Practical Identity Based Broadcast Encryption for Online Social Networks

Stijn Meul, Filipe Beato, Bart Preneel, and Vincent Rijmen,

Abstract—Nowadays Online Social Networks (OSNs) constitute an important and useful communication channel. At the same time, coarse-grained privacy preferences protect the shared information insufficiently. Cryptographic techniques can provide interesting mechanism to protect privacy of users in OSNs. However, this approach faces several issues, such as, OSN provider acceptance, user adoption, key management and usability. We suggest a practical solution that uses Identity Based Encryption (IBE) to simplify key management and enforce confidentiality of data in OSNs. Moreover, we devise an outsider anonymous broadcast IBE scheme to disseminate information among multiple users, even if they are not using the system. Finally, we demonstrate the viability and tolerable overhead of our solution via an open-source prototype.

Index Terms—identity-based encryption (IBE), broadcast encryption (BE), distributed key generation (DKG), online social networks (OSNs).

1 Introduction

Online Social Networks (OSNs) such as Facebook, Google+, and Twitter are increasingly being used and have become a prominent communication channel for many millions of users. OSNs offer users an efficient and reliable channel to distribute and share information. At the same time, OSNs store large amounts of data which prompts several privacy concerns. In particular, it is possible to infer a considerable amount of sensitive information from the shared and stored content. Currently, users are allowed to configure "privacy preferences" in order to limit and select which users or groups can access the shared content. These preferences are generally too coarse-grained and difficult to configure [?]. Another problem is that these preferences do not exclude the provider along with the dangers of data leaks [?] nor external governments [?].

sm

June 6, 2014

1.1 Problem Statement

All these worrisome issues motivate the need for effective techniques to properly protect user's privacy in OSNs. Several solutions have been proposed and advocated to use cryptographic mechanisms in order to address the privacy issues, either by an add-on atop of existing OSNs [?], [?], [?], [?], or by complete new privacy-friendly architectures [?], mainly decentralized [?], [?]. In general, those solutions suffer from user adoption and key management issues as users are required to register and then share, certify and store public keys [?]. Completely new architectures represent a difficult step for users as the trade off of moving away from the commonly used social ecosystem compared with the risk of losing interactions is high. Arguably, current centralized OSNs are here to stay and will be continue to be actively used by millions of people. In light of recent events, such as Edward Snowden's whistle-blowing on US surveillance programs [?], OSN providers have all interest to maintain their users and a privacy-friendly image. Hence, it is important to protect user's sharing information and the recipient set as it can contain private and sensitive information

Manuscript received April 19, 2005; revised December 27, 2012.

to the user.

1.2 Main Idea

Identity Based Encryption (IBE) [?] solutions overcome the key management problem as the public key of the user can be represented by any valid string, such as the email, unique `id` and username. Therefore, by using a OSN username any savvy and concerned user can share encrypted content with other users who are not using the solution, thereby motivating curious ones to use the system as well. Nevertheless, IBE-based systems require a trusted central Private Key Generator (PKG) server to generate the private parameters for each user based on a master secret. Consequently, such an architecture only shifts the trusted party from the OSN to the PKG. However, this problem can be mitigated if the master secret is divided among multiple PKGs following a Distributed Key Generation (DKG) [?] protocol based on Verifiable Secret Sharing (VSS) [?]. A DKG protocol allows n entities to jointly generate a secret requiring that a threshold t of the n entities does not get compromised. In fact, each entity holds only a share of the master secret, that can be reconstructed by at least t shares.

Many OSN users are not only represented on a single OSN but on several, thus, can also hold multiple public keys. Moreover, the multi-PKG setting could be supported and maintained by several existing OSNs. In particular, collaboration between OSN providers that compete along is assumed to be a difficult task and orthogonal to their economical business model. Figure 1 depicts an overview example of the proposed model, where a user authenticates to t-PKGs of his choice using, e.g., a similar token as in open id protocols, to retrieve his private key. This action can be performed after the reception of encrypted content as a consequence of user curiosity . The PKG servers can also be represented by governmental entities from different continents, with no incentives to collaborate nor overcome more powerful adversaries using legal measures [?] among at least t-PKGs.

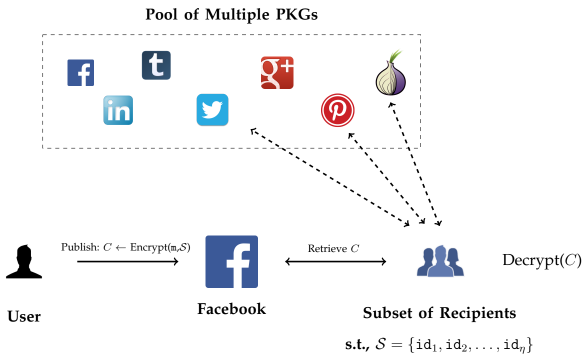
Pool of Multiple PKGs
Publish: $C \leftarrow \text{Encrypt}(\mathtt{m},\mathcal{S})$
Retrieve C
Decrypt(C)
User
Facebook
Subset of Recipients
s.t., $\mathcal{S} = \{\mathtt{id}_1, \mathtt{id}_2, \ldots, \mathtt{id}_\eta\}$

Fig. 1. Multiple (n, t)-PKG IBE for OSNs overview, for a message $\mathtt{m}$ published for the set $\mathcal{S}$ for $t = 3$.

1.3 Contribution:

In this paper, we propose a novel practical solution that uses IBE with multiple untrusted PKGs atop of current OSNs. We highlight the fact that those multi-PKGs can be supported by several existing OSNs under the business competition assumption, and motivated by the possible attractive incentives towards more privacy concerned audience. Along with the multi-PKG IBE model we devise an IBE broadcast encryption protocol to support multiple recipients. Using a broadcast IBE-based mechanism we allow users to share content with multiple recipients, even if they are not using the system, and, thus, enforce confidentiality of the data while hiding the recipient set. Finally, we implemented our solution on top of the Scramble Firefox extension [?], and show that only a small overhead is required.

1.4 Roadmap:

The remainder of this paper is organized as follows. Section **??** gives a brief overview of the cryptographic background. Next, Section **??** presents the model followed by the description of the suggested solution in Section **??**. Section **??** describes the implementation details, while Section **??** reviews related work. Finally, Section **??** summarizes and concludes the paper.

1.5 Subsection Heading Here

Subsection text here.

1.5.1 Subsubsection Heading Here

Subsubsection text here.

2 Conclusion

The conclusion goes here.

Appendix A
Proof of the First Zonklar Equation

Appendix one text goes here.

Appendix B

Appendix two text goes here.

Acknowledgments

The authors would like to thank...

PLACE
PHOTO
HERE

Michael Shell Biography text here.

John Doe Biography text here.

Jane Doe Biography text here.