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

Authentication is a fundamental aspect of security and can be viewed from two main perspectives: credentials and protocols [4]. Our Focus is on the credentials aspect and particularly the integration of non-binary credentials, such as biometrics, into authentication protocols aiming to enhance security and usability.

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 (means that the system doesn't just output a single decision or label (e.g., "this is a cat") 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 that above threshold t.

In case, there are 5 similarities out of 8 between 2 fingerprints and the threshold was 4 therefore these 2 fingerprints will be considered equal. Face has done the same if the DFFs are lower than a threshold. FAR is the False accept among those equals and those lower than the threshold.

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.

No existing work, to our knowledge, has explored the integration of probabilistic non-binary credentials with differing distributions across multiple fusion mechanisms, as proposed in this study.

3 Symmetric Distribution Function

3.1 Symmetric Gaussian Distribution Function

3.2 Symmetric Uniform Distribution Function

3.3 Symmetric Parabolic Distribution Function

4 Asymmetric Distribution Function

4.1 Asymmetric Gaussian Distribution Function

4.2 Asymmetric Uniform Distribution Function

4.3 Asymmetric Parabolic Distribution Function

5 Model

5.1 Mechanism Success 2 credentials

5.2 Mechanism Success 3 credentials

6 Optimal Mechanism

7 Conclusion

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.