Mobile Biometrics: Towards A Comprehensive Evaluation Methodology

Attaullah Buriro[1], Zahid Akhtar[3], Bruno Crispo[1,2], Sandeep Gupta[1]

[1]DISI University of Trento, Italy

[2]DistriNet - KULeuven, Belgium

[3]INRS-EMT, University of Quebec, Montreal, Canada

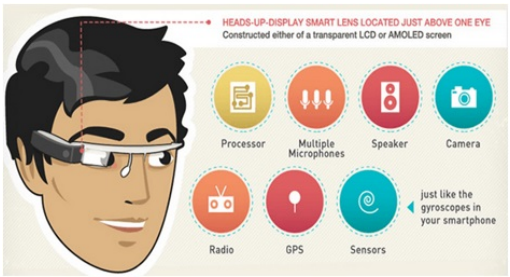
{attaullah.buriro, sandeep.gupta, bruno.crispo}@unitn.it
bruno.crispo@cs.kuleuven.be
zahid.akhtar.momin@emt.inrs.ca,

October 26, 2017

Outline

- **Motivation**
- **Problem statement**
- **Guidelines/Recommendations**
- **Conclusion**

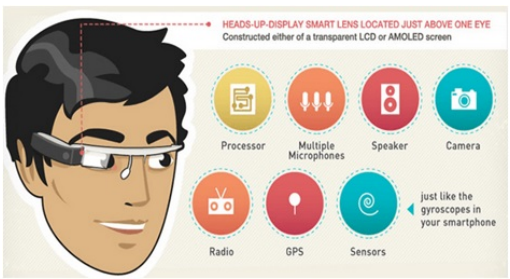
New Generation Devices



[1] https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2015/cmr-uk-2015

[2] https://www.extremetech.com/computing/226867-comscore-computer-usage-falls-as-20-of-millennials-go-mobile-only.

New Generation Devices

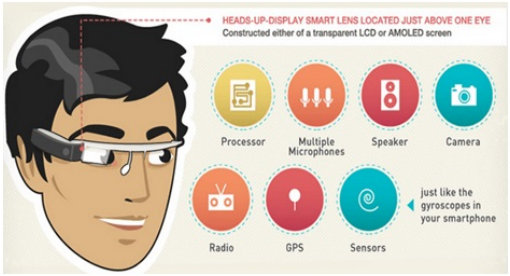


- **The UK is now a smartphone society**[1]

[1] https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2015/cmr-uk-2015

[2] https://www.extremetech.com/computing/226867-comscore-computer-usage-falls-as-20-of-millennials-go-mobile-only.

New Generation Devices



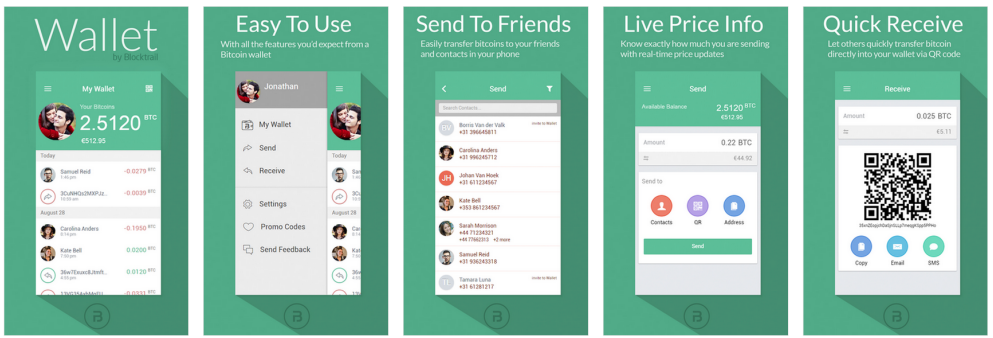
- The UK is now a smartphone society[1]
- **Computer usage falls as 20% of millennials go mobile-only[2]**

[1] https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2015/cmr-uk-2015

[2] https://www.extremetech.com/computing/226867-comscore-computer-usage-falls-as-20-of-millennials-go-mobile-only.

New generation devices: personal, connected and powerful!

