In static systems, scanned image is processed and compared with the stored image to authenticate.
- **In dynamic/online systems, signature is acquired (by stylus or pen) and processed in real time and extracted global features are compared to authenticate.**

[1] http://www.sutisoft.com/sutisign/

Handwritten Biometric Recognition

- In static systems, scanned image is processed and compared with the stored image to authenticate.
- In dynamic/online systems, signature is acquired (by stylus or pen) and processed in real time and extracted global features are compared to authenticate.
  - **spatial coordinates x(t)**
  - **spatial coordinates x(t)**
  - **pressure p(t)**
  - **inclination angles in(t), etc.**

[1] http://www.sutisoft.com/sutisign/

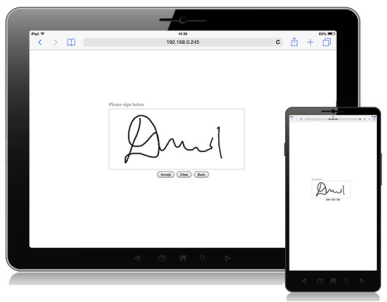
Handwritten Biometric Recognition

- In static systems, scanned image is processed and compared with the stored image to authenticate.
- In dynamic/online systems, signature is acquired (by stylus or pen) and processed in real time and extracted global features are compared to authenticate.
  - spatial coordinates x(t)
  - spatial coordinates x(t)
  - pressure p(t)
  - inclination angles in(t), etc.

[1] http://www.sutisoft.com/sutisign/

Handwritten Biometric Recognition

- In static systems, scanned image is processed and compared with the stored image to authenticate.
- In dynamic/online systems, signature is acquired (by stylus or pen) and processed in real time and extracted global features are compared to authenticate.
  - spatial coordinates x(t)
  - spatial coordinates x(t)
  - pressure p(t)
  - inclination angles in(t), etc.



- **iSignOn, SignEasy and eSignature (sutisoft[1]) use signature image to authenticate.**

[1] http://www.sutisoft.com/sutisign/

Design Requirements

- Must be able to run on the smartphones

[2] De Luca, Alexander, et al. "I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones." Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2015.

Design Requirements

- Must be able to run on the smartphones
- **Usability is very important for user acceptance**
  - **Must be quick**
  - **easy to use**
  - **"I Feel Like I'm Taking Selfies All Day!"**
  - **"It can be a bit embarrassing to hold your phone up in a weird position while in public just to unlock it!"**[2]

[2] De Luca, Alexander, et al. "I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones." Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2015.

Design Requirements

- Must be able to run on the smartphones
- Usability is very important for user acceptance
  - Must be quick
  - easy to use
  - "I Feel Like I'm Taking Selfies All Day!"
  - "It can be a bit embarrassing to hold your phone up in a weird position while in public just to unlock it!"[2]
- **Must be secure, i.e., should provide acceptable security.**

[2] De Luca, Alexander, et al. "I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones." Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2015.

Our Proposed Solution

Hold & Sign

Hold & Sign

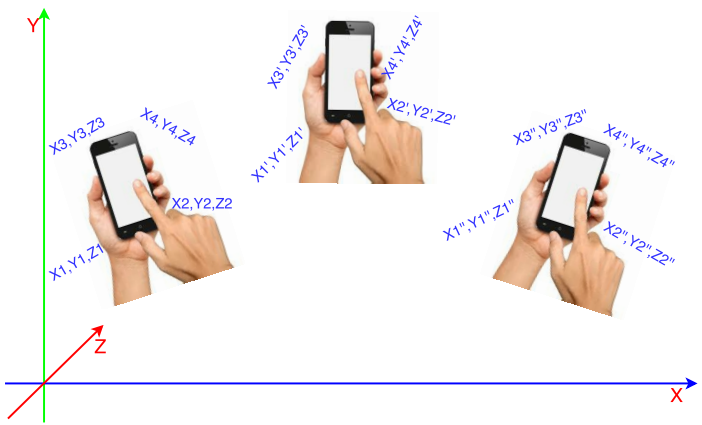
- Bi-Modal System

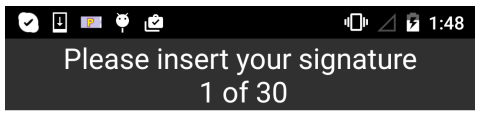
Hold & Sign

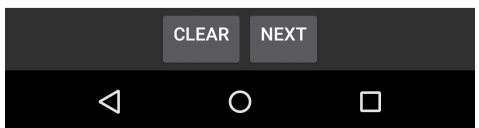
- Bi-Modal System
  - **Sign - touch (points pressed while signing)**

