Ran Zhao

Weekly Report I

Date: September 19th, 2012

Summary

During the first week, I read several related papers to gain the background knowledge. Meanwhile, I discussed with Professor Ford and David about my project proposal. The proposal is an extended abstract and I will improve it with the project progress.

Reading List

1. *Dissent: Accountable Anonymous Group Messaging* (Henry Corrigan-Gibbs and Bryan Ford)
2. *Identity-based Cryptosystem and Signature Schemes* (Adi Shamir)
3. *Identity-Based Encryption from Weil Pairing* (Dan Boneh and Matthew Franklin)
4. *Faceless: Decentralized Anonymous Group Messaging for Online Social Networks* (Xiaoxiao Song, David Wolinsky, and Bryan Ford)
5. *An Identity Based Encryption System* (Louise Owens, Adam Duffy and Tom Dowling)
6. *Practical Implementation of Identity Based Encryption for Secure E-mail Communication*
7. *The OAuth 2.0 Authorization Protocol* (Released by Facebook)
8. *Linkable Ring Signatures: Security Models and New Schemes* (Extended Abstract)(Joseph K.Liu and Duncan S.Wong)
9. *The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability* (David Chaum)
10. *How to Leak a Secret* (Ronald L. Rivest, Adi Shamir and Yael Tauman)
11. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* (RSA)
12. *Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms* (David L. Chaum)
13. *Verifiable Mixing (Shuffling) of ElGamal Pairs* (C. Andrew Neff)

Ran Zhao

Proposal (Extended Abstract)

Part I. Define problem and Task

I intend to practically implement of Identity-based Encryption for social network anonymous group messaging. The target social network website is Facebook. As the first step, I will take the whole social network of Facebook as a big social group and consider the group division or aggregation later. Before building a real decentralized system, I assume the PKG(private key generator) server is trustworthy. Basically, there are six challenging tasks:

(1) Design the protocol between social network server and PKG server.
(2) Implement the IBE schema (Depends on the PBC and GMP library).
(3) Connect the IBE with Facebook.
(4) The way of public key distribution
(5) The way of private key storage
(6) User Interface of IBE application

Part II. Protocol prototype

Step1: The client should access the PKG server by login with Facebook Connect.

Step2: Facebook will authorize the client identity to our PKG server (third party).

Step3: After authorization, Facebook server will send us the basic information of the client(including unique FacebookID) and his social graph (friend-list).

Step4: We will create a “contact book” for client to store his friends’ public keys.

Step5: We will search on client Facebook social graph and collect his friends who had registered on our application, putting their FacebookIDs(as public key) to his contact book. Then the sever will send the request to each of his registered friends to update their contact book.

Step6: Client will automatically send the request to the PKG server to request his private key with his FacebookID.

Step7: The PKG server will generate the private key for the client. The private key will be transmitted through a secure channel and the client should store the private key in an appropriate place (The place should be resolved during the research).

PartIII. Future work

(1) In order to make the PKG server more trustworthy, I intend to improve it by using multi-server. Thus, I should design a schema to make the multi-server collaborate to generate the private key.
(2) Social group division or aggregation.