2015 IEEE 35th International Conference on Distributed Computing Systems

# RahasNym: Protecting Against Linkability in the Digital Identity Ecosystem

Hasini Gunasinghe
Department of Computer Science
Purdue University
West Lafayette, Indiana
Email: huralali@purdue.edu

Elisa Bertino
Department of Computer Science and Cyber Center
Purdue University
West Lafayette, Indiana
Email: bertino@purdue.edu

***Abstract*—Unlinkability and accountability are conflicting yet critical requirements for on-line transactions that need to be addressed in order to preserve users' privacy as well as to protect service providers in today identity ecosystems. In this poster paper we introduce a pseudonymous identity management system in which users can carry out unlinkable on-line transactions without having to disclose their actual identity to the service providers. At the same time, the service providers have strong assurance about the authenticity of the identity and credentials. In our approach, users' identity is cryptographically encoded in pseudonymous identity tokens issued by trusted identity providers. Our system includes a lightweight policy language which enables users and service providers to express their requirements pertaining to pseudonymous identity verification and a suite of protocols based on zero-knowledge-proofs which enables the fulfillment of these requirements.**

## I. Introduction

Repositories storing users' identity information managed at various on-line service providers (SPs), have become the target of attackers. Some attacks exploit user identity information linked across multiple accounts of the same individual held at different SPs. An example is the epic attack [1] on the multiple cloud accounts of the Wired writer Mat Honan, which were linked by his real name. In this attack, the attackers used the last four digits of his credit card number, stolen from his Amazon account, in order to gain access to his iCloud account through which they deleted the data stored in all his Apple devices. Apart from external attackers, SPs themselves can link user identities associated with different accounts and transactions for various purposes that may undermine user privacy.

Therefore, it is important that the identity management systems enable users to manage accounts and carryout transactions in an unlinkable manner. By default, such solutions should also preserve the confidentiality of user's identity information. On the other hand, it is also critical to protect SPs from abuses that could be perpetrated by individuals hidden by pseudonyms. For example, users may overuse a certain privilege by associating it with multiple different pseudonyms. Therefore, SPs need to have assurance about the ownership of the users' identities, accountability and authenticity of the transactions. Accordingly, the requirements concerning pseudonymous identity verification vary depending on the nature of the transaction at hand as well as the preferences of the users and the SPs involved in the transaction. Hence, we need flexible identity management systems which are able to verify identity according to such requirements.

In order to prevent privacy breaches resulting from identity linkability, advanced use of pseudonymous or anonymous credentials has been proposed [2], [3]. However, previous schemes have certain drawbacks such as they address only a subset of the critical requirements, require more than three parties in order to support accountability and revocation, and use bulky tokens with complex cryptographic protocols. To date there is no comprehensive identity management system that supports different requirements concerning pseudonymous identity verification in the context of different transactions.

In this paper, we propose a pseudonymous identity management system (called RahasNym) that supports identity verification related to on-line transactions be carried out in a secure and unlinkable manner. In RahasNym, identity verification is performed using *pseudonym-bound identity tokens* (IDT) which encode different identity attributes of the user in cryptographic commitments. RahasNym also includes a policy language which facilitates users and SPs in the specification of their requirements pertaining to identity verification in on-line transactions. The suite of protocols provided by RahasNym is designed according to such requirements. The suite consists of one protocol for acquiring IDTs (Protocol 1) from identity providers (IDPs) and three protocols for proof of identity. The protocols for proof of identity are based on different Zero-Knowledge-Proof-of-Knowledge (ZKPK) schemes, namely Interactive ZKPK protocol (Protocol 2), Non-Interactive ZKPK protocol (Protocol 3) and Non-Interactive ZKPK with signature protocol (Protocol 4). They differ from each other depending on how the prover and verifier interacts during the protocol execution and how the identity proof is created.

## II. Overview of the RahasNym

RahasNym involves three main parties: user, SP and IDP. During the initialization phase of RahasNym, both the user and the SP define their identity verification policies with fine-grained rules. When the user wants to perform a certain transaction, the user agent (i.e: the software in the user's device) obtains from the SP the identity verification policy

1063-6927/15 $31.00 © 2015 IEEE
DOI 10.1109/ICDCS.2015.102

related to that particular operation and checks if this policy matches the user policy. If they match, the user agent acquires the IDTs required to perform the transaction from the corresponding IDP(s). For example, if credit card numer (CCN) is required for the transaction, the CCN-IDT is obtained from the user's credit card issuer and if the email address is required for the transaction, the email-IDT is obtained from the user's email provider. The IDP cryptographically encodes the user's identity information using the Pedersen Commitment scheme [4] and sends back to the user agent the digitally signed IDT. Then the user agent and the SP executes the matching identity verification protocol through which the user proves his/her identity to the SP in zero-knowledge.

