

Privacy Preserving Biometrics based Remote Authentication Protocol for Mobile Devices

Faculty supervising the research: Professor Elisa Bertino.
PhD student nominated: Hasini Gunasinghe.

1 Motivation

There has been a major shift from traditional passwords based authentication to biometrics based authentication in consumer applications in the recent past as major service providers such as the leaders in banking [1, 2, 3], credit cards [4] and e-commerce [5, 6] are adopting biometrics to authenticate users. Biometrics is a strong authentication factor due to its ability to uniquely identify an individual. Different vendors have adopted it for different motivations. For example, Amazon uses selfies based on facial recognition techniques to avoid the difficulty of typing passwords to authenticate transactions in mobile devices with small screens [5]; Master Card has adopted it in order to drastically cut-down the cost of falsely declined transactions [4].

Two main contexts in which biometrics is being used for authentication are: in-person authentication [7] and remote authentication [2]. In the first case, the user is present at the authenticator's premise when authentication is performed whereas in the second case, authentication is performed over the network. While there are common challenges w.r.t both cases due to sensitivity as biometrics is tightly coupled with one's identity, non-repeatability as no two biometrics samples of the same individual match exactly, and non-revocability as biometrics cannot be canceled/revoked, the second case is more challenging than the first one due to spoofing attacks, attacks on the communication channel, and attacks on the user's device.

Remote commercial authentication systems being deployed today have key security problems irrespective of whether they incorporate state-of-the-art facial/voice recognition algorithms and liveness verification techniques. First, since users' biometrics templates are stored in the server databases for matching during the authentication, these databases become major targets of attackers. For example, in Google Hands Free system [7], user's picture taken at the authentication time is matched with the user's Hands Free profile picture. In the Citi bank system, the user's pre-recorded voice samples are matched with the voice captured when the user call in. Second, multiple third party service providers store different biometrics traits of the same user (such as face, voice and fingerprint) for their proprietary authentication protocols. This creates multiple points of vulnerability on one's biometrics identity, due to linkability [8]. Third, the current protocols require the users to send a raw biometrics sample over the network each time the user remotely authenticates using biometrics, which is not desirable. Stolen biometrics templates lead to identity theft which poses severe threat to user's digital identity, compared to the case in which a password is stolen, because biometrics samples reveal sensitive features of the user's biometrics identity which can not be revoked.

Therefore, it is critical that secure biometrics based remote authentication protocol to not require storing and transmitting sensitive biometrics information during authentication. The second issue mentioned above can be addressed by introducing a trusted identity provider (IDP) to enroll user's biometrics identity [7, 9]. However, if the IDP is involved in each transaction in which the user authenticates, such approach undermines the user's privacy since the IDP learns information about different transactions that the user performs with different service providers (SPs).

To address aforementioned security and privacy issues, we aim to develop a biometrics based remote authentication protocol which addresses the following requirements:

1. The user's biometrics identity is enrolled with only a trusted IDP (i.e: biometrics is not stored with multiple SPs).
2. The sensitive features of user's biometrics are not stored anywhere.
3. The sensitive features of user's biometrics are not revealed during authentication.
4. After the initial enrollment with the IDP, users can carry out biometrics based authentication with multiple SPs without involving the IDP. (i.e: user-centric as opposed to traditional IDP-centric authentication protocol).
5. Enrolled biometrics identity is revocable and renewable.
6. Efficiency in terms of computation and communication in order for it to be carried out from user's mobile devices.

In what follows we describe our roadmap for designing and developing a privacy preserving biometrics based remote authentication protocol which addresses the above requirements.