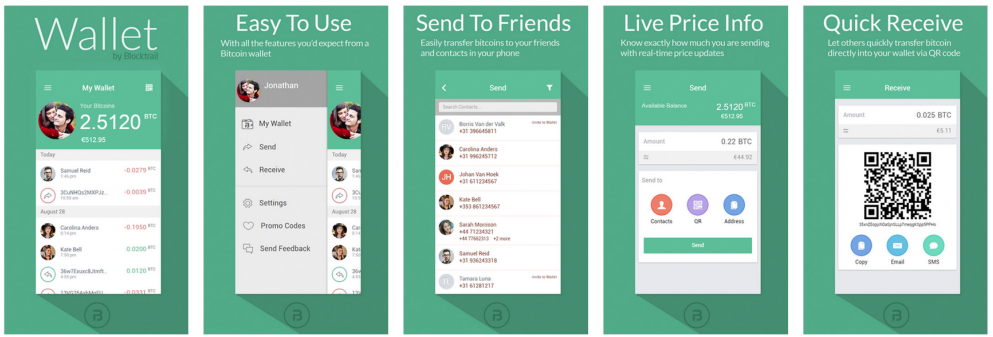
- **Beyond classical communication**
  - **Taking pictures & making movies and sharing with others**
  - **Social Networking**
    - **Facebook, Viber, whatsApp, Skype, Twitter, etc.**
  - **Online Transactions**
    - **Google Wallet, Paypal, XOOM, etc.**



- **They continuously track the user location and have full control over user's emails**

New generation devices: personal, connected and powerful!

- Beyond classical communication
  - Taking pictures & making movies and sharing with others
  - Social Networking
    - Facebook, Viber, whatsApp, Skype, Twitter, etc.
  - Online Transactions
    - Google Wallet, Paypal, XOOM, etc.



- They continuously track the user location and have full control over user's emails
- **All of these apps generate and store very personal user information which needs to be protected**

Authentication

- **What is Authentication?**
  - **Being able to prove a user is who she claims to be**

Authentication

- *What is Authentication?*
  - *Being able to prove a user is who she claims to be*
- **Authentication was introduced for**

Authentication

- *What is Authentication?*
  - *Being able to prove a user is who she claims to be*
- Authentication was introduced for
  - **Protecting long term sessions**
  - **One-shot - TOCTOU problem**
  - **Binary decision**

Authentication

- *What is Authentication?*
  - *Being able to prove a user is who she claims to be*
- Authentication was introduced for
  - Protecting long term sessions
  - One-shot - TOCTOU problem
  - Binary decision
- **Authentication is required for**

Authentication

- *What is Authentication?*
  - *Being able to prove a user is who she claims to be*
- Authentication was introduced for
  - Protecting long term sessions
  - One-shot - TOCTOU problem
  - Binary decision
- Authentication is required for
  - **Long, short & frequent sessions**
  - **Repeatable (as and when required)**
  - **Risk-based and adaptive**
  - **Continuous**

Usage pattern shift

- **Usability study show that users interact with their smartphones every 6.5 minutes (in 24 h).**

Usage pattern shift

- Usability study show that users interact with their smartphones every 6.5 minutes (in 24 h).
- **Passwords, PINs and physical biometrics do not fit the current interaction model for newer devices.**

Usage pattern shift

- Usability study show that users interact with their smartphones every 6.5 minutes (in 24 h).
- Passwords, PINs and physical biometrics do not fit the current interaction model for newer devices.
- **Research has been diverted to design new acceptable & secure metaphors for user authentication.**

Usage pattern shift

- Usability study show that users interact with their smartphones every 6.5 minutes (in 24 h).
- Passwords, PINs and physical biometrics do not fit the current interaction model for newer devices.
- Research has been diverted to design new acceptable & secure metaphors for user authentication.
- **Evaluation is mainly based on security (under zero-effort) not on the other operational issues, i.e., usability, robustness against attacks, and computational overhead.**

Usage pattern shift

- Usability study show that users interact with their smartphones every 6.5 minutes (in 24 h).
- Passwords, PINs and physical biometrics do not fit the current interaction model for newer devices.
- Research has been diverted to design new acceptable & secure metaphors for user authentication.
- Evaluation is mainly based on security (under zero-effort) not on the other operational issues, i.e., usability, robustness against attacks, and computational overhead.
- **We present a set of guidelines for designing, implementation, and evaluating newer user authentication methods for a positive impact on future technological developments.**

Guidelines!

