Integrating Continuous Credentials in Authentication Mechanisms

Dor Malka, Ittay Eyal

July 20, 2025

1 Abstract

Authentication is a fundamental aspect of security that can be viewed from two main perspectives: credentials and protocols. The credentials aspect is familiar to most of us through username and password, or OTPs used when accessing personal bank account or authenticating into services such as Google/Apple ID. While these discrete credentials, which rely on simply having or knowing something are widely used, there remains a largely unexplored space: continuous credentials.

Continuous credentials appear in several applications such as biometric authentication (fingerprints, eigenface or iris) and SSO mechanisms that rely on behavioral or environmental signals like GPS location etc. These credentials are not evaluated in a discrete way. Rather, they are measured by a mechanism that determines whether there are enough similarities above a predetermined threshold between an input and a stored figure.

These mechanisms introduce a spectrum of confidence instead of a strict yes or no decision. As achieving high security level based on one credential and satisfying the mechanism might be hard, we aim to study the integration of several continuous credentials. Our research will explore how multiple continuous credentials can be fused to form a robust authentication mechanism and determine an optimal mechanism, achieving high security level in wallet design for both digital and physical assets.

2 Related Work

Lin Hong et al. [1] found that automatic personal identification system based solely on fingerprints or faces is often not able to reach sufficiently low FAR and FRR. They integrated a biometric system which makes personal identification by integrating both faces and fingerprints operates during identification mode. The decision fusion of their system is designed to operate at measurement level, that is the system doesn't just output a single decision or label but rather a set of labels with confidence values. The system decision is based on the confidence of each one of the modules which might lead to a more reliable and informative overall confidence score.

These confidence values are characterized by the FAR values of the credential. The FAR values were calculated as the number of similarities between 2 measures above a threshold t. If there are 5 similarities out of 8 between 2 fingerprints and the threshold was 4, these 2 fingerprints will be considered equal.

Prabhakar et al. [2] examined the tradeoff between False Acceptance Rate (FAR) and False Rejection Rate (FRR), highlighting its impact on both the accuracy and security of biometric systems. Their findings suggest that most applications aim to operate at a point that balances these two metrics.

This concept is further developed by Sarkar et al. [3], who introduced it as the Equal Error Rate (EER). Sarkar defined this point as the operating point of the biometric system, emphasizing that the lower the EER value, the greater the performance of the biometric authentication system.

Eyal et al. [5] designed and formulated a foundational wallet model, defining four possible states for each credential – safe, loss, leak and theft. However, this work did not address the type of credentials involved, nor proposed a method to determine the probability of each credential's state.

3   Authentication Model

We analyzed the authentication model as a wallet w based on continuous credentials, each defined by a distinct probabilistic distribution functions. Then, We formalized the systems success and identified the optimal operating point for both single or multiple credentials.

3.1   Model Details

We follow the definitions given by Eyal [5]. A wallet w is defined by predicate of availability of N keys. Each key can be in one of the following states. Safe: only the user has access to the key. Loss: neither the user nor the attacker has access to the key. Leak: both the user and the attacker have access to the key. Theft: only the attacker has access to the key.

We define the probability associated with each state as follows: P_{safe}, P_{loss}, P_{leak} and P_{theft} corresponding respectively to the states of safe, loss, leak, and theft. Furthermore, the confidence associated with different decisions may be characterized by the genuine distribution and the impostor distribution, which are used to establish two error rates: false acceptance rate (FAR), which is defined as the probability of an impostor being accepted as a genuine individual and false rejection rate (FRR), which is defined as the probability of a genuine individual being rejected as an impostor.

3.2   Single Credential

We've built FAR vs FRR curves for Uniform, Triangle, Parabolic and Gaussian probabilistic distribution functions and defined each one of the states as follows:

$$P_{\text{loss}} = \text{FRR} \cdot (1 - \text{FAR})$$

$$P_{\text{leak}} = \text{FAR} \cdot (1 - \text{FRR})$$

$$P_{\text{theft}} = \text{FRR} \cdot \text{FAR}$$

$$P_{\text{safe}} = 1 - P_{\text{loss}} - P_{\text{leak}} - P_{\text{theft}}$$

$$P_{\text{Success\_AND}} = P_{\text{safe1}} \cdot P_{\text{safe2}} + P_{\text{safe1}} \cdot P_{\text{leak2}} + P_{\text{safe2}} \cdot P_{\text{leak1}}$$

$$P_{\text{Success\_OR}} = P_{\text{safe1}} \cdot P_{\text{safe2}} + P_{\text{safe1}} \cdot P_{\text{loss2}} + P_{\text{safe2}} \cdot P_{\text{loss1}}$$

References

[1] Lin Hong and Anil Jain. *Integrating Faces and Fingerprints for Personal Identification.*
IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998.

[2] S. Prabhakar, S. Pankanti, and A. K. Jain.
Biometric recognition: Security and privacy concerns.
IEEE Security & Privacy, 1(2), 33–42, 2003.

[3] Arpita Sarkar and Binod K. Singh.
A review on performance, security and various biometric template protection schemes for biometric authentication systems.
Multimedia Tools and Applications, vol. 79, nos. 37–38, pp. 27721–27776, Oct. 2020.

[4] Marwa Mouallem and Ittay Eyal.
Asynchronous Authentication.
CCS 2024 - Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security, pp. 3257–3271.

[5] Ittay Eyal.
On cryptocurrency wallet design..
Cryptology ePrint Archive, Paper 2021/1522,2021. https://eprint.iacr.org/2021/1522.