Hold & Sign

- Bi-Modal System
  - Sign - touch (points pressed while signing)
  - **Hold - phone's micro-movements while signing**

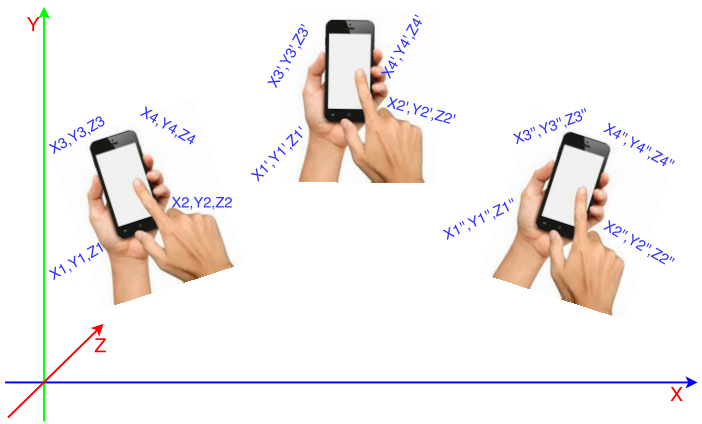


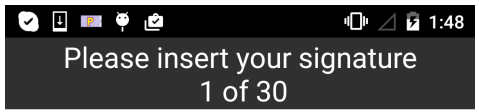


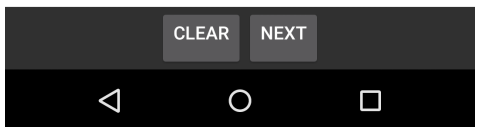


Hold & Sign

- Bi-Modal System
  - Sign - touch (points pressed while signing)
  - Hold - phone's micro-movements while signing
- **No additional hardware required.**

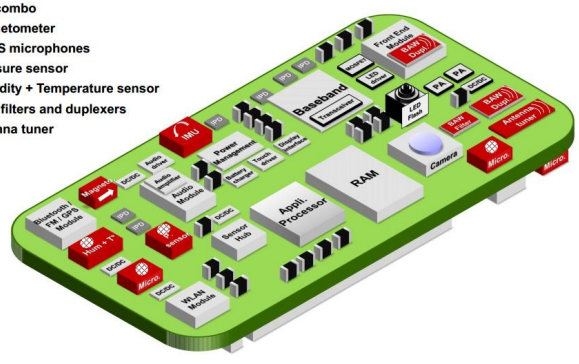






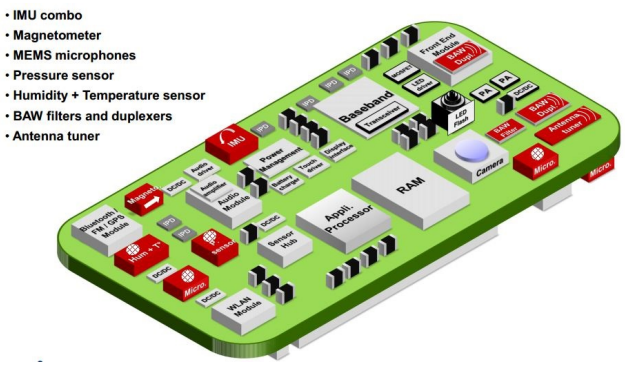
Smartphone Sensors

- IMU combo
- Magnetometer
- MEMS microphones
- Pressure sensor
- Humidity + Temperature sensor
- BAW filters and duplexers
- Antenna tuner