Data Collection Protocol

- **Higher number of users (preferably from diverse background) and samples are always better.**

Data Collection Protocol

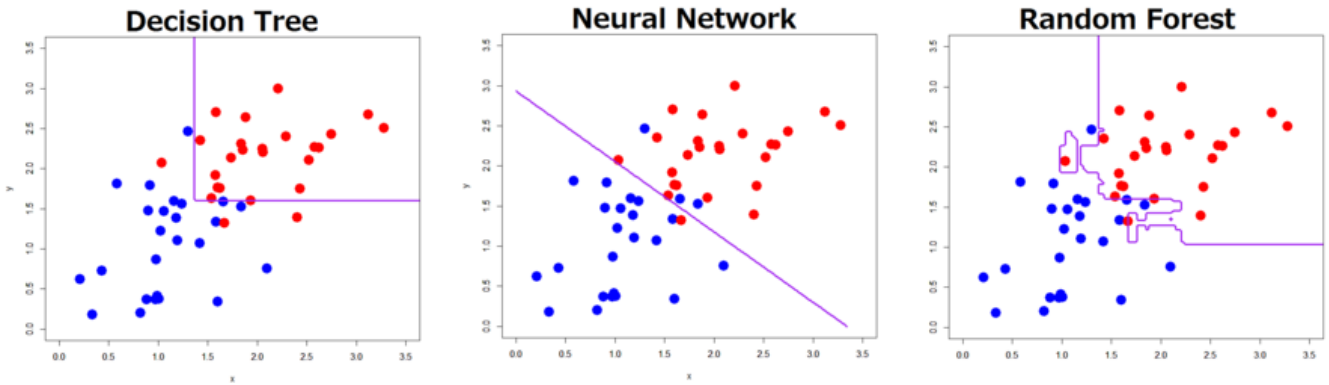
- Higher number of users (preferably from diverse background) and samples are always better.
- **Data should be collected anonymously or their data privacy should be ensured.**

Data Collection Protocol

- Higher number of users (preferably from diverse background) and samples are always better.
- Data should be collected anonymously or their data privacy should be ensured.
- **We recommend to collect data in a natural way, i.e., data should be collected in multiple sessions so that the participant should not be able to memorize the behavior.**

