Computer Communications xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Practical identity-based private sharing for online social networks

Q1 Filipe Beato*, Stijn Meul, Bart Preneel

ESAT/COSIC - KU Leuven and iMinds, Leuven, Belgium

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Online social networks
Privacy
Identity-based encryption

ABSTRACT

Online Social Networks (OSNs) constitute vital communication and information sharing channels. Unfortunately, existing coarse-grained privacy preferences insufficiently protect the shared information. Although cryptographic techniques provide interesting mechanisms to protect privacy, several issues remain problematic, such as, OSN provider acceptance, user adoption, key management and usability. To mitigate these problems, we propose a practical solution that uses Identity-Based Encryption to simplify key management and enforce data confidentiality. Moreover, we devise an Identity-Based outsider anonymous private sharing scheme to disseminate information among multiple users. Furthermore, we demonstrate the viability and tolerable overhead of our solution via an open-source prototype.

1. Introduction

Online Social Networks (OSNs), such as Facebook, Google+, and Twitter present a significant growth 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 as it is possible to infer a considerable amount of sensitive information from the shared and stored content. Although users are allowed to configure “privacy preferences” to limit access and select which users or groups can access the shared content, these preferences are generally too coarse-grained and difficult to configure [1]. In addition, these preferences do not exclude providers along with the dangers of data beaches and leaks [2] nor government. As proved by recent events like the PRISM project [3] and the iCloud breach [4].

All these worrisome issues motivate the need for effective techniques to properly protect user’s privacy in OSNs. Several solutions have been proposed advocating the use of cryptographic mechanisms to address the privacy issues, either by an add-on atop of existing OSNs [5–8], or by complete new privacy-friendly architectures [9], mainly decentralized [10,11]. 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 [12]. Günther et al. [13] formalize cryptographic models for private profile management achieving confidentiality and unlinkability, however their sharing information protocols similar complex key management do not protect privacy of the recipients. 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 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 [3], OSN providers have an interest to maintain their users and a privacy-friendly image. Hence, it is important to protect user’s sharing information, such as text and media content, as well as the identity of the recipients as it can contain private and sensitive information.

Main Idea. Identity Based Encryption (IBE) [14] 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. However, IBE-based systems require a trusted central Private Key Generator (PKG) server to generate the private parameters for each user based on the PKG master secret. Consequently, such an architecture only shifts the trusted party from the OSN to the PKG. This problem can be mitigated if the master secret is divided among multiple PKGs following a Distributed Key Generation (DKG) [15] protocol based on Verifiable Secret Sharing (VSS) [16]. 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 atleast t shares.

Many OSN users are represented on several OSNs, and potentially hold multiple public keys. In this way, the multi-PKG setting could

Q2 * Corresponding author. Tel.: +3216321818.
E-mail addresses: filipe.beato@esat.kuleuven.be (F. Beato), stijn.meul@esat.kuleuven.be (S. Meul), bart.preneel@esat.kuleuven.be (B. Preneel).

http://dx.doi.org/10.1016/j.comcom.2015.07.009
0140-3664/© 2015 Published by Elsevier B.V.

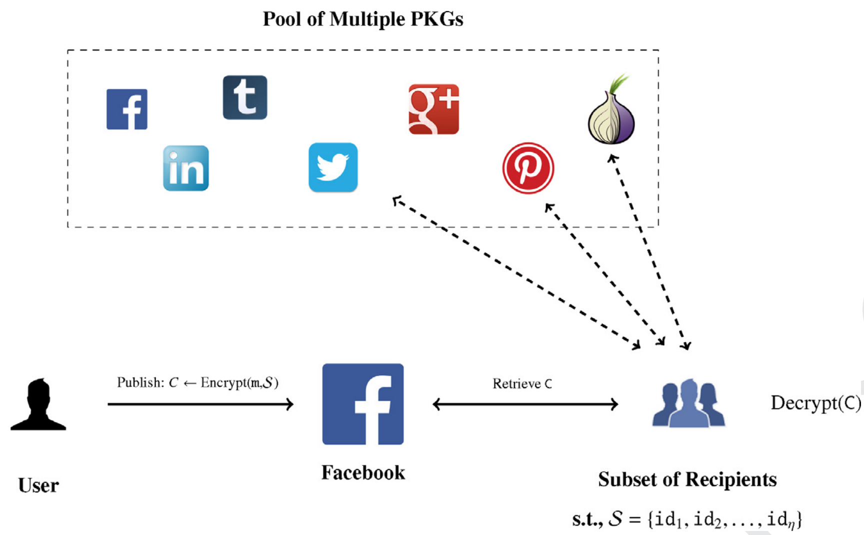

Fig. 1. Multiple (n, t)-PKG IBE for OSNs overview, for a message m published for the set $\mathcal{S}$ for $t = 3$.

be supported and maintained by several OSNs, in particular if considering the collaboration between competing OSN providers to be difficult and orthogonal to their business model. Fig. 1 shows an overview of the proposed model, in which users authenticate to t-PKGs of their choice; to retrieve private keys. This action is performed after the reception of encrypted content. For an additional level of security, PKG servers can also be represented by governmental entities from different continents, with no incentives to collaborate, thus overcoming more powerful adversaries using legal measures [17] that may at least affect t-PKGs.

