Continuous biometric authentication using mobile devices

Jesús Friginal, Giovanna Sannino,
Alessandro Testa, Stefania Tosi

Some basics on authentication

- In general, **authentication** is the act of confirming the truth of a datum or entity
- In a system requiring the human interaction, we talk about **user authentication** when it is necessary to confirm the user identity to perform a given operation.
- Traditionally, user authentication has depended on
  - What you have (e.g., id cards)
  - What you know (e.g., login and password)

Challenges & opportunities to authentication

- New challenging scenarios for user authentication involving the presence of more **sophisticated attacks** and the increasing use of **mobile devices**:
  - Identity based on **what you know** and **what you have** can be easily stolen/spoofed
- At the end, user authentication is a question of **accuracy**: the higher the accuracy, the higher the trust (security)
  - The notion of **what you are** introduces new opportunities to user authentication

Biometric authentication

- Introducing the notion of **biometric authentication** is essential to improve accuracy on user authentication
- A biometric is a characteristic of a human being that can distinguish one person from another and that can be used for identification or verification of identity
- More transparent to user than traditional login prompt, so more usable for disabled or aged people

Characterization of biometric mechanisms

- According to the type of sources
  - Physiological sources: Iris, Fingerprints, Hand, Retinal and Face recognition
  - Behavioral sources: Voice, Typing pattern, Signature
- According to the number of sources
  - Unimodal: they rely on a single source of information for authentication (e.g., fingerprint OR face)
  - Multimodal: they rely on several sources of information for authentication (e.g., fingerprint AND face)
- According to the authentication frequency
  - Single-shot: only one authentication
  - Continuous: several authentications along time

Characterization of biometric mechanisms

- According to the type of sources
  - Physiological sources: Iris, Fingerprints, Hand, Retinal and Face recognition
  - Behavioral sources: Voice, Typing pattern, Signature

Biometric Technology	Accuracy	Cost	Devices required	Social acceptability
ADN	High	High	Test equipment	Low
Iris recognition	High	High	Camera	Medium-low
Retinal Scan	High	High	Camera	Low
Facial recognition	Medium-low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature recognition	Low	Medium	Optic pen, touch panel	High

Overview of possible combinations

System	Accuracy of authentication	Resources cost (mem & CPU)	Intrusiveness
Unimodal & single-shot	Low	Low	Low
Multimodal & single-shot	Medium	Medium	Medium
Unimodal & Continuous	High	Medium	Medium
Multimodal & Continuous	Very high	High	High

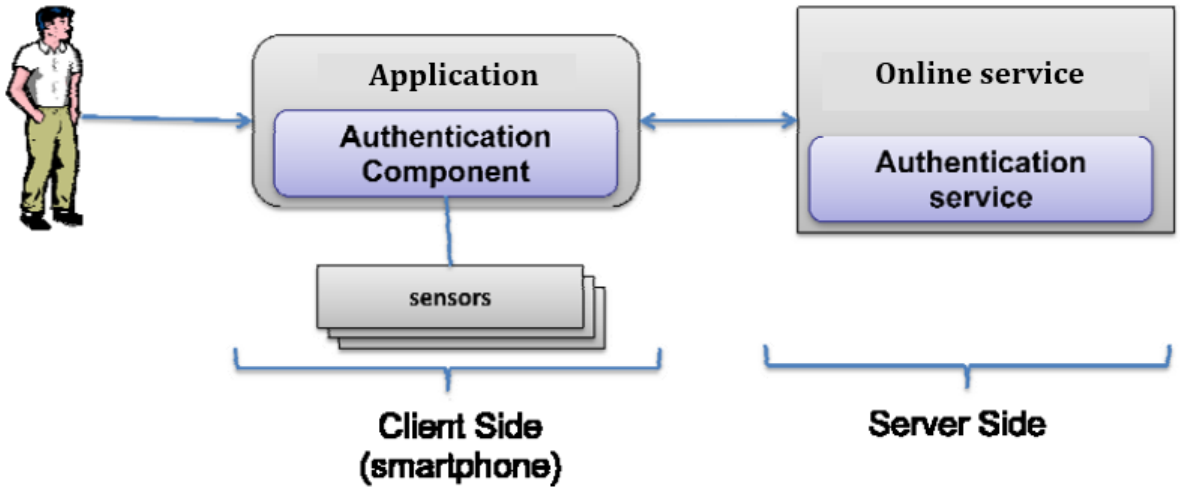
- What is the best option in general terms??
  - Accuracy of authentication: Multimodal & continuous
  - Resources cost: Unimodal & single-shot
  - Intrusiveness: Unimodal & single-shot
- What about dynamic scenarios (e.g., use of mobile devices)??
  - Dynamic scenarios require dynamic solutions

