Private Anonymous Messaging With Friends

Ruchith Fernando , Cristina Nita-Rotaru
Department of Computer Science, Purdue University
West Lafayette, IN
{rfernand, crisn}@cs.purdue.edu

***Abstract*—The abstract goes here.**

I. Introduction

We identify a set of requirements in broadcasting messages amoung trusted peers using a peer to peer setup. Then we propose a scheme for contacts of a peer to obtain broadcast updates of the peer using a pull mechnism where the contacts' identities are maintained anonymous. We propose a modification to the hierarchical identity based encryption scheme propsed by Boneh et. al [1] where a peer can request messages of a common peer from another peer while remaining anonymouse.

The following section introduces the setup of the network of peers and how they are connected and the requirements that we try to satisfy with our scheme. This is followed by the preliminary notions and then we describe our solution that meets the stated requirements. Implementation of the proposed cryptographic primitives is presented in section V followed by future directions of this work and conclusion.

II. Problem

A. Background

A peer in this system is a user who has a set of other peers registerd with it as contacts. This peer registration is bi-directional. In other words when peer A becomes a contact of peer B, peer B becomes a contact of peer A.

A peer intends to send messages to all its contacts. All of these messages are to be delivered to the peer's contacts at that point of time. This is similar to the notion of microblogging. (Example: Twitter[2]). Such a message is identified as an $update$.

We demote the a peer generating an $update$ as P and its contacts as the set $C = \{C_{P_i}\}$ where $i \in \{1, ..., n\}$ where n is the number of contacts of P.

B. Requirements

We identify the following requirements in distributing messages in the above system.

- A peer P should be able to simply send its $update$ M_P only to those contacts who are available online at the point of time it sends the update using direct connections to those peers. We denote the set of online contacts as $C^+ \subseteq C$ where $|C^+| \geq 1$.
- Those other contacts of P who were offline at when P sent M_P should be able to obtain M_P when they are available online. We denote these contacts as $C^- \subset C$.
- Any $C_{P_i} \in C^-$ will be able to publish a query requsting an update of P. This is called an update request and is denoted by Q_P.
- Any $C_{P_i} \in C^+$ will be able to publish a response to a Q_P. This response is denoted by S_P and an eavedropper with polynomially bounded resources should not be able to compute the original M_P using S_P.
- The contact who provides S_P should not be able to learn who generated Q_P.
- The contact who generates Q_P and receives the corresponding S_P should not be able to learn who generated S_P.
- When the composition of C changes to new set of peers C', P should be able to update private configuration of the members of C' with the issue of a public message.
- After such an update those peers in the set $C - C'$ should not be able to obtain an $update$ of P.

The scheme we propose in section IV addresses all these requirements.

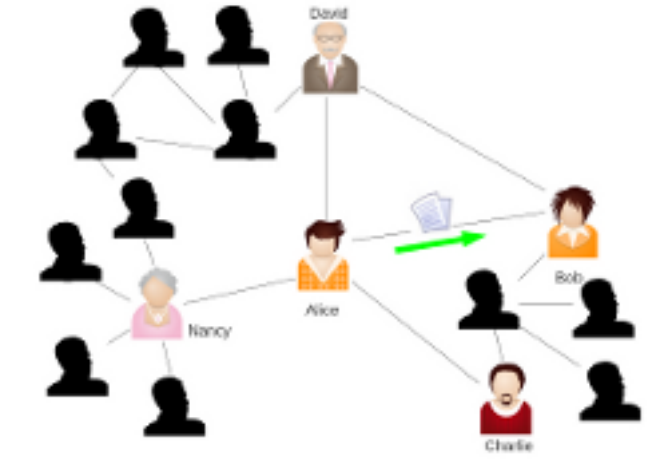

Fig. 1. A user (Alice) and her contacts (Bob, Charlie, David and Nancy)

For example consider figure 1 above. In this situation Alice is P. Alice has four contacts: Bob, Charlie, David and Nancy, out of which only Bob gets the $update$ M_P. Therefore: $C = \{Bob, Charlie, David, Nancy\}$, $C^+ = \{Bob\}$ and $C^- = \{Charlie, David, Nancy\}$. Note that Alice only trusts and has knowledge of her immediate contacts and is not aware of connections between those peers and their contacts.

III. Priliminary Notions

In this section we introduce the necessary background information that our work is based on.

A. Hierarchical Identity Based Encryption

Identity based encryption first proposed by Shamir[3] is a public key encryption scheme where the identity of an entity can be used as the public key. The first complete solution for this was presented by Boneh and Franklin [4]. Any party who intends to send a message to another will simply use a set of public parameters of a trusted authority along with the identity of the recipient will encrypt using this scheme. The recipient of the cipher text will be able to obtain the corresponding private key from the thrid party (who excutes private key generation algorithm for the given identity after authenticating the requester) and decrypt the cipher text to obtain the plain text.

This idea of identity based encryption was extended to a hierarchy of identities [5], [1], where at each level the private key is used as the input to the key generation algorithm along with the global parameteres defined by the root. We modified the scheme presented in [1] to derive our solution and the basic idea is presented as follows.

There are four algorithms: $Setup$, $KeyGen$, $Encrypt$ and $Decrypt$.

- $Setup$
- $KeyGen$
- $Encrypt$
- $Decrypt$

IV. Proposed Solution

Here we present the scheme that addresses the requirements identified in section II.

A. Encryption

Note that in the hierarchical identity based encyrption scheme [1] the plain identity values of an entity are used in generating the cipher text. During the encryption the following value is derived using the identity values of the target.

Identity is simply a random number in the group

B. Re-key

V. Evaluation

VI. Implementation

The proposed scheme was implemented in Java as a library using Java Pairing Based Cryptography [6] library. The demo application developed uses this library in to demonstrate the features of this library. This work available under LGPL at anon-encrypt project hosted in google code [7].

A. Library

Talk about test cases also

B. Demo application

VII. Future Work

TODO Add comparison with broadcast encryption somewhere

Reduce the re-key size

A. Size of re-key information

Currently we generate a minimum amount of information that is required to re-key a peer and its contacts. But in this scheme the re-key informaiton is of order n where n is the number of contacts of the peer. It would be interesting to evaluate the possibility of reducing the size of this public information while maintaining the same properties.

B. Security roof

We plan to prove that an adversary with polynomially bounded resources will not be able to ...??

C. Implementation of message routing

The current implementation only covers the cryptographic primitives. It will be interesting to use these with a peer to peer network where the peers are connected only to their private contacts and evaluate the performance. It might be possible to be implemented as a plugin to Freenet [8].

VIII. Conclusion

The conclusion goes here.

References

[1] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Ronald Cramer, editor, *Proceedings of Eurocrypt 2005*, LNCS. Springer, 2005.

[2] Twitter. http://twitter.com.

[3] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 47–53, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[4] Dan Boneh and Matthew Franklin. Identity-based encryption from the weil pairing. *SIAM J. Comput.*, 32:586–615, March 2003.

[5] Jeremy Horwitz and Ben Lynn. Toward hierarchical identity-based encryption, 2002.

[6] The Java Pairing Based Cryptography Library (jPBC). http://gas.dia.unisa.it/projects/jpbc/.

[7] Project anon-encrypt at Google code. http://code.google.com/p/anon-encrypt/.

[8] Freenet. http://freenetproject.org/.