CORMORANT: Towards Continuous Risk-Aware Multi-Modal Cross-Device Authentication

Daniel Hintze
FHDW Paderborn
Fürstenallee 3 - 5
33102 Paderborn, Germany
daniel.hintze@fhdw.de

Eckhard Koch
FHDW Paderborn
Fürstenallee 3 - 5
33102 Paderborn, Germany
eckhard.koch@fhdw.de

Rainhard D. Findling
UAS Upper Austria
Softwarepark 11
4232 Hagenberg, Austria
rainhard.findlinge@fh-hagenberg.at

René Mayrhofer
JKU Linz
Altenbergerstraße 69
4040 Linz, Austria
rene.mayrhofer@jku.at

Muhammad Muaaz
UAS Upper Austria
Softwarepark 11
4232 Hagenberg, Austria
muhammad.muaaz@fh-hagenberg.at

Ubicomp/ISWC '15 Adjunct, September 7–11, 2015, Osaka, Japan.

ACM 978-1-4503-3575-1/15/09...$15.00.
http://dx.doi.org/10.1145/2800835.2800906

Abstract
Nowadays, people own and carry an increasing number of mobile devices, such as smartphones and smartwatches. Since these devices store and provide access to sensitive information, authentication is required to prevent unauthorized access. Widely used mechanisms like PIN and password, however, don't scale well with the growing number of devices and interactions. We present the preliminary design of *CORMORANT*, an extensible, risk-aware, multi-modal, cross-device authentication framework that enables transparent continuous authentication using different biometrics across multiple trusted devices.

Author Keywords
Authentication; biometrics; risk assessment

ACM Classification Keywords
D.4.6 [Security and Protection]: Authentication.

Introduction
Mobile devices, ubiquitous in modern lifestyle, embody and provide access to valuable assets, information and services. Since mobile devices have a high propensity to become lost or stolen, strong authentication is indispensable to prevent unauthorized access. Commonly applied knowledge-based mechanisms like PIN, pattern and password, however, require significant effort in proportion to usually short usage

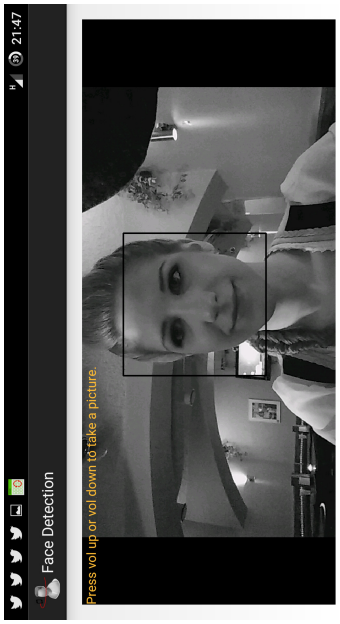

Figure 1: Face detection authentication module

sessions [3], don't scale well with the growing number of devices used simultaneously, and constitute a one-time all-or-nothing validation of the user's identity, ignoring the fact that different data and services feature different sensitivities.

Ubiquitous authentication in the form of continuous unobtrusive user identity verification allows overcoming the aforementioned drawbacks. Biometric features proving applicable for this purpose include keystroke dynamics, mouse dynamics, user interface interaction, finger pressure, voice, and gait. Since no single biometric is available at all times, several *multi-modal* biometric schemes have been developed to derive a device confidence level from different biometrics by applying strategies like feature level fusion, matching score level fusion, and decision level fusion [8].

By their nature, biometrics yield confidence levels (i. e., probabilities) rather than binary states. They are commonly used, however, for an all-or-nothing decision, resulting in access to a calculator being equally strong (and thus costly) secured as access to a mobile banking application. Security measures are applied to mitigate a *risk*, which can be seen as the probability of an adverse event occurring multiplied by the resulting cost. Both factors, however, vary based on context. For instance, mobile phone theft is more likely in public places than at home while the exposure of private pictures might be more costly than compromising one's music playlist. *Risk-awareness* could therefore facilitate adequately tailored security mechanisms [5].

Approaches towards multi-modal biometric authentication systems proposed so far operate on a single device [8]. With the increasing number of different interconnected devices owned and used by a single individual, it seems desirable to extend the scope in order to leverage contextual and biometric information gathered within a group of trusted devices to increase both security and usability [4, 9]. In this abstract, we therefore present the preliminary design of *CORMORANT*, an extensible, risk-aware multi-modal cross-device authentication framework that enables transparent continuous user identity verification across multiple trusted devices.