Context-Aware biometric authentication

The authentication system determines what is the best configuration according to:

- Level of noise in the environment
- Level of accuracy required by each scenario
- Level of available resources in the mobile device

General Architecture



Key parameters taken into account for our approach

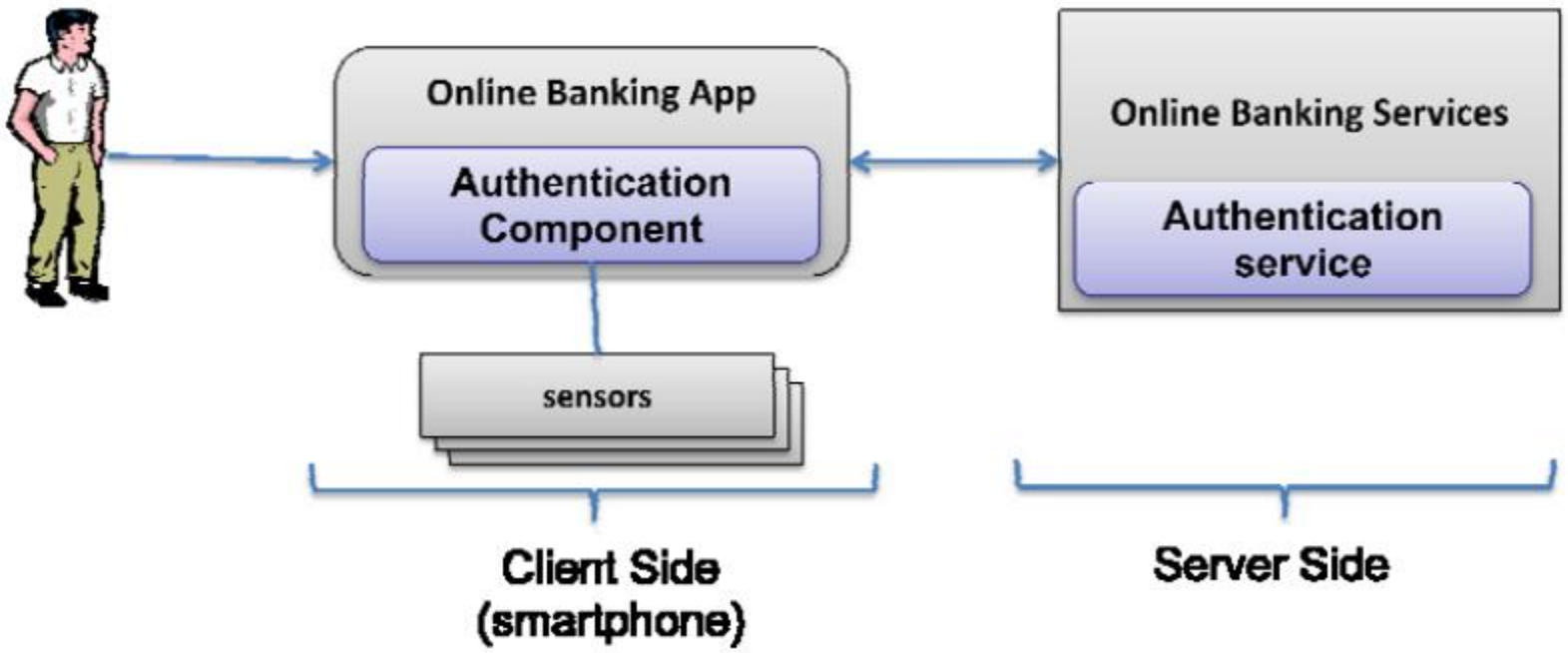
- Client side
  - –Type of sources
  - –Number of sources
  - –Authentication frequency
- Server side
  - –Redundant use of features-processing algorithms, considering diversification

Scenarios under evaluation

- Online banking scenario requirements
  - High accuracy/security
  - High availability