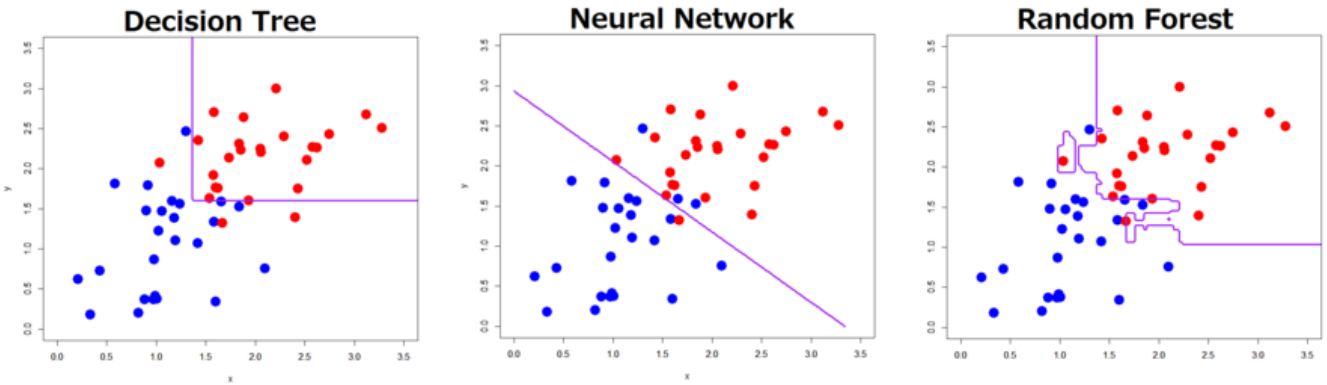
Classification Protocol

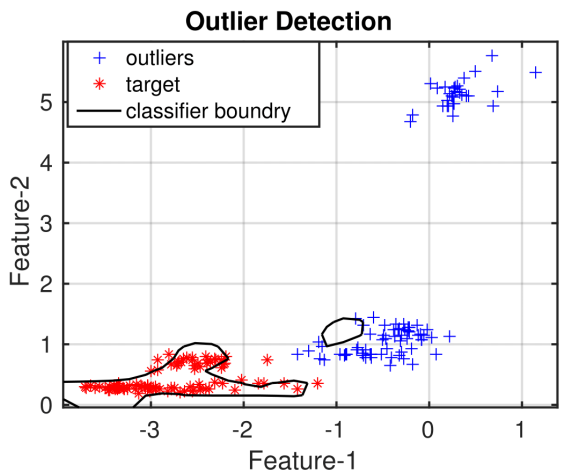
- **The mobile user authentication problem essentially is a one-class classification problem, it is thus unreasonable to formulate mobile user authentication as the binary class classification problem.**



Classification Protocol

- The mobile user authentication problem essentially is a one-class classification problem, it is thus unreasonable to formulate mobile user authentication as the binary class classification problem.



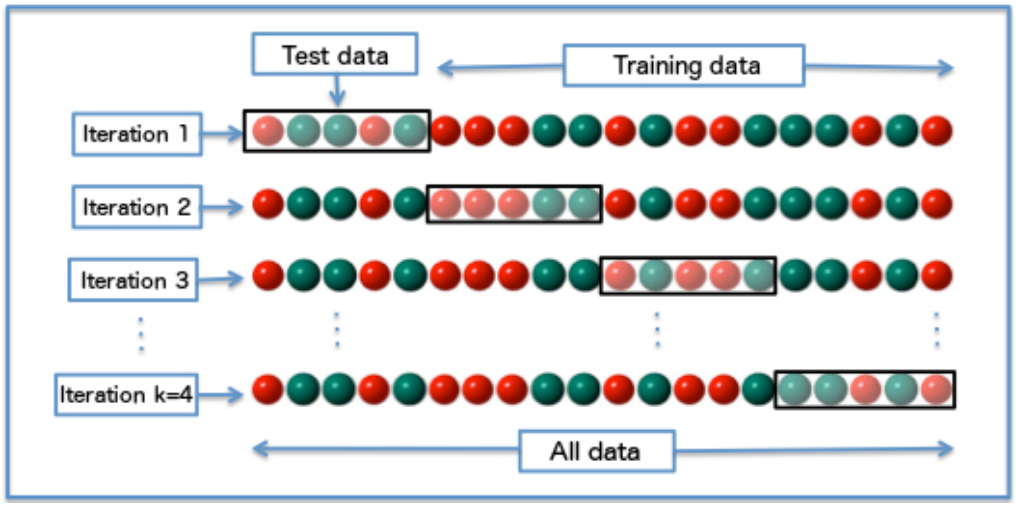


Cross-validation / Training-testing Protocol

- **We consider classifier training with initial set of observations, e.g., first 5 or 10, more realistic as compared to using a large fraction for the classifier training.**

Cross-validation / Training-testing Protocol

- We consider classifier training with initial set of observations, e.g., first 5 or 10, more realistic as compared to using a large fraction for the classifier training.

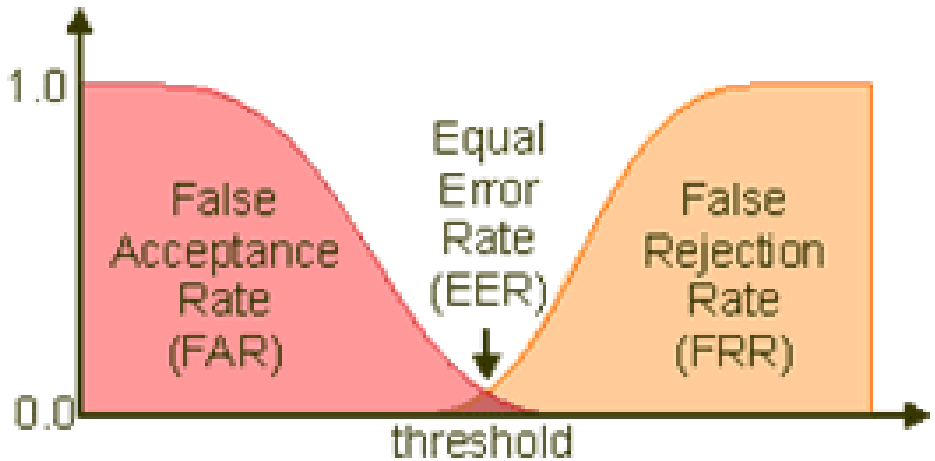


Success Metric

- **New mechanisms are normally evaluated in terms of False Reject Rate (FRR), False Acceptance Rate (FAR), Equal Error Rate (EER).**