2 Past and on-going research work

In our past research we have determined that zero knowledge proof (ZKP) of identity [10] is a suitable cryptographic primitive to be used along with a secure commitment scheme [11], in order to perform biometric-based authentication with a SP without revealing any sensitive biometrics information to the SP. The concept of ZKP of identity, first proposed by Feige, Fiat and Shamir [10] in 1988, has been used to develop numerous identity based authentication schemes [12, 13] for static identities such as email, credit card number, etc. Making it applicable to the domain of biometrics based remote authentication is not straightforward due to non-repeatable nature of biometrics identity. Since the biometrics sample used to create the commitment does not exactly match the biometrics sample captured during authentication, the ZKP might not succeed even for the genuine prover, unlike in the case of static identity. Previous approaches which addressed the non-repeatability issue of biometrics, mainly in the domain of biometrics based encryption, have used distance matching with threshold, by applying error correction techniques to the features extracted from the second sample. Our goal is to generate a unique, repeatable and revocable biometrics based identifier for the user, to be used in creating the identity commitment during the enrollment of identity and to be used in authentication via ZKP of identity. We employ a machine learning based classification model to generate such biometrics identifier (BID), based on the discriminative features of the user's biometrics.

Overview of the solution

In what follows we provide an overview of the protocol that we have proposed, using the aforementioned building blocks. Please refer to our paper [14] for more details. This protocol involves three main parties namely: IDP, SP, and user. It involves two main phases namely: enrollment phase and authentication phase.

Enrollment Phase: First, the IDP trains a classification model using the biometrics features extracted from biometrics images. The output is a file encapsulating the base-classification model that encodes the information required for prediction. During enrollment of each user, the base classification model is customized by randomizing the class labels encoded in the model. This step is performed as a security measure to protect the BIDs of the other users of the system, if one user's device is compromised. Features extracted from the biometrics image of the enrolling user are given as input to the customized classification model and the corresponding class label is obtained through prediction. This class label is combined with the user provided secret to generate the BID, which is used in creating the identity commitment. The identity commitment, which is based on the Pedersen commitment scheme [11], takes the form: $C(x, r) = g^x h^r \text{mod } p$, where $x = \text{BID}$ and $r = \text{user provided secret}$. Password based key generation is used to derive multiple secrets used in the protocol from a single password provided by the user. The BID generated according to our strategy preserves its uniqueness as it is based on the discriminatory features of the user's biometrics, is repeatable based on the prediction accuracy of the classification model, and is revocable as the user can cancel any existing BID and obtain a new one simply by requesting the IDP to issue a new customized classification model, which will return a different class label, and by changing the password from which the secret used to create the BID is derived. At the end of the enrollment process, the user is issued an identity token (IDT) which contains the identity commitment signed by the IDP and the customized classification model, to be used during the authentication phase, which are securely stored in the user's device.

Authentication Phase: During the authentication phase, the user provides the IDT issued by the trusted IDP, to the SP and carries out a ZKP of the biometrics identity with the SP. The authentication succeeds if the user is able to prove the SP in zero-knowledge, his/her ownership of the biometrics identity and the knowledge of the secret encoded in the identity commitment recorded in the IDT. In order to carry out the proof, features extracted from a new biometrics image of the user are given as input to the customized classification model stored in the user's device and the BID is generated according to the same steps used for the BID generation in the enrollment phase. This BID and the secret derived from the user's password are used to carry out the ZKP of biometric identity.

Our protocol [14] complies with the first five requirements mentioned in Section 1. The research goal of the current semester (Spring 2016) is to implement it in the mobile device and to evaluate the performance in order to assess its efficiency.

3 Next research goal

In our solution, we assume the support of a Trusted Execution Environment (TEE) in the user's mobile device to securely store the artifacts obtained from the IDP during the enrollment phase and to execute the BID generation process using the classification model during the authentication phase. TEE isolates the storage and the execution from other applications that run in the device which provides protection against Trojan type attacks, in addition to just providing encrypted storage for the artifacts. TEE is used by Apple touch ID and Android fingerprint authentication framework as well. Although there are extensive research on the development of TEE technology [15], there are attacks that have been discovered [16] on them too. Since widely used implementations of TEE technology such as ARM's TrustZone are proprietary and are not disclosed for public review, the level of assurance provided against a given threat model is unclear [17].

Furthermore, recent advances in memory forensics techniques [18] have introduced new privacy threats as these techniques show is that is possible to recover data from memory images even long after the processing of the data has completed. Although it is theoretically possible to clear the related memory upon destruction of a process, such approach is not practical because it requires accurate tracking of each data object, which is a very heavy-weight operation that no commodity operating system performs.