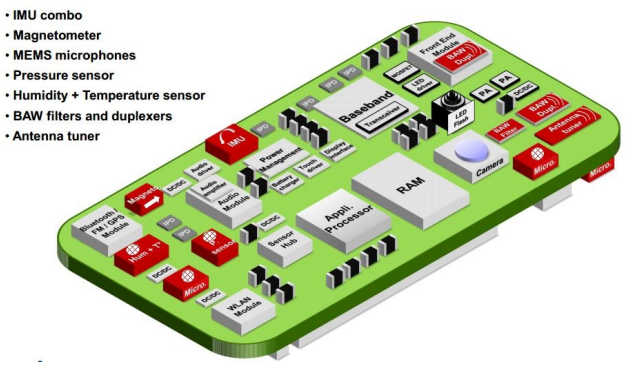
Smartphone Sensors

- Accelerometer - 3 variants, i.e., RAW, LPF and HPF
  - **accelerations in** 3 **dimensions**
- **Gravity**
  - **gravity forces in** 3 **dimensions**
- Magnetometer
  - Strength and direction of magnetic field in 3 dimensions
- Touchscreen
- Hold & Sign utilizes the existing hardware



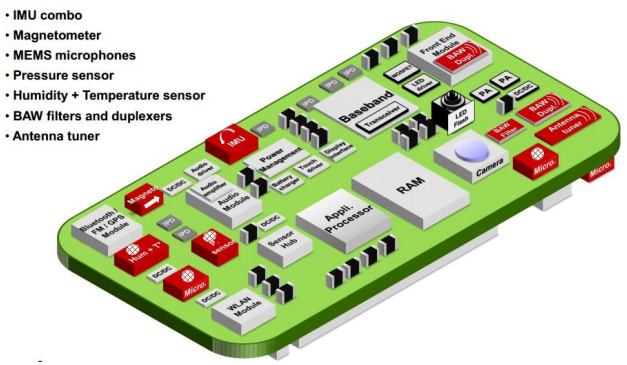
Smartphone Sensors

- Accelerometer - 3 variants, i.e., RAW, LPF and HPF
  - accelerations in 3 dimensions
- Gravity
  - gravity forces in 3 dimensions
- **Magnetometer**
  - **Strength and direction of magnetic field in 3 dimensions**
- Touchscreen
- Hold & Sign utilizes the existing hardware



Smartphone Sensors

- Accelerometer - 3 variants, i.e., RAW, LPF and HPF
  - accelerations in 3 dimensions
- Gravity
  - gravity forces in 3 dimensions
- Magnetometer
  - Strength and direction of magnetic field in 3 dimensions
- **Touchscreen**
- **Hold & Sign utilizes the existing hardware**



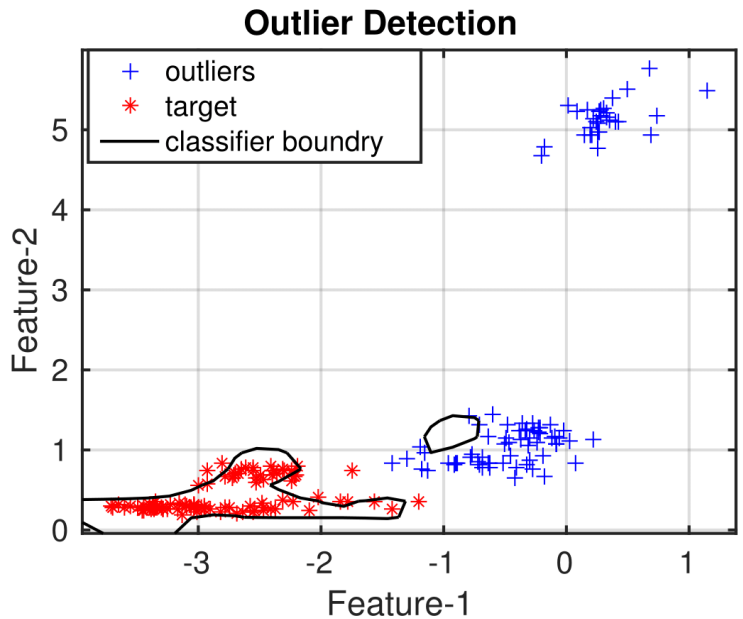
Validation

- Data Collection
  - 30 samples in each activity (total 90)
  - 3 activities (sitting, standing, walking)

- 30 **participants (22 male), all of them Masters/PhD students, Google Nexus** 5