Success Metric

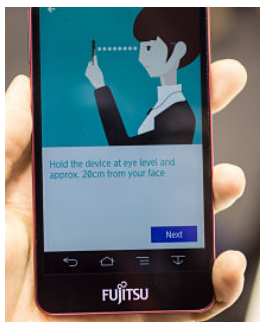
- New mechanisms are normally evaluated in terms of False Reject Rate (FRR), False Acceptance Rate (FAR), Equal Error Rate (EER).
- **Failure to Acquire Rate (FTAR)**
- **Failure to Enroll Rate (FTER)**



Usability Study

1. **Sample Acquisition Time**
   - **Biometric researchers should minimize the required sample acquisition time in order to increase the acceptability of their proposed scheme.**

Figure: Time Consuming (15-20s)[3]

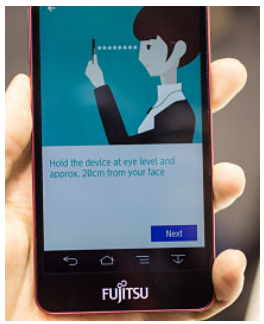


[3] http://www.ibtimes.co.uk/unlocking-phone-your-eyes-fujitsu-iris-recognition-tech-coming-smartphones-2015-1490297

Usability Study

1. Sample Acquisition Time
   - Biometric researchers should minimize the required sample acquisition time in order to increase the acceptability of their proposed scheme.
2. **Classifier's Training/Testing Times**
   - **Larger testing time could end up in annoying the user and won't get the wide user acceptability.**

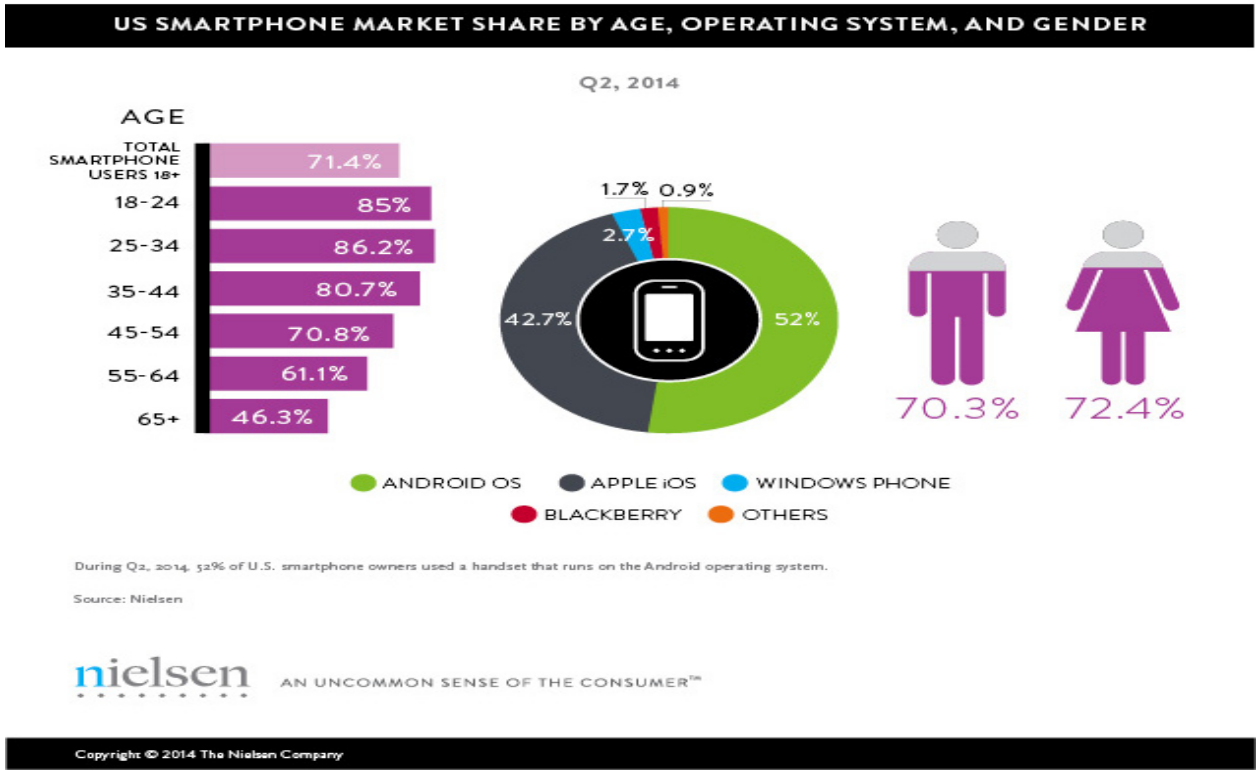
Figure: Time Consuming (15-20s)[3]