Therefore, our next research goal is to develop a biometrics based authentication protocol which achieves all the security and privacy goals mentioned in Section 1, based only on theoretical foundations and without assuming any platform security support. Fully homomorphic encryption (FHE) [19] is one solution that does not require decryption of sensitive information during authentication. However, FHE has several limitations, including: the SP learns the authentication function, which is the classification model in our case; and SP needs to obtain the secret key to decrypt the authentication decision, which in turn allows the SP to decrypt the biometrics data as well. Yao's garbled circuit [20], on the other hand, is a better cryptographic building block as it allows secure computation of a function f on an input data x to obtain the result $f(x)$ while hiding both the function and the input data from the function evaluator.

Overview of the proposed solution

In what follows we present the initial design of the solution that we aim to develop next.

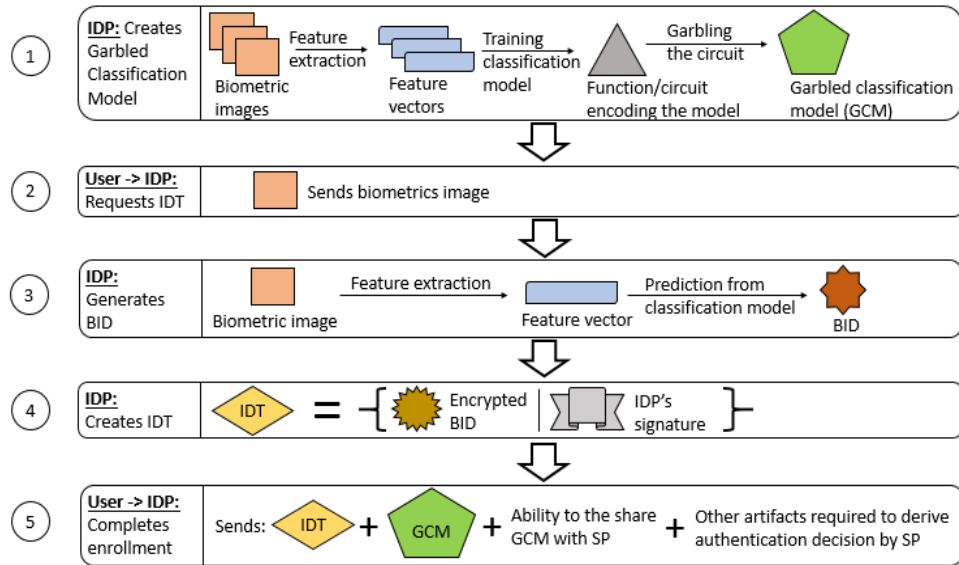


Figure 1: Proposed Enrollment Phase

Enrollment Phase: As shown in Figure 1, the IDP first creates a trained classification model (which is a function that can be encoded as a circuit) and then creates a garbled version of it (step 1). This is shared with the enrolling user, to be used during authentication, along with other artifacts and the IDT (step 5). The IDT in this case is the encrypted and signed BID of the user (step 4). The encryption used here facilitates the comparison in encrypted domain without requiring any secret key to decrypt the comparison result. This is achieved by providing a garbled version of the decryption function to the evaluator (see step 3.ii of Figure 2). The BID is obtained as the classifi-

