Privacy Preserving Biometrics based Remote Authentication Protocol for Mobile Devices

March 25, 2016

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 factor of authentication due to its ability to uniquely identify an individual. Different vendors have adopted it for different motivations, for examples, Amazon uses selfies based on facial recognition techniques to avoid the difficulty in typing passwords to authenticate transactions in mobile devices with small screens [5] and Master cards has adopted it in order to drastically cut-down the cost of false decilned 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, user is present at the authenticator's premise when authentication is performed and a device of the autheticator captures the biometrics. In the second case, authentication is performed over the network and the biometrics is captured by the user's device. While there are common challenges w.r.t both cases due to the sensitivity (being tightly coupled with one's identity) non-repeatability (no two biometrics samples of the same individual match exactly) and non-revocable (inability to cancel/renew) nature of biometrics, the second case involves more challenges than the first one in terms of liveliness verification of the biometrics to avoid spoofing attacks, secure transmission of the authentication information and security of the user's device. Furthermore, remote biometrics based authentication is being widely used since online-banking and e-commerce applications are increasingly adopting it.
Aforementioned commercial authentication systems that are being deplyoed today, inherit key security concerns irrespective of the fact that they incorporate state-of-the-art facial/voice recognition algorithms and liveliness verification techniques. First, since users' biometrics templates are stored in the server databases for matching during the authentication, they become major targets of attackers. For examples, in Google Hands Free system [7], user's picture taken at the authentication time is matched with the user's Hands Free profile picture and in Citi bank system, user's pre-recorded voice samples are matched with the voice captured when the user call in. Second, multiple third party service providers are storing different biometrics traits of the same user (such as face, voice and fingerprint) for their proprietaty 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 from the server databases or from the authentication channels 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 best to avoid storing and transmitting sensitive biometrics information during authentication, when developing a secure biometrics based remote authentication protocol. The second issue mentioned above can be avoided by getting a trusted identity provider (IDP) to enroll user's biometrics identity [7, 9]. However, if the IDP is involved in each transaction that the user authenticates, it undermines the user's privacy since the IDP gets to know about different transactions that the user performs with different service providers.
To address aforementioned security and privacy concerns, we aim to develop a biometrics based remote authentication protocol with following characteristics:

1. User's biometrics identity is enrolled with only a trusted IDP (i.e: biometrics is not stored with multiple service providers).

2. Sensitive features of user's biometrics is not stored anywhere.

3. Sensitive features of user's biometrics is not revealed during authentication.

4. After the initial enrollment with the IDP, users can carry out biometrics based authentication with multiple service providers without involving the IDP. (i.e: user-centric authentication protocol as opposed to traditional IDP-centric authentication protocol).

5. Efficient 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 of realizing the goal of developing a privacy preserving biometrics based remote authentication protocol with the aforementioned characteristics.

2 Past and on-going research work:

We found Zero Knowlede Proof (ZKP) of identity to be a suitable cryptographic primitive to be used along with a secure commitment scheme [10], in order to authenticate without revealing any sensitive biometrics information to the SP. The concept of ZKP of identity, first proposed by Feige, Fiat and Shamir [11] 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 in the domain of biometrics based remote authentication is not straight forward due to non-repeatable nature of biometrics identity. In other words, since the biometrics sample used to create the commitment does not exactly match the biometrics sample captured during authentication, the ZKP might not suceed even for the genuine prover, unlike in the case of static identity. Previous approaches which addressed the non-repeatability of biometrics, mainly in the domain of biometrics based encryption, have used distance matching with threshold, by applying error correction on the features extracted from the second sample. Our goal is to generate a unique and repeatable biomtrics based identifier for the user, based on discriminative features of his/her biometrics, to be used in creating the identity commitment during the enrollment of identity and to be used later for authentication via ZKP of identity usig such commitment. We employ a machine learning based classification model to generate such biometrics identifier (BID).
In what follows we provide an overview of the solution that we have proposed. Please refer to our paper [14].
(Write about the ZKPK based solution that we have proposed and currently working on in implementing in the mobile device, to achieve the above goal.)
We needed to develop a mechanism that creates repeatable, revocable and unique BID. We use ML methods as opposed to traditional distance matching (I need to do a benchmarking to prove that ML outperforms distance matching).
Unique, non-repeatable, non-revocable.