[3] http://www.ibtimes.co.uk/unlocking-phone-your-eyes-fujitsu-iris-recognition-tech-coming-smartphones-2015-1490297

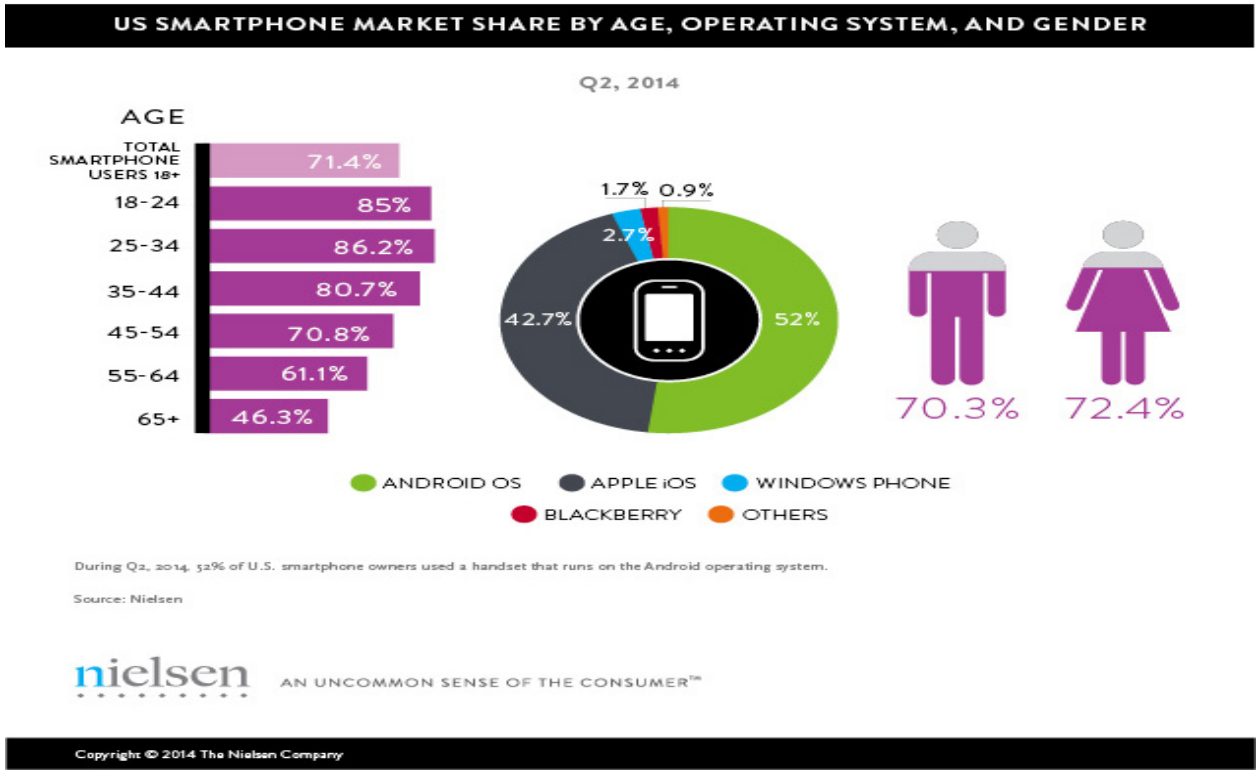
Usability Study (2)