Figure 1 shows an high level overview of the architecture of RahasNym. The shaded areas represent the main components of RahasNym that are distributed across three main parties involved in the identity management system. The user agent consists of two different RahasNym components: 1) The client API - that interacts with the SP and 2) The identity management module (IDMM) - that obtains IDTs from IDPs and creates proofs of identity on those IDTs. The client application that interacts with the SP can either be a web based application running in the user's web browser or a native client application installed in the user's device. The IDMM is a trusted application that runs as a background service in the user's device.

The sequence of interactions between different entities (see Figure 1) is as follows: (1) The client application obtains the identity verification policy from the corresponding SP. (2) The client application hands over the SP's policy to the IDMM. (3) The IDMM compiles the policy agreed by both parties, by combining the SP's and the user's policies. It then contacts the corresponding IDP(s) to obtain the required IDT(s) which is(are) handed over to the client application. (4),(5) The client application acts as a mediator between the SP and the IDMM during identity verification, by forwarding the challenges sent by the SP to the IDMM and forwarding the identity proofs provided by the IDMM to the SP. The intended transaction is completed after successful verification of identity.

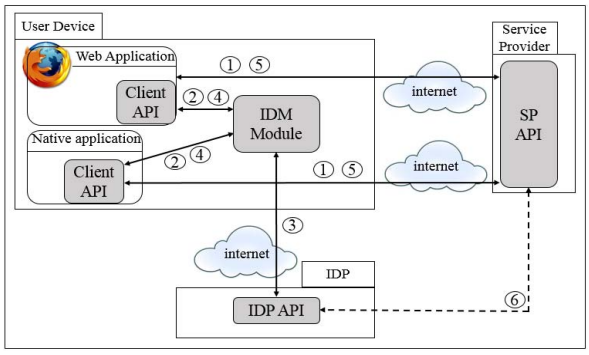


Fig. 1. Architecture overview and the interactions between the different parties in RahasNym. Please refer the text for the details about numbered interactions.

## III. Requirements Addressed by RahasNym

As we have mentioned in Section 1, the requirements expected to be satisfied by a pseudonymous identity management system vary depending on multiple factors. Table I lists the set of key requirements that we have identified and the mechanisms used in RahasNym to address them.

TABLE I
SUMMARY OF KEY REQUIREMENTS AND THE MECHANISMS IN RAHASNYM THAT ADDRESS THEM.

| Requirements | Enabling Mechanisms |
|---|---|
| Ownership assurance of IDTs | -IDTs are bound to user's pseudonyms.<br>-Identity verification is performed via ZKPK.<br>-Biometric identity is attached to IDTs (optional).<br>-Identity of SP is bound to IDTs. |
| Unlinkability | -Unique pseudonym attached to each IDT.<br>-Limited trust placed on IDPs. |
| Confidentiality | -Encoding identity in Pedersen commitments.<br>-Encoding pseudonyms in cryptographic hash based commitments.<br>-Avoiding the storage of secrets in the user device. |
| Accountability | -Getting the IDPs to keep track of all issued IDTs.<br>-In case of a fraud, de-anonymizing the user with the participation of all the related IDPs. |
| Non-shareability of IDTs | -Discouraging shared IDTs by causing the user to share the secrets associated with the IDTs.<br>-Preventing shared IDTs by requiring to attach biometric identity and verifying it. |
| Authenticity of the transaction | -Non-interactive ZKP with signature that binds the transaction with the identity verification. |
| Revocability | -Having IDTs with short time-to-live. |

TABLE II
EXECUTION TIME AND COMMUNICATION SIZE OF PROTOCOLS.

| Steps \Protocol | Protocol 1 | Protocol 2 | Protocol 3 | Protocol 4 |
|---|---|---|---|---|
| Execution time (ms) | 2.945 | 84.257 | 82.148 | 148.48 |
| Communication size | 3.5 KB | 3.5 KB | 3.5 KB | 3.6 KB |

## IV. Conclusion

Based on RahasNym, we have implemented a prototype system which simulates identity verification carried out for different transactions in an on-line shopping portal, as a proof of concept. As reported in Table II, the execution time of the four protocols is in the order of milliseconds and the communication size is few kilobytes. Accordingly, the proposed identity management system can be adopted by existing on-line transactions systems for secure, unlinkable and accountable identity verification, without introducing any significant architectural changes and performance overhead.

## References

[1] M. Honan. (2012, Aug.) How Apple and Amazon Security Flaws Led to My Epic Hacking. [Online]. Available: http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/

[2] D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," in *Communications of the ACM*, vol. 28. ACM, October 1985, pp. 1030–1044.

[3] J. Camenisch and A. Lysyanskaya, "An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation," in *Proceedings EUROCRYPT '01*, pp. 93–118.

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