Inonymous: Anonymous Invitation-Based System

Sanaz Taheri Boshrooyeh and Alptekin Küpçü
Department of Computer Engineering, Koç University, İstanbul, Turkey
{staheri14,akupcu}@ku.edu.tr

ABSTRACT

In invitation-based systems, a user is allowed to join upon receipt of a certain number of invitations from the existing members. The system administrator approves the new membership if he authenticates the inviters and the invitations, knowing who is invited by whom. However, the inviter-invitee relationship is privacy-sensitive information and can be exploited for inference attacks: The invitee's profile (e.g., political view or location) might leak through the inviters' profiles. To cope with this problem, we propose Inonymous, an anonymous invitation-based system where the administrator and the existing members do not know who is invited by whom. We formally prove the inviter anonymity and the unforgeability of invitations. Inonymous is efficiently scalable in the sense that once a user joins the system, he can immediately act as an inviter, without re-keying and imposing overhead on the existing members.

KEYWORDS

Invitation-based system, Anonymity, Unforgeability, Integrity

1 PROBLEM DEFINITION AND MOTIVATION

Invitation-based systems typically consist of a server (i.e., administrator) and a group of members. Each new user can join the system only by obtaining invitations from a certain number of existing members that are called referee or inviter. Afterward, any authentication technique e.g., a password, can be utilized for the further logging into the system.

The motivations behind employing an invitation-based system are the limited number of server resources to serve a rising number of users, improving the quality of services by constraining the number of members, securing the system against fake users, and providing data or service privacy for the system. As a well-known historical example, Google applied invitation-based registration in the early stages of its new services like Gmail, Orkut, and Google Wave [1].

There exists a great privacy concern with the existing invitation-based systems as the identities of the existing members who invite a new user to join the system are in a transparent exposure to the administrator. Some invitation-based systems like Telegram are making this concern tenser by broadcasting the identity of the inviter to all the members of the group that the new user joins. The user's inviters are more likely among the user's acquaintances (e.g., colleagues, home mates, family members, and close friends) who have many common preferences with the user. This enables extracting sensitive information about the newcomer by analyzing the common features among her inviters e.g., location, religious beliefs, sexual orientation, and political views [2, 3].

To make the invitation-based systems privacy-preserving, we propose ***Inonymous*** [4] which is an anonymous invitation-based system. *Inonymous* preserves the inviter's anonymity against both the administrator and the other members.

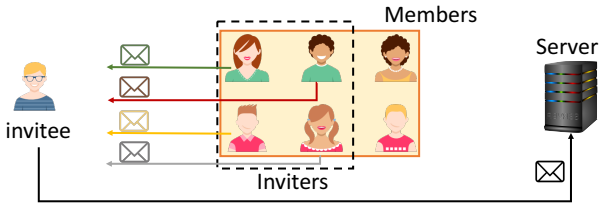

Figure 1: *Inonymous* system overview.

2 INONYMOUS

The system overview of *Inonymous* is depicted in Figure1. The design includes a server, a set of initial members and an invitee (newcomer). The invitee knows his inviters prior to joining the system. He collects and aggregates individual invitations to make a single final invitation letter. Once the newcomer hands over his invitation to the server, the server is in charge to authenticate the invitation and provide necessary information for him.

Inonymous anonymizes the inviters of the same invitee in a symmetric manner with no inviter being able to infer anything about the rest of inviters. Using *Inonymous* the system administrator is still able to authenticate the integrity of user's invitations without the need to know (or even having a way to know) the identity of the issuers. *Inonymous* also secures the system against the malicious invitees who aim to join the system with at least one forged invitation. Furthermore, *Inonymous* provides scalability where it efficiently enables the recently invited users to act as inviters. This is done instantly and without re-issuing the system keys or additional contacting the existing members.

We develop *Inonymous* on two cryptographic tools that are Shamir Secret Sharing Scheme (SSS) and El Gamal Encryption. The server has a secret value S which shares among the initial members by means of SSS. Shares are denoted by s_i. The newcomer is given a token to be used by her inviters in the invitation generation. Using the token, each inviter issues an invitation which is a masked version of her share s_i. The masking value is separately encrypted under El Gamal encryption. The newcomer submits the aggregation of her invitations to the server who authenticates the registration. The security of *Inonymous* is formally proven relying on the robustness and security of the underlying techniques. In the poster presentation, we plan to provide *Inonymous* 's design details, algorithms, and its security proof.

REFERENCES

[1] "http://www.macworld.com/article/1055383/gmail.html."
[2] S. Mahmood, "Online social networks: Privacy threats and defenses," in *Security and Privacy Preserving in Social Networks*. Springer, 2013, pp. 47–71.
[3] A. Chaabane, G. Acs, M. A. Kaafar *et al.*, "You are what you like! information leakage through users' interests," in *Proceedings of the 19th Annual Network & Distributed System Security Symposium (NDSS)*, 2012.
[4] S. T. Boshrooyeh and A. Küpçü, "Inonymous: Anonymous invitation-based system," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 2017, pp. 219–235.