1. **Applicability to all users of all age-groups**



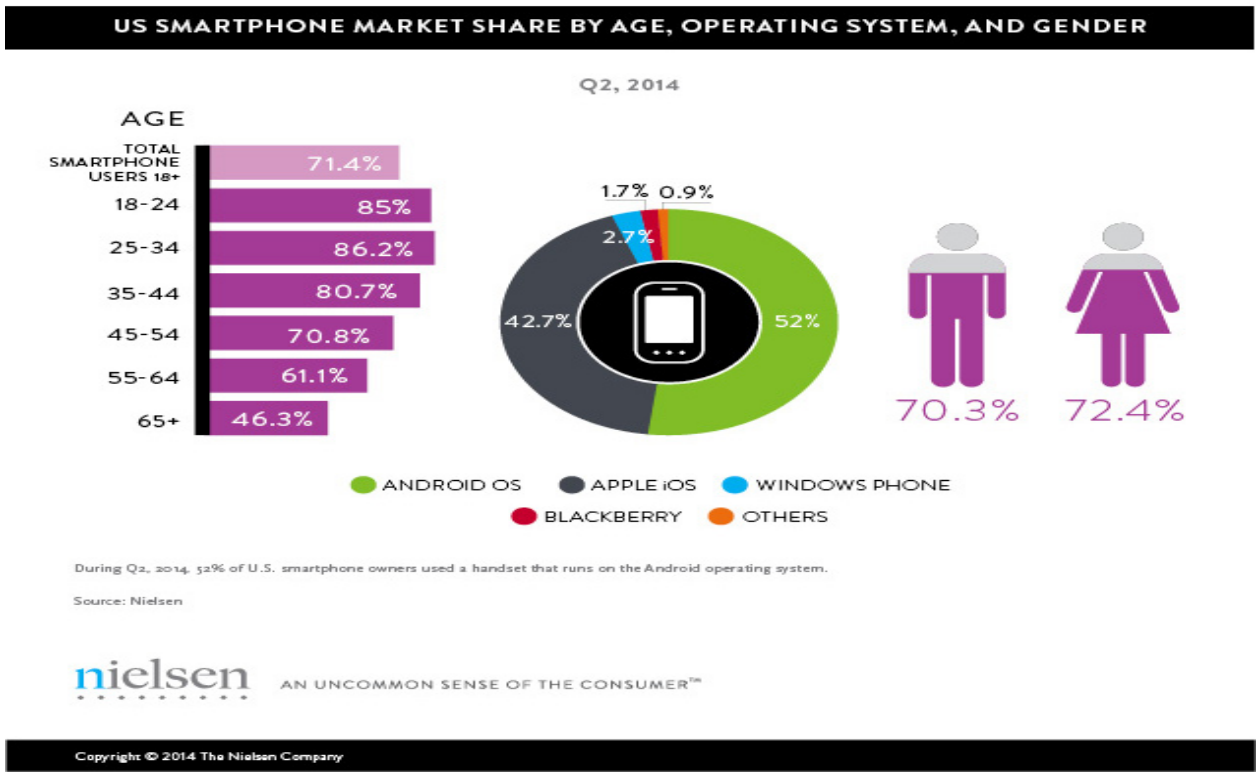
Usability Study (2)

1. Applicability to all users of all age-groups
2. **Applicability in different situations**



Usability Study (2)

1. Applicability to all users of all age-groups
2. Applicability in different situations
   - **The newly proposed authentication scheme needs to be evaluated in multiple common activities in order to obtain a clear picture of their final accuracy.**

