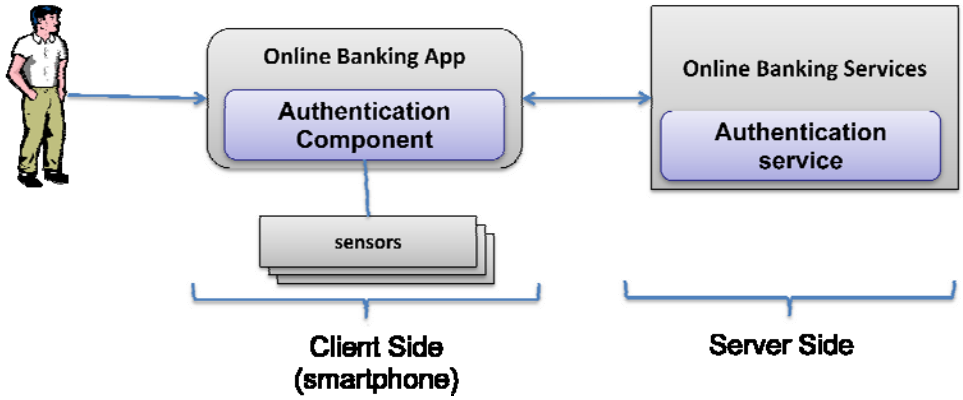
Title: “Continuous biometric authentication using mobile devices”

Description

Session management in distributed Internet services is traditionally based on username and password, and explicit logouts and timeouts that expire due to idle activity of the user. Biometric solutions allow to substitute username and password with biometric data; e.g., a user may submit its fingerprint instead of the pair username-password. However a single verification step is still deemed sufficient, and the identity of a user is considered immutable during the entire session. Additionally, the static length of the session timeout may impact on the usability of the service and consequent client satisfaction.



An alternative for the establishment and management of sessions is offered by biometrics, and consists on *multi-modal biometric continuous authentication* performed through continuous user verification based on biometric data acquired [1], [3]. The sensors on the client (e.g., the camera and microphone of a smartphone or of a laptop) acquire biometric data transparently to the user and sent to the authentication service. This makes user verification a continuous process, rather than a one-time occurrence. Also the length of the timeout may be configured depending on the user history and the trust that the authentication service place in the user [2].

Objectives

State of the art

Determine the state of the art on solutions for continuous authentication in *distributed* and *mobile* systems. Consider in particular the case of a user holding a mobile device (e.g., a smartphones) which accesses an Internet service.

Challenges and opportunities

Considering separately uni-modal and multi-modal biometrics systems, identify:

- the main challenges of applying a continuous authentication approach for Internet services using a mobile device in heterogeneous environments (e.g., noisy environments as train stations or marketplace), and
- the main opportunities offered by such approach.

Design a Solution

Design and evaluate a simple continuous authentication for mobile devices that authenticate to Internet services. Consider separately the case of uni-modal biometric systems and a multi-modal ones. Consider two different kinds of Internet services:

- Internet services with stringent requirements in terms of security
- Internet services with stringent requirements in terms of availability of the communication, but relaxed requirements on security

References

[1] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions," In *Proceedings of the 21st Annual Computer Security Applications Conference* (ACSAC '05), pp. 441-450, 2005. IEEE Computer Society, Washington, DC, USA. http://www.acsac.org/2005/papers/126.pdf

[2] A. Altinok and M. Turk, "Temporal integration for continuous multimodal biometrics," In Multimodal User Authentication, pp. 11-12, 2003. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.169.7004

[3] S. Ojala, J. Keinanen, J. Skytta, "Wearable authentication device for transparent login in nomadic applications environment," In 2nd International Conference on Signals, Circuits and Systems (SCS 2008), pp. 1-6, 7-9 Nov. 2008.

[4] BioID, Biometric Authentication as a Service (BaaS), BioID press release, 3 March 2011, https://www.bioid.com/ .