Privacy Preserving Biometrics based Authentication Protocol for Mobile Devices

March 19, 2016

1 Motivation:

Biometrics has been used as a strong factor of authentication.
Unique, non-repeatable, non-revocable.
Major banks, credit card companies and e-commerce giants are shifting to biometrics based authentication.
Different merchants are adapting it for different motivations/goals.
In in-person (Google pilot project for in-store profile picture for payment verification) and remote authentication (Amazon and Ali-play). More challenges in remore authentication compared to in-person.
Popular e-commerce applications moving towards this, for user friendliness (hard to enter passwords in small screens and people forget) and security. Although their FRT and liveliness checks is improving, security wise their using traditional template matching. It has several critical risks:
- Several SPs maintaining it (e.g: Master card servers, Ali-pay etc.). This can be avoided by having a trusted IDP doing the auth verification for you. E.g: Google's Hands Free pay. But then the problem is: IDP knows about every place you make purchases which undermines your privacy.
- Need to protect the database.
- Need to reveal the biometrics each time. Higher risk of getting stolen.
- If compromised, higher risk than password.
Our goal is to develop a privacy preserving one - no storage of biometrics, no revealation of biometrics during auth, user-centric (no IDP involved after initial enrollment.) still the authenticator is confirmed that user is authenticated using his/her biometrics.

2 Past and on-going research work:

ZKP. This has been used for static identity based authentication for a long time, since its first inception in 1986 - FFS. Fulfils all requirements except for one major challenge. Challenge is using biometrics as the identity due to its non-static nature. We needed to develop a mechanism that creates repeatable, revocable and unique BID.

2.0.1 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.

3 Next research goal:

In the previous approach, - depend upon trust of hardware of phone to protect artifacts stored on the phone. But there has been attacks on trust zone uncovered in the past, which has been fixed. Although there is research going on that area as well, it is good to rely on them as less as possible. - We argue that attack window is very small. But there are recent attacks to recover sensitive info. from physical memory images.

To address such concerns, GC is a good candidate.

Challenges:

Reusability of the garbled circuits. Performance. Protocol achieving all the security and privacy goals.

Related work:

What people have already done in this direction:

Contribution of this work:

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.