- VoIP scenario requirements
  - Low accuracy/security
  - High availability

1st scenario – Online banking

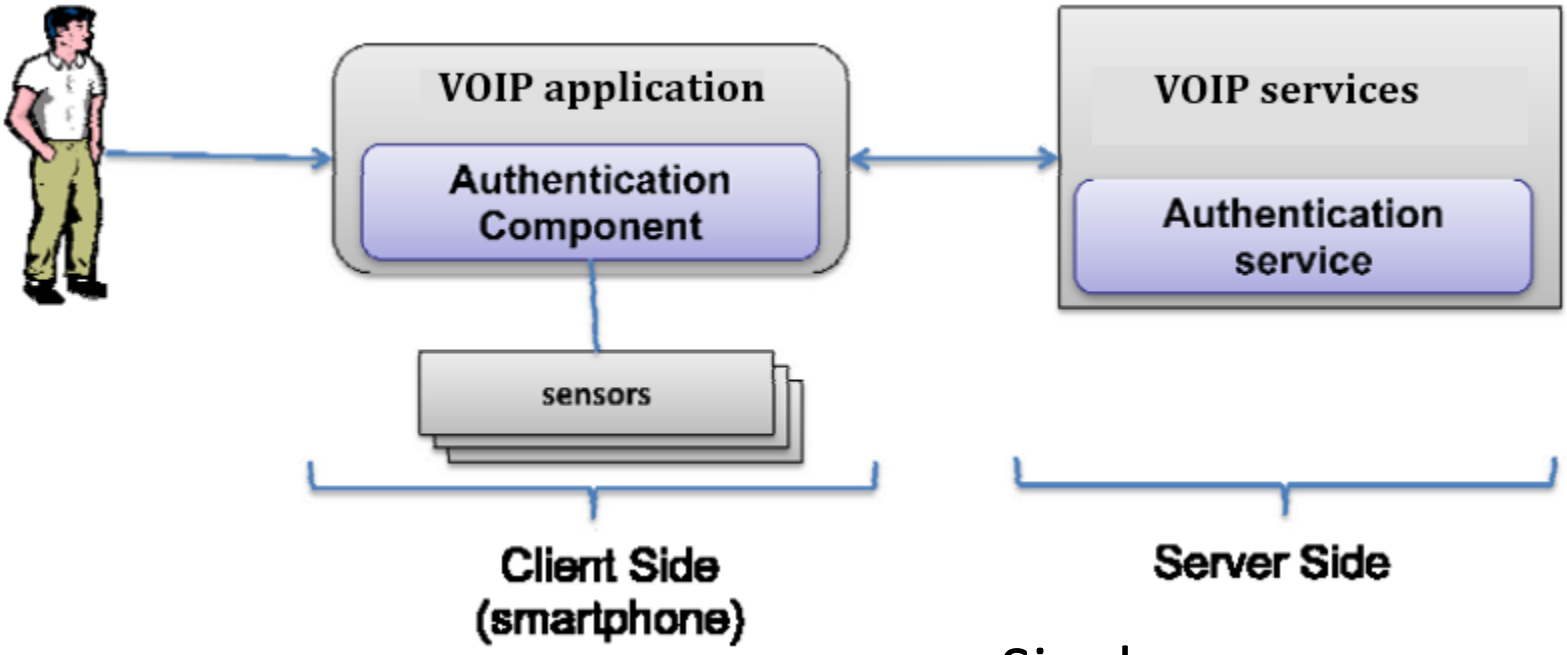


- Scenario requirements:
  - High accuracy/security
  - High availability

→

  - Different sources
  - High number of samples
  - High frequency
  - Redundant algorithms

2nd scenario – VoIP service



- Scenario requirements:
  - Low accuracy/security
  - High availability

→

  - Single source
  - Low number of samples
  - Low frequency
  - Non-redundant algorithms

Comparison of biometric solutions for the online banking service

Low Availability of Resources

System	Accuracy of Authentication	Resources Cost (mem & CPU)	Intrusiveness
Unimodal & single-shot	Low	Low	Low
Multimodal & single-shot	Medium	Medium	Medium
Unimodal & Continuous	High	Medium	Medium
Multimodal & Continuous	Very high	High	High
Our Proposal	**Very high**	**Low***	**Low/Medium**

High Availability of Resources

System	Accuracy of Authentication	Resources Cost (mem & CPU)	Intrusiveness
Unimodal & single-shot	Low	Low	Low
Multimodal & single-shot	Medium	Medium	Medium
Unimodal & Continuous	High	Medium	Medium
Multimodal & Continuous	Very high	High	High
Our Proposal	**Very high**	**Medium***	**High**

Comparison of biometric solutions for the VoIP service

Low/High Availability of Resources

System	Accuracy of Authentication	Resources Cost (mem & CPU)	Intrusiveness
Unimodal & single-shot	Low	Low	Low
Multimodal & single-shot	Medium	Medium	Medium
Unimodal & Continuous	High	Medium	Medium
Multimodal & Continuous	Very high	High	High
Our Proposal	**Low**	**Low**	**Low**

Conclusions

- Applying context-aware authentication in the domain of mobile devices enables the user to increase the accuracy of identification and verification with biometric data wherever while saving resources