The *CORMORANT* Framework

Motivation and Goals

Our motivation and overall goal is to contribute to user-friendly authentication on mobile devices. As part of this effort, we are developing an open, extensible framework capable of utilizing arbitrary continuous and explicit authentication techniques. *CORMORANT* is novel in two aspects: It applies context-based risk assessment to fine-tune access control in order to task the user as much necessary but as little as possible. The second distinctive feature is the inclusion of information not only from one but possibly all device a user possesses. This facilitates a number of interesting application. For example, devices could derive sufficient confidence in the user's identity from nearby trusted devices to omit explicit authentication. If, for instance a user is continuously authenticated through gait recognition applied on his smartwatch [7], a notebook he is approaching could establish his identity if both devices trust each other and are able to determine their close proximity.

Architecture Design

The proposed framework is designed to be easily extensible through *authentication plugins* as well as *risk assessment plugins*, as outlined in fig. 2. While we provide some plugins like gait, voice, and face recognitions (see fig. 1), the framework itself is independent from any specific authentication or risk assessment mechanism and solely relies on the presence of corresponding plugins. With *CORMORANT*, we envision a platform that allows other researchers easy utilization of the features provided by the framework. By developing plugins and thus focusing on their primary research goals rather than being forced to develop the necessary infrastructure, ef-

forts are combined into one streamlined framework. In order to maximize accessibility of the framework, we expect plugins to feature only a minimal interface that enable their integration into the *CORMORANT* framework. Changes in confidence risk assessment are communicated either event-based by a particular module or on framework request, used for both periodical refreshes as well as to trigger explicit authentication upon necessity.

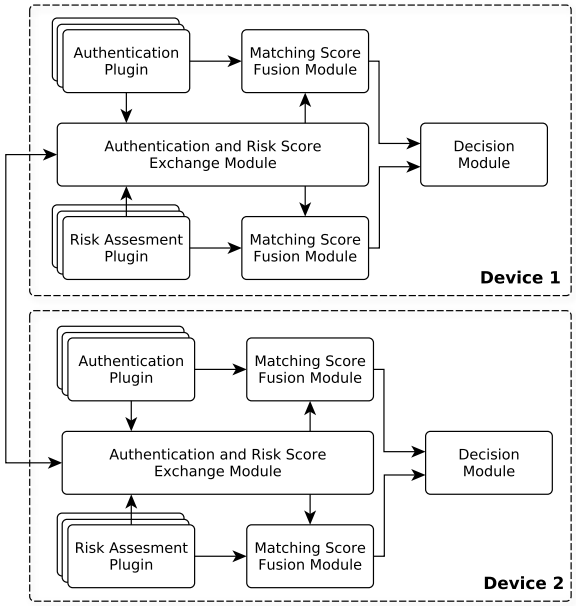

Figure 2: Preliminary architectural overview

In the *CORMORANT* framework, trusted devices owned and primarily used by a single user can form a single swarm continuously exchanging confidence scores as well as risk assessments. Trust between devices in the swarm is established using an initial pairing while a group key agreement approach such as Tree-based Group Diffie-Hellman is applied to secure the group communication protocol. An integral component of the *authentication and risk score exchange module* is spatial distance estimation, which, based on techniques known from indoor location systems, estimates the distance between trusted devices in the swarm. In general terms, devices within close proximity (e. g., < 1 m) are likely to be under physical control by the same individual, hence user confidence as well as risk assessment can be - to some extent - transferred. If, however, two devices that are not co-located have confidence in the user's presence at the same time, this could indicate that at least one of the devices has been compromised, resulting in both devices instantly locking down.

To integrate multiple confidence values or risk assessments from different available plugins, multi-modal fusion is applied within the *match score fusion module*. A number of approaches thereto exist, ranging from simple aggregate functions (e. g., minimum, maximum, average) to sophisticated machine learning strategies [1, 6]. Since the *CORMORANT* framework is novel in that it introduces spatial distance as well as device trust as additional factors in the fusion, we have yet to evaluate which fusion approach is best-suited for this application.