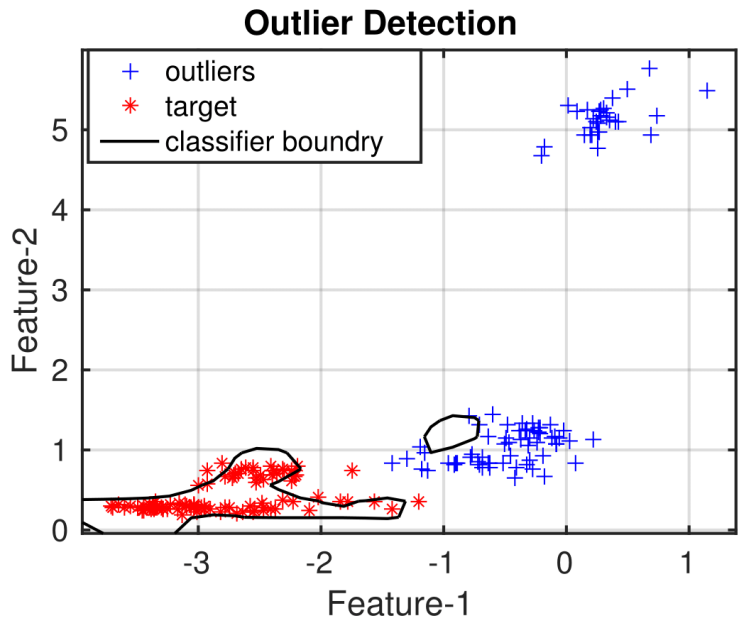
One Class Classification (Anomaly Detection)

- **Verifiers**
  - We used a set of four conceptually different verifiers.
    - 3-NN (K-Nearest Neighbor)
    - 3-layer MLP (Multilayer Perceptron)
    - BayesNet
    - Random Forest



One Class Classification (Anomaly Detection)

- Verifiers
  - We used a set of four conceptually different verifiers.
    - 3-NN (K-Nearest Neighbor)
    - 3-layer MLP (Multilayer Perceptron)
    - BayesNet
    - Random Forest



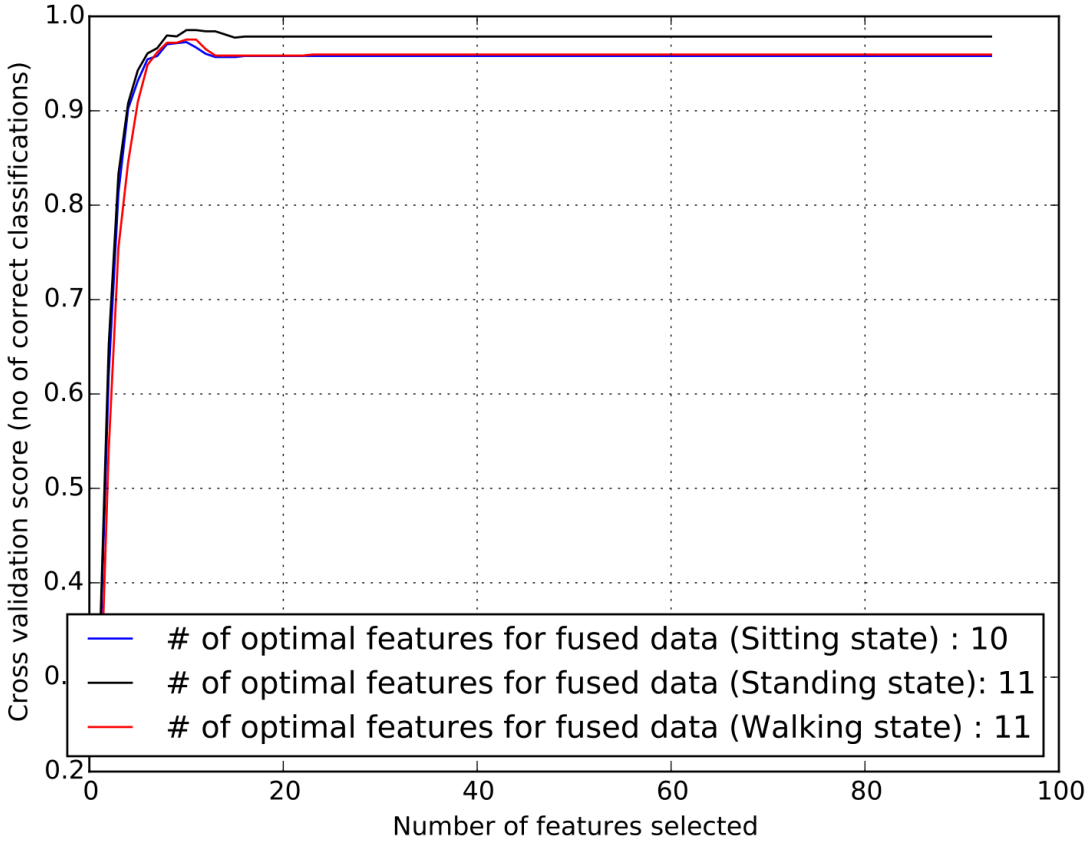
- **After initial experiments we selected MLP since it performed consistently across situations(TAR=79% , FAR=0.1%)**