Overview of the solution

(from our paper)
Currently, we are implementing it in the mobile phone, to test its feasibility interms of performance and security. Auth app is separate - which is trusted, which is invoked by any third party client app.

3 Next research goal:

In the aforementioned solution that we develop to achive our goal mentioned in Section 1, we assume the support of 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 BID generation using the classifier during the authentication phase. TEE isolates the storage and execution from other applications which provides further protection in addition to encrypting the artifacts during storage and which is being used by Apple touch ID and android fingerprint authentication framework as well. While there are extensive research on the develpment of TEE technology [15], there are attacks being discovered [16] on them too. Since widely

used implementations of TEE technology such as ARM's TrustZone are proprietary and not disclosed for public review, the level of assurance provided against a given threat model is unclear [17].
Furthermore, recent advancement in memory forensics techniques [18], pose threats on processing sensitive data in the memory of user's device in clear text, as it is proved that such data could be recovered from memory images even long after the processing of such data is finished. Although it is theoretically possible to clear the memory soon after the processing of sensitive data, it is not practical because it requires accurate tracking of each data object in order to clear them upon destruction of the process, which is a very heavy-weight operation that no commodity operating system performs.
Therefore, it is at our best interest to develop a privacy preserving biometrics based authentication protocol which achieves all the security and privacy goals mentioned in Section 1, based on theoretical foundations and without assuming any hardware security support. Fully homomorphic encryption (FHE) [19] is one solution to avoid decryption of sensitive biometrics information during authentication, however, it has certain drawbacks to be used in building an authentication protocol with the aforementioned characteristics, as the service provider learns the authentication function, which is the classification model in our case, and it needs to obtain the secret key to decrypt the authentication result, which in turn allows it 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 input data x to obtain the result $f(x)$ while hiding both the function and the input data from the function evaluator.

Related work:

What people have already done in this direction: - GC for biometrics authentication - GC on mobile devices - GC for classification - Reusabile GC.

Proposed Solution:

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 causes the user to communicate with the IDP each time the user needs to authenticate to a service provider, 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 the reusable garbled circuit contstruct was proposed by Shafi et. al in 2013 [21]. This new construct looks promising to develop the biometrics based authentication protocol that we target, as it allows the secure authentication artifacts to be used multiple times without exposing any sensitive information during the process. Utilizing this construct in designing and developing our target biometrics authentication protocol, however, requires addressing several challenges. Firstly, the scheme poposed in [21] is presented in the context of two party secure computation. Although original garbled circuit construct can be used in three-party context, it is currently not straight forward to see how the re-usable garbled circuit contruct could be extended to three-party protocol, which we need to investigate further. Secondly, all the current efficient implementations of garbled circuits do not support this construct, which is currently a challenge when it comes to implemention of the protocol. Therefore, we believe that designing and developing a privacy preserving biometrics authentication protocol using this construct will contribute important results to the research literature.

Contribution of this work:

We aim to produce the following research output:

1. Designing a privacy preserving biometrics based remote authentication protocol with aforementioned characteristics, 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.

4 Background and potential impact:

- After the current work is over, at the end of this semester, we will have a working prototype of our past approach in the mobile phone. PhD student Hasini will be attending a summer school conducted by leaders of secure mpc and oblivious computation research to learn the current-state-of-the-art techniques. She has got a travel grant form NSF to participate in this. - Google ATAP project has accepted a proposal written by us and has funded Purdue. - Can help make existing biometrics based remote authentication in day-to-day transactions such as online-banking and e-commerce secure, which already has a large user base and increasing.
- Generalization of this techniques can have impact on other ML tasks where privacy is a concern.

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] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proceedings of CRYPTO'91*, 1992.

[11] A. S. U. Feige, A. Fiat, "Zero-knowledge proofs of identity," *Journal of Cryptology*, 1988.

[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. Kostiainen, "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*.