Ran Zhao

Project Proposal

--- Build a Distributed PKG server

Introduction

In practical, people always use PKI to generate the public/private key for message encryption. This infrastructure requires the recipient's certification from CA. Thus, it provides a very strong authentication of user. However, there are several obvious disadvantages. Firstly, senders and recipients should be pre-enrolled before sending and receiving the message. Secondly, the certificate directories may possibly leak the important information. Thirdly, the sender should obtain and check the recipient's certificate status before sending the message. Fourthly, the key recovery is difficult and costs long time.

To avoid all of those disadvantages above, I consider using the Identity Based Encryption instead of PKI. On IBE system, there is a PKG server, which is in charge of generating the private key for the user. The sender does not need to collect the certificate and could use any arbitrary string as the public key of recipient. When the recipient receives an encrypted message, he only needs to authorize himself to PKG server with his ID and requests his private key. Then the PKG server will generate the corresponding private key for the user based on his ID. Comparing to the PKI, it has several obvious advantages. Firstly, it does not require the user to pre-enroll. Secondly, it extends messaging to all users, even with the users who does not have certificate. Thirdly, it makes the key recovery process easy by making the request to the PKG server. Fourthly, it does not require the sender to check the certificate status of recipients and supports the off-line capability.

Statement of Problem

As I choose to use IBE to generate the private key for the users, I intend to build a distributed PKG server. On IBE system, I firstly assume that the PKG server will be trustworthy, which plays a role of a CA in PKI. I integrate the IBE system with a social network, which could help IBE system to authorize the user identity and provide each user a unique public key. For an example, every time when the user makes a request for the private key, he should authorize himself to the PKG server by using a social network authorization API. In my project, I choose Facebook as my target social network website. However, I intend to reduce the risk of this kind of "trust" by making a distributed PKG server. I split a single PKG server into multiples, which will more or less reduce the centralized trust of the server.

Object Design

(1) Design private key pick up protocol for single version PKG server.
(2) Implement a single version PKG server.
(3) Design private key pick up protocol for multiple PKG servers.
(4) Make the PKG server distributed.

Technique approach and challenge

- Firstly, in single server private key pick up protocol, I intend to use facebook authorization API to authorize the user for PKG server. Then after the server gets the user Facebook access token, it will generate the private key for him and send it through a secure channel.

- I intend to implement the single server IBE system based on the Boneh-Franklin scheme. I intend to choose C as my primary language and include GMP library and PBC library, which will be able to generate the elliptic curve for the bilinear map.

- After the PKG server is split into multiple, I am facing a technique challenge of combing the multi-authority IBE system with single-sign-on system. Thus, I should make a new private key pick up protocol for multiple PKG servers.

- Make the multiple PKG servers work together to generate the private key for the users.

Project Management

Deadline: I intend to finish this project by December 10th, 2012.
Timeline with milestone:

(1) Design private key pick up protocol for single version PKG server, complete date : October 3rd.
(2) Implement a single version PKG server, complete date: October 22nd.
(3) Design private key pick up protocol for multiple PKG servers, complete date: October 31st.
(4) Make the PKG server distributed, complete date: November 28st, 2012.
(5) Write a small project demo and finish the project report, complete date: December 10th, 2012

Future work

I intend to integrate the IBE system with the Dissent project. The first step o fthe future work should be developing IBE version linkable ring signature scheme and give a proof.