Feature Selection

- 93 features (80 hold and 13 sign)

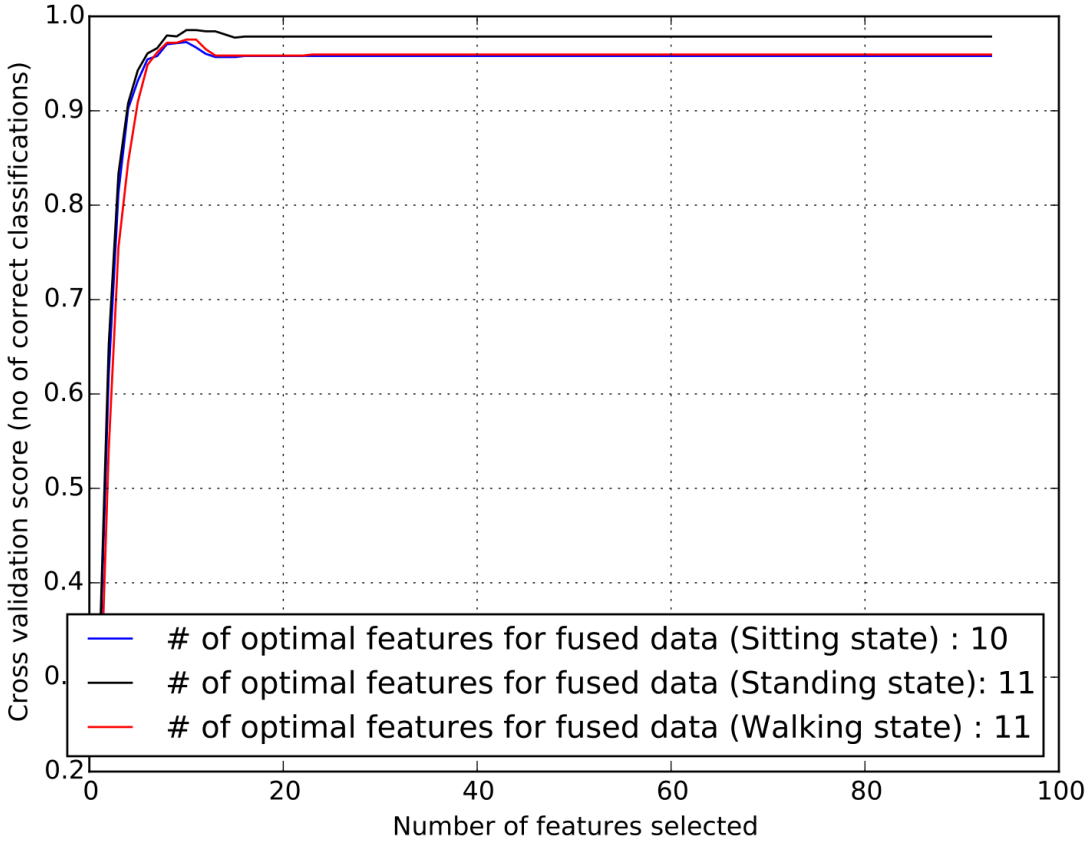
Feature Selection

- 93 features (80 hold and 13 sign)
- **Recursive Feature Elimination (RFE) Method**



Feature Selection

- 93 features (80 hold and 13 sign)
- Recursive Feature Elimination (RFE) Method
  - **Scikit-learn,** 10**-fold cross validation**