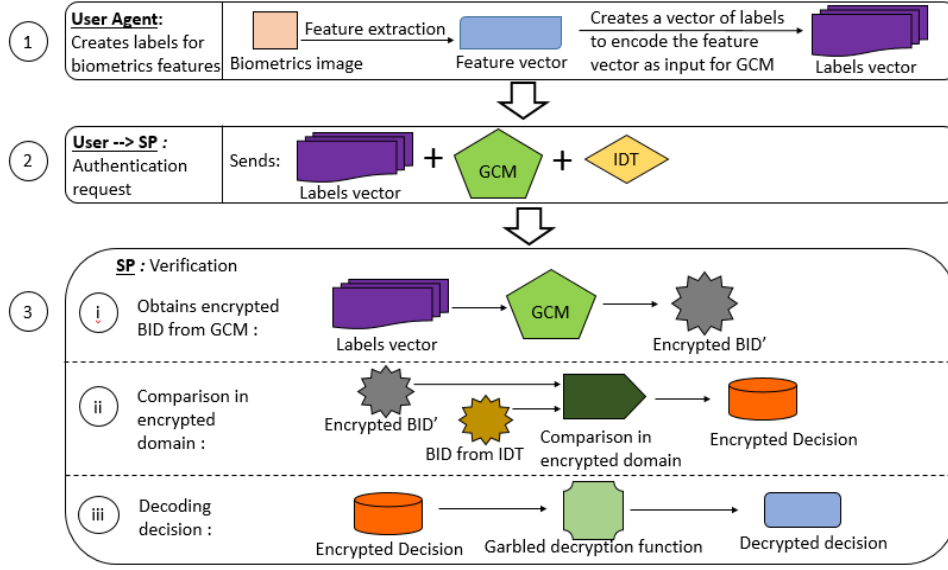


Figure 2: Proposed Authentication Phase

cation output of the biometrics features of the user which is given as input to the trained classification model (step 2).

Authentication Phase: The authentication phase is illustrated in Figure 2. Using the ability to share the GCM with the authenticator (i.e: SP) which is delegated by the IDP (step 5 of Figure 1), the user creates labels corresponding to the biometrics feature vector (step 1), for the SP to evaluate the GCM and obtain the encrypted BID (step 3.i). During the verification, the SP compares in the encrypted domain, the output obtained in the step 3.i with the encrypted BID in the IDT issued by the IDP (step 3.ii). SP uses the provided garbled decryption function to obtain the decrypted authentication result (step 3.iii) without learning any other sensitive information about the user’s biometrics.

Challenges: One basic limitation of the original garbled circuit construction is that it offers only one-time usage. Specifically, evaluating a circuit on any new input requires an entirely new garbling of the circuit [21]. This requires the user to communicate with the IDP each time the user needs to authenticate to a SP, which we need to avoid as per the 4th requirement mentioned in Section 1. The problem of reusing garbled circuits has been open for 30 years until very recently when the notion of reusable garbled circuit construct was proposed by Shafi et. al in 2013 [21]. This new construct sounds promising for the development of our target biometrics based authentication protocol, as it makes it possible to use multiple times the secure authentication artifacts that are issued upon enrollment (step 5 of Figure 1) without exposing any sensitive information during the authentication process.

Utilizing this construct in designing and developing our target biometrics authentication protocol, however, requires addressing several challenges. First, the scheme proposed in [21] is used in the context of two party secure computation protocols. We need to extend it to the case of a three-party secure computation protocol to build our solution, specifically as we need to address the question of how the IDP (which is the circuit generator) delegates the ability to the user (step 5 of Figure 1) to issue labels to the SP(s) (step 1 of Figure 2) for the SPs to evaluate the garbled classification model (step 3.1 of Figure 2). Second, encoding the classification model as a garbled function is a challenge. Very recent efforts [22] have focused on developing building blocks to construct privacy preserving classifiers which will be useful in addressing this challenge. Third, we need to investigate whether it is possible to combine the three substeps in the step 3 of the authentication phase into one garbled circuit or whether these substeps must be executed separately, based on technical feasibility, security and efficiency. Fourth, we need to make sure that delegation of the ability to share the GCM by the IDP to the user does not require storing secret information at the user’s device. Fifth, all the existing efficient implementations of garbled circuits do not support this construct, which is a major implementation challenge of our protocol.

Therefore, we believe that addressing such challenges and developing a design and implementation of a secure and privacy preserving biometrics authentication protocol using this construct will result in groundbreaking contributions to the area of remote, privacy-preserving, and strong authentication techniques, and may also contribute to enhance current products. Finally we believe that, as the proposed architecture is modular and independent from specific

device hardware characteristics, that our protocols and software tools can be used also for authentication in IoT (Internet-of-Things) contexts and can be easily transferred as a commercial product.

Contribution of this work:

We aim to produce the following research output:

1. Designing a secure and privacy preserving biometrics based remote authentication protocol which complies with the requirements listed in section 1, using re-usable garbled circuit construct.
2. A prototype implementation of the protocol that is able to run in mobile devices.
3. Security and performance analysis of the protocol.