Contribution. In this paper, we propose a novel practical solution using IBE with multiple semi-trusted PKGs on top of current OSNs. We highlight that multi-PKGs can be supported by several OSNs in view of business competition. We present an IBE broadcast encryption protocol with a multi-PKG model to support multiple recipients. Using a broadcast IBE-based mechanism users can share content with multiple recipients, thus, enforcing data confidentiality while hiding the recipient set. Furthermore, this solution is implemented on top of the Scramble Firefox extension [6], requiring a relatively small overhead.

Roadmap. The remainder of this paper is organized as follows. Section 2 gives a brief overview of the cryptographic background. Next, Section 3 presents the model followed by the description of the suggested solution in Section 4. Section 5 describes the implementation details, while Section 6 reviews related work. Finally, Section 7 summarizes and concludes the paper.

2. Background

In this section we briefly overview the cryptographic tools and building blocks used in this paper. For ease of explanation we omit the definitions of the underlying cryptographic primitives. This section can, however, be skipped with no loss of continuity.

2.1. Identity based encryption

The concept of Identity Based Encryption (IBE) was introduced by Shamir [14], with the main idea of using any string as the public key. IBE requires no certificates as users can rely on publicly known identifiers such as an e-mail address or a telephone number, thus, reducing the complexity of establishing and managing a public key infrastructure. Boneh and Franklin proposed the first practical IBE using bilinear pairings [18], later extended by Gentry [19].

A generic IBE scheme is composed of four randomized algorithms:

$\texttt{IBE.Setup}(\lambda)$: On the input of a security parameter λ, outputs a master secret *msk* and the master public parameters $mpk \leftarrow params$.
$\texttt{IBE.Extract}(params, msk, \texttt{id})$: Takes the public parameters *params*, the master secret *msk*, and an id and returns the private key $sk_{\texttt{id}}$.
$\texttt{IBE.Encrypt}(params, \texttt{m}, \texttt{id})$: Returns the encryption C of the message m on the input of the *params*, the id, and the arbitrary length message m.
$\texttt{IBE.Decrypt}(params, sk_{\texttt{id}}, \texttt{C})$: Reconstruct m from C by using the secret $sk_{\texttt{id}}$ and the public parameters. Otherwise return $\perp$.

The IBE.Setup and IBE.Extract algorithms are executed by a trusted Private Key Generator (PKG) server, whereas IBE.Encrypt and IBE.Decrypt are performed by two players, e.g., Alice and Bob. Consequently, key escrow is performed implicitly in the classic IBE scheme as the PKG holds the master secret key. The correctness property holds with overwhelming probability for all $sk_{\texttt{id}} \leftarrow \texttt{IBE.Extract}(params, msk, \texttt{id}_i)$, such that, $\texttt{m} = \texttt{IBE.Decrypt}(sk_{\texttt{id}}), (\texttt{C} \leftarrow \texttt{IBE.Encrypt}(\texttt{m}, \texttt{id}_i))$.

2.2. Anonymous broadcast encryption

The notion of Broadcast encryption (BE) was introduced by Fiat and Naor [20], as a public-key generalization to a multi-user setting. A BE scheme allows a user to encrypt a message to a subset $\mathcal{S}$ of users, such that, only the users in the set $\mathcal{S}$ are able to decrypt the message. The computational overhead of the BE is generally bounded to the size of the ciphertext and the number of recipients. To overcome the overhead issue, the set $\mathcal{S}$ of recipients is generally known. Barth et al. [21] and Libert et al. [22] extended the notion of BE and introduced the notion of Anonymous Broadcast Encryption (ANOBE) scheme, where the recipient set $\mathcal{S}$ remains private even to the members in the set. Fazio and Perera [23] suggested the notion of outsider anonymous BE that represents a more relaxed notion of ANOBE. Thus, a generic broadcast encryption (BE) scheme consists of four randomized algorithms:

$\texttt{BE.Setup}(\lambda, n)$: On the input of a security parameter λ, generates the public parameters $params \leftarrow (mpk, msk)$ of the system.
$\texttt{BE.KeyGen}(params, i)$: Returns the public and private key (pk_i, sk_i) for each user i according to the *params*.

Please cite this article as: F. Beato et al., Practical identity-based private sharing for online social networks, Computer Communications (2015), http://dx.doi.org/10.1016/j.comcom.2015.07.009