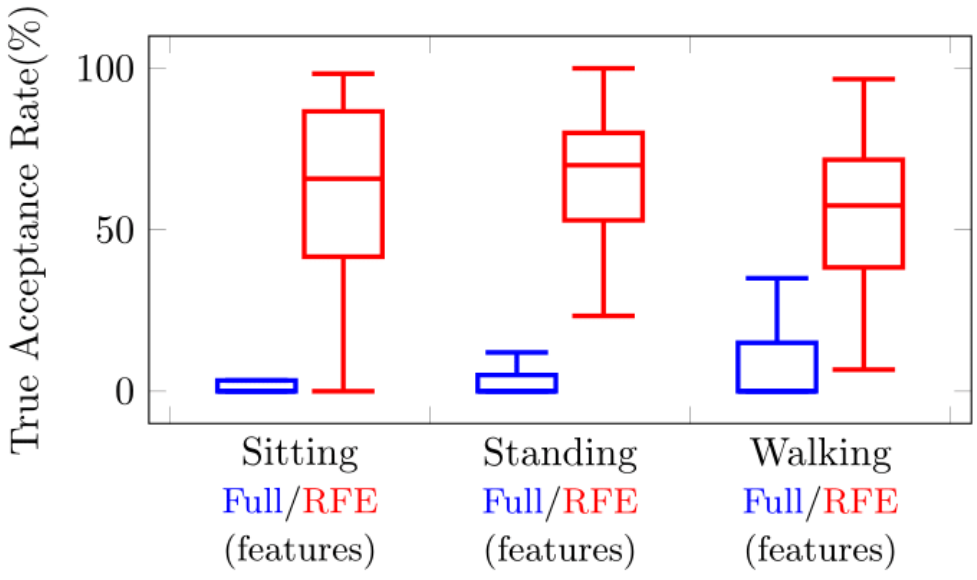


Results

- The results are averaged over 30 users

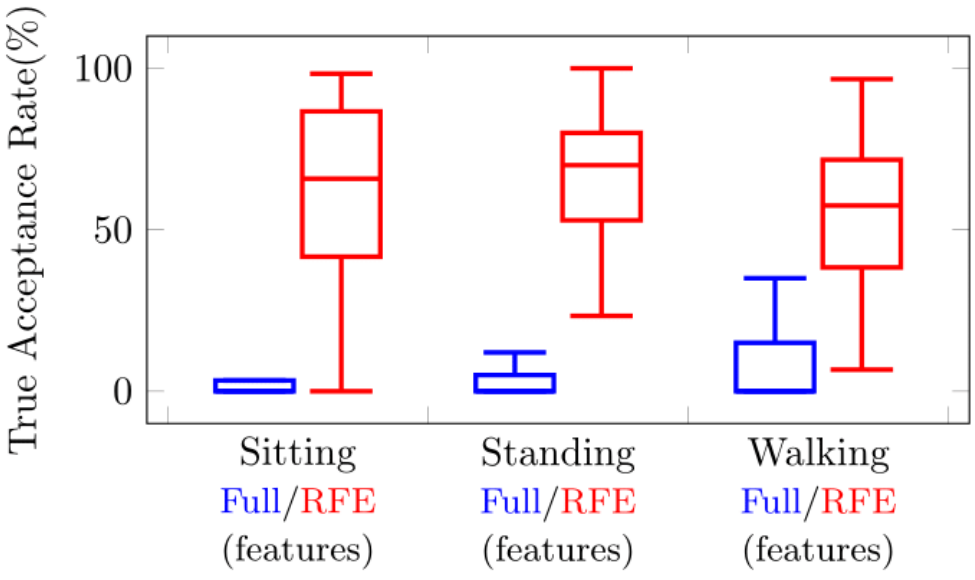
Results

- The results are averaged over 30 users
  - **Inter-Activity**



Results

- The results are averaged over 30 users
  - Inter-Activity



  - **Combined-Activities (RFE)**

Classifier	*TAR(%)*	*FRR (%)*	*FAR (%)*	*TRR(%)*
MLP	94.8	5.2	3.1	96.9

Performance

- Sample Acquisition Time

Method	Sample Acquisition Time(s)
Hold & Sign	3.5
PIN	3.7
Voice	5.15
Face	5.55
Password	7.46
Face + Voice	7.63
Gesture	8.10
Gesture + Voice	9.91

S. Trewin, et. al, Biometric authentication on a mobile device: a study of user effort, error and task disruption, 28th ACM ACSAC, 2012, pp. 159168.

