Security in ChronoShare

Yukai Tu (ytu@cs.ucla.edu), Zhiyi Zhang (zhiyi@cs.ucla.edu)

Motivation

Different with most of today's file sharing applications, which resort to a centralized design paradigm, ChronoShare is a completely decentralized distributed file sharing application builds on top of the Named Data Networking(NDN) architecture. Users synchronize their knowledge about files information through ChronoSync [17], a distributed synchronization protocol over NDN. Using ChronoSync, users exchange their knowledge about the file state digest through an interest, called sync interest. And fetch the actions and corresponds files through request Interest. In ChronoShare, both sync replies and information request need to be secured. If sync replies are not secured, an attacker may force users to fetch malicious data from a fake user. If information request are not secured, attackers can easily launch impersonation attack. File access control is also an important security part in ChronoShare. For better usage purpose we need to implement security part in ChronoShare.

Contribution to NDN

As an important application over NDN, we hope ChronoShare can be released and be really used in real life. To serve this purpose, the ChronoShare should be implemented with security. We believe that the widely used application can make people more willing to accept and use NDN, and ChronoShare will be one of that kind of application.

Tasks

First the ChronoShare may need user authentication module. Since we use the same concept with ChronoChat, we need to first ensure the group initiator can authenticate people into group and information can only be shared within the group. The attacker without certificate can't no share malicious data with group and can not affect the group information sharing. For data level, when users require the secure data transmission, the data encrypt is also needed in ChronoShare. Furthermore, the file access control can be introduced and guarantee the file permissions for certain users.

Required Knowledge for Participants

The ChronoShare is implemented in C++, compiled by waf script. The whole communication model is implemented in NDN so the participants need basic knowledge about NDN. For detail about ChronoShare, refer to Technical Report of ChronoShare. Currently we plan to use Endorsement-based Key Management System Module for ChronoShare. For detail about Endorsement-based Key Management System Module, refer to Technical Report 23.

Expected Outcome

At the end of the Hackathon, we expect the basic group authentication is implemented, which means when initiator create and invite the specific devices into group, the devices without permission can't access to the content. Follow up the directory access control can also be implemented, which means only the devices don't given access to a certain directory can't make any change on that to all group members.