References

- [1] B. Yurcan. (2016) Banks embrace biometrics, but will customers? [Online]. Available: <http://www.americanbanker.com/news/bank-technology/banks-embrace-biometrics-but-will-customers-1078867-1.html>
- [2] N. Cappella. (2016, Feb.) Hsbc announces biometric banking with voice and fingerprints. [Online]. Available: <https://thestack.com/world/2016/02/19/hsbc-voice-biometric-online-banking/>
- [3] P. Crosman. (2015, Feb.) Biometric tipping point: Usaa deploys face, voice recognition. [Online]. Available: <http://www.americanbanker.com/news/bank-technology/biometric-tipping-point-usaa-deploys-face-voice-recognition-1072509-1.html>
- [4] A. MacGregor. (2016, Feb.) Security in rich internet applications. [Online]. Available: <https://thestack.com/iot/2016/02/22/mastercard-rolls-out-selfie-verification-for-mobile-payments/>
- [5] A. MacGregor. (2016) Amazon wants to replace passwords with selfies and videos. [Online]. Available: <https://thestack.com/security/2016/03/15/amazon-wants-to-replace-passwords-with-selfies-and-videos/>
- [6] M. Anderson. (2015) Alibaba demonstrates facial recognition payment system at cebit. [Online]. Available: <https://thestack.com/security/2015/03/16/alibaba-demonstrates-facial-recognition-payment-system-at-cebit/>
- [7] M. Anderson. (2016) Google testing facial recognition payments on android and ios in san francisco. [Online]. Available: <https://thestack.com/cloud/2016/03/03/google-hands-free-facial-recognition-trial-san-francisco/>
- [8] H. Gunasinghe and E. Bertino, “Rahasnym: Protecting against linkability in the digital identity ecosystem,” in *The 35th IEEE International Conference on Distributed Computing Systems*. IEEE, June 2015.
- [9] “IdentityX | World-Class Mobile Biometric Authentication,” <http://www.identityx.com>.
- [10] A. S. U. Feige, A. Fiat, “Zero-knowledge proofs of identity,” *Journal of Cryptology*, 1988.
- [11] T. P. Pedersen, “Non-interactive and information-theoretic secure verifiable secret sharing,” in *Proceedings of CRYPTO’91*, 1992.
- [12] J. Camenisch and A. Lysyanskaya, “An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation,” in *Proceedings of EUROCRYPT ’01*, pp. 93–118.
- [13] J. C. E. Brickell and L. Chen, “Direct anonymous attestation,” in *ACM Conference on Computer and Communications Security*, 2004.
- [14] H. Gunasinghe and E. Bertino, “Privacy Preserving Biometrics-Based and User Centric Authentication Protocol,” in *Network and System Security - 8th International Conference, NSS 2014*, 2014, pp. 15–17.
- [15] N. Asokan, J. Ekberg, and K. Kostianen, “The untapped potential of trusted execution environments on mobile devices,” in *Proceedings of Financial Cryptography and Data Security*, April 2013, pp. 293–294.
- [16] D. Shen. (2015) Attacking-your-trusted-core-exploiting-trustzone-on-android. [Online]. Available: <https://www.blackhat.com/docs/us-15/materials/us-15-Shen-Attacking-Your-Trusted-Core-Exploiting-Trustzone-On-Android-wp.pdf>
- [17] Wikipedia. (2014) Arm architecture. [Online]. Available: https://en.wikipedia.org/wiki/ARM_architecture
- [18] Z. Lin, J. Rhee, C. Wu, X. Zhang, and D. Xu, “Dimsum: Discovering semantic data of interest from un-mappable memory with confidence,” in *Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS12)*. ACM, 2012.
- [19] M. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully homomorphic encryption over the integers.” In EUROCRYPT, 2010.
- [20] A. C. Yao., “Protocols for secure computations.” in *In FOCS*, 1982.
- [21] S. Goldwasser, Y. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich, “Reusable garbled circuits and succinct functional encryption,” in *Proceedings of STOC13*.
- [22] R. Bost, R. A. Popa, and S. T. amd S. Goldwasser, “Machine learning classification over encrypted data,” in *NDSS ’15*, 2015.