Performance

- Testing Time

Scheme	*Device*	*Classifiers*	*# Users*	*Testing Time (s)*
Hold & Sign	Nexus 5	MLP	30	0.215 – 0.250
Lee & Lee[3]	Nexus 5	SVM	8	20
Li et al[4].	Motorolla Droid	Sliding patterns	75	0.648
Nickel et al[5].	Motorolla Milestoon	KNN	36	30

[3] W.-H. Lee and R. B. Lee, Multi-sensor authentication to improve smartphone security, in International Conference on Information Systems Security and Privacy, 2015.

[4] Li, X. Zhao, and G. Xue, Unobservable re-authentication for smartphones. in NDSS, 2013.

[5] C. Nickel, T. Wirtl, and C. Busch, Authentication of smartphone users based on the way they walk using k-nn algorithm, in 8th IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012

Performance

- Power Consumption

[6] Sitova et al. "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users." IEEE Transactions on Information Forensics and Security 11.5 (2016): 877-892.

[7] https://play.google.com/store/apps/details?id=com.quicinc.trepn

[8] https://developer.qualcomm.com/blog/mobile-apps-and-power-consumption-basics-part-1

Performance

- Power Consumption
  - **In order to check the overhead resulting from use of the application (in different steps), we terminated all the running applications and all Google services, switched off WiFi, Bluetooth, and cellular radios. The screen was kept running for the entire duration of the experiment with brightness at the lowest level and automatic brightness adjustment disabled[6]. We used Trepn[7]to profile power usage.**

---

[6] Sitova et al. "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users." IEEE Transactions on Information Forensics and Security 11.5 (2016): 877-892.

[7] https://play.google.com/store/apps/details?id=com.quicinc.trepn

[8] https://developer.qualcomm.com/blog/mobile-apps-and-power-consumption-basics-part-1

Performance

- Power Consumption
  - In order to check the overhead resulting from use of the application (in different steps), we terminated all the running applications and all Google services, switched off WiFi, Bluetooth, and cellular radios. The screen was kept running for the entire duration of the experiment with brightness at the lowest level and automatic brightness adjustment disabled[6]. We used Trepn[7]to profile power usage.
  - **our app consumes $\approx$1000mW (for 35 attempts) all in the stages of decision making (less than the power consumed in one-minute of phone call($\approx$1054mW[8]) during all the stages.**

---

[6]Sitova et al. "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users." IEEE Transactions on Information Forensics and Security 11.5 (2016): 877-892.

[7]https://play.google.com/store/apps/details?id=com.quicinc.trepn

[8]https://developer.qualcomm.com/blog/mobile-apps-and-power-consumption-basics-part-1