Finally, fused confidence values and risk assessments are combined in the *decision module* deciding whether to lock or unlock the device, allow or deny requested access to an application or resource, or to enforce additional explicit authentication. Individual decisions for each device allow for different results based on different risk assessments even if devices are situated in the same context, matching the requested confidence levels to the assets at stake.

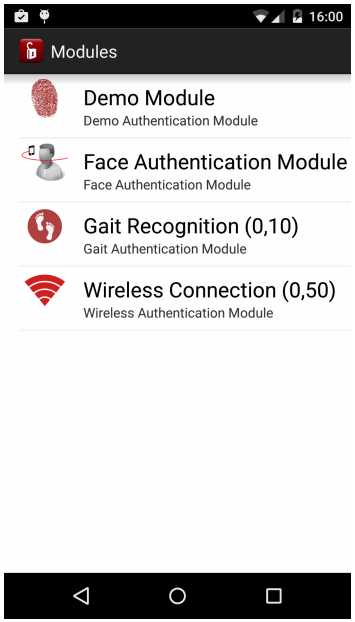

Figure 3: Android prototype displaying active authentication modules

Implementation

We implemented an elementary prototype of the *CORMORANT* framework for Android (fig. 3) to evaluate the feasibility of the plugin approach as well as the plugin interface design. Alongside, we developed early stages of biometric authentication plugins, namely gait and face recognition [2, 7].

Conclusion and Future Work

In this abstract we presented our preliminary design of a continuous risk-aware multi-modal cross-device authentication framework that utilizes information perceived within a swarm of trusted devices owned and controlled by the same user. The use of risk-assessment alongside inter-device cooperation has the potential to realize continuous and transparent authentication, enabling convenient and user-friendly security. We intend to choose or develop adequate strategies for both fusing user confidence and risk assessment, taking into account the role of cooperating trusted devices. Also, we will further specify a process of exchanging risk and authentication scores across devices to come up with a protocol that deals with initial pairing, group key exchange, device exclusion, and spatial distance estimation. Finally, we will evaluate the usability, performance, and practicality of the *CORMORANT* framework via an extensive user study under real-world conditions.

Acknowledgments

This work has been carried out partially within the scope of u'smile, the Josef Ressel Center for User-Friendly Secure Mobile Environments. We gratefully acknowledge funding and support by the German Federal Ministry of Education and Research, Christian Doppler Gesellschaft, A1 Telekom Austria AG, Drei-Banken-EDV GmbH, LG Nexera Business Solutions AG, NXP Semiconductors Austria GmbH, and Österreichische Staatsdruckerei GmbH.

REFERENCES

1. Kyle O. Bailey, James S. Okolica, and Gilbert L. Peterson. 2014. User identification and authentication using multi-modal behavioral biometrics. *Computers and Security* 43 (2014), 77–89.
2. Findling, Rainhard D and Rene Mayrhofer. 2013. Towards Pan Shot Face Unlock: Using Biometric Face Information from Different Perspectives to Unlock Mobile Devices. *International Journal of Pervasive Computing and Communications* (2013), 190—-208.
3. Daniel Hintze, Rainhard D Findling, Sebastian Scholz, and René Mayrhofer. 2014. Mobile Device Usage Characteristics: The Effect of Context and Form Factor on Locked and Unlocked Usage. In *Proceedings of MoMM 2014*.
4. Christopher G. Hocking, Steven M. Furnell, Nathan L. Clarke, and Paul L. Reynolds. 2011. Authentication Aura - A distributed approach to user authentication. *Information Assurance and Security* 6, 2 (2011).
5. Adam Hurkala and Jaroslaw Hurkala. 2014. Architecture of Context-Risk-Aware Authentication System for Web Environments. *ICIEIS'2014* (2014), 219–228.
6. Soumik Mondal and Patrick Bours. 2015. A computational approach to the continuous authentication biometric system. *Information Sciences* 304 (2015), 28–53.
7. Muhammad Muaaz and Rene Mayrhofer. 2014. Orientation Independent Cell Phone Based Gait Authentication. *Proceedings of MoMM 2014* (2014).
8. P. S. Sanjekar and J. B. Patil. 2013. An Overview of Multimodal Biometrics. *Signal & Image Processing (SIPIJ)* 4, 1 (2013), 57–64.
9. Frank Stajano. 2011. Pico: No more passwords! *Lecture Notes in Computer Science* 7114 LNCS (2011), 49–81.