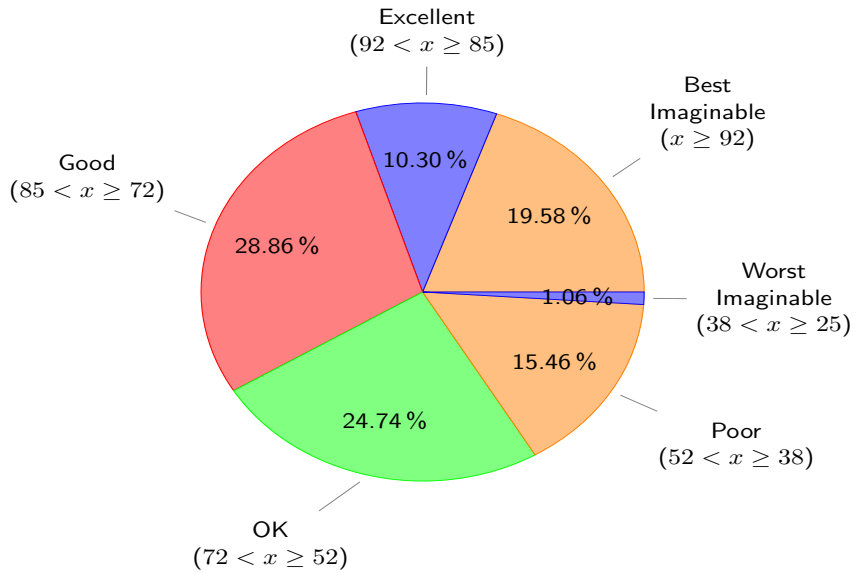


Usability Study (3)

1. **Roll of Hardware Variability**
   - **It would be worth investigating to evaluate the newly proposed authentication scheme on different devices and/or multiple models and reporting the results accordingly.**

Usability Study (3)

1. Roll of Hardware Variability
   - It would be worth investigating to evaluate the newly proposed authentication scheme on different devices and/or multiple models and reporting the results accordingly.
2. **Software Usability Scale (SUS)**
   - **Research proposing new mobile biometric should also include initial usability evaluation to get an impression of user acceptability of their scheme.**



Performance Analysis

1. **Power Overhead**
   - **Any proposed mobile biometric recognition system must not consume much power to be adopted in the real-world applications.**

Performance Analysis

1. Power Overhead
   - Any proposed mobile biometric recognition system must not consume much power to be adopted in the real-world applications.
2. **Computational Overhead**
   - **It is strongly recommended to report CPU and memory overhead usage estimation for the proposed mechanism(s) to avoid any bad user-experience.**

Performance Analysis

1. Power Overhead
   - Any proposed mobile biometric recognition system must not consume much power to be adopted in the real-world applications.
2. Computational Overhead
   - It is strongly recommended to report CPU and memory overhead usage estimation for the proposed mechanism(s) to avoid any bad user-experience.
3. **Some Bench-Mark Applications**
   - **AnTuTu**
   - **GreekBench**
   - **Quadrant Standard**

Adversarial Analysis

1. **Random Attacks**
   - **To obtain such attacks samples, the participants should be asked to try randomly unlocking the device without knowing the implemented authentication mechanism.**

Adversarial Analysis

1. Random Attacks
   - To obtain such attacks samples, the participants should be asked to try randomly unlocking the device without knowing the implemented authentication mechanism.
2. **Mimic Attacks**
   - **To obtain such attacks samples, a genuine user could be asked to use the mechanism in front of the test-adversaries as many times as possible. In this way the adversaries may get a better overview of the implemented mechanism as well as legitimate user's behaviors that is to be mimicked.**

Adversarial Analysis

1. Random Attacks
   - To obtain such attacks samples, the participants should be asked to try randomly unlocking the device without knowing the implemented authentication mechanism.
2. Mimic Attacks
   - To obtain such attacks samples, a genuine user could be asked to use the mechanism in front of the test-adversaries as many times as possible. In this way the adversaries may get a better overview of the implemented mechanism as well as legitimate user's behaviors that is to be mimicked.
3. **Engineered Attacks**
   - **We admit that executing this type of attack is a bit time taking, cumbersome, and tricky, but the claims regarding the robustness of their proposed schemes should only be made after such evaluation.**

Conclusions

- **Motivation**
  - **Recent years have witnessed a lot of effort targeting the development newer (secure and usable) authentication solutions for smart devices.**

Conclusions

- Motivation
  - Recent years have witnessed a lot of effort targeting the development newer (secure and usable) authentication solutions for smart devices.
- **Guidelines**
  - **We presented some guidelines, particularly targeting researchers of smart-devices authentication domain, for helping them in designing, implementation, and evaluation of their proposed schemes.**

Conclusions

- Motivation
  - Recent years have witnessed a lot of effort targeting the development newer (secure and usable) authentication solutions for smart devices.
- Guidelines
  - We presented some guidelines, particularly targeting researchers of smart-devices authentication domain, for helping them in designing, implementation, and evaluation of their proposed schemes.
- **Objective**
  - **In order to maximize the impact and usability of the proposed schemes, it becomes extremely important to design, develop and evaluate, comprehensively, the upcoming schemes diverse criterion.**

Thank You!