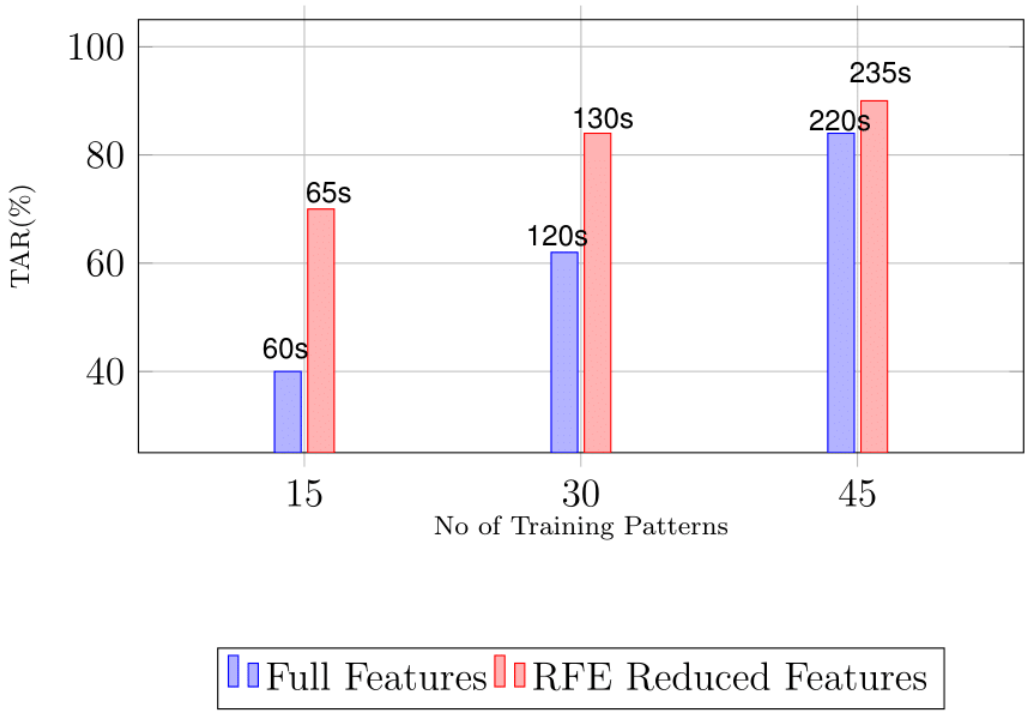
Usability

- Trade-off between training & accuracy.

[9] https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

Usability

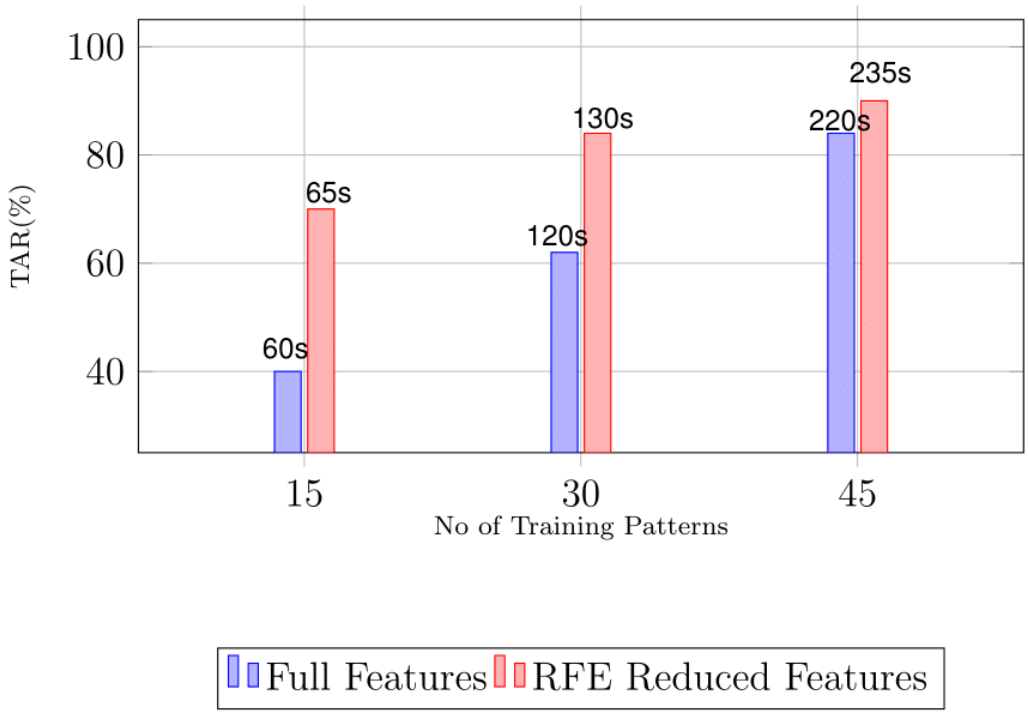
- Trade-off between training & accuracy.



[9] https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

Usability

- Trade-off between training & accuracy.



- **System Usability Scale (SUS[9]) Evaluation** - 68.3% (72% **or higher is considered good.)**

[9] https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

Hold & Sign in Action

- This one-minute video shows the working of Hold & Sign.

Open Issues

- **Extend number of testers and run tests on the field.**

Open Issues

- Extend number of testers and run tests on the field.
- **Reduce training time without compromising (too much) security**

Open Issues

- Extend number of testers and run tests on the field.
- Reduce training time without compromising (too much) security
- **Unplanned Situations**

Open Issues

- Extend number of testers and run tests on the field.
- Reduce training time without compromising (too much) security
- Unplanned Situations
- **Assess its robustness to multiple attacks.**

Open Issues

- Extend number of testers and run tests on the field.
- Reduce training time without compromising (too much) security
- Unplanned Situations
- Assess its robustness to multiple attacks.
- **Variability depending on OS (iOS) and on HW (different phones, sensors)**

Thank You!

- attaullah.buriro@unitn.it
- bruno.crispo@cs.kuleuven.be