Rutgers CS 419 Group Project Report

xh195 & ql169 & lt457

December 5, 2021

1 Problem Description

1. What is the goal of this project? (functionality of this artifacts)
   - To build a database that can be managed by assigned permissions.
2. Where will this program be deployed or used? (platform, users)
   - It is designed for small size organizations that need to manage their data and want to prevent information leakge. Those company need to have their data stored and make sure people who does not have permission can not view it.

2 Problem Analysis

1. What is the threat model? Attackers' knowledge, capability and goals?
   - Because this is a local database that is designed for small organizations, we will consider less from the online attack. We will assume that the attackers are people who try to login by decryping the password, or people who have username and password by chance and want to destroy the database. The hacker would sneak into the company and try to download and delete the secret file. Also the hacker would try to delete members to make chaos.
2. What is the security goal and guarantee?
   - The goal is to make sure the leader has the ability to restore the file, add the members back. The most important thing is to make sure the encrypted file downloaded by the hacker can not be decrypted.

3 Program Design

1. How did you achieve your goal? functionality and security.
   - The system works by hierarchy (Leader, Manager, member...). People with higher positions would have higher permissions.
     (a) Member
         - Read
         - Require Permissions

     (b) Manager
         - Read
         - Edit
         - Download
         - Fire member
         - Give out permissions
         - Require Permissions

     (c) Leader
         - Read

- Edit
- download
- Add member
- Fire member
- Give out permissions
- Demote co-leader to member
- Promote member to co-leader
- Sync
- Restore

2. How can it provide the security guarantee you intended?
   - The hacker who is promoted to co-leader would use the download permission to download the encrypted file and edit permission to delete the file. Then he would delete all the members in the company to make chaos.
   - At this time, the leader would use the restore permission to copy the backup file to the main file. Also, he would use the add permission to add all the members back.
   - When the hacker gets the encrypted file, he would find it is encrypted by multiple IND-CPA so that he has no way to decrypt it.
   - Of course, the leader would demote the hacker to a member and fire him.

```
Read = False
Edit = False
Download = False

Member = ["Bob","Alice"]
CoLeader = ["TheMan"]

def checkForDomian (Username):
    name = Username
    if name in Member:
        Read = True
    elif name in CoLeader:
        Read = True
        Edit = True
        Download = True
    return

def text():
    modifiedTime = 10
    filename = "Tempfile"

def storedtext():
    syncTime = 10
    filename = "sync"


def Sync():
    if text.modifedTime != storedtext.syncTime:
        #Copy Tempfile to sync
        return
```

4 Evaluation

4.1 Evaluation Strategy

What and how to evaluate? platform, datasets, user study?, how to measure, effectiveness, efficiency, security

- We will use Python or java to evaluate the program to prevent attacks that is based on the lack of memory management in lower-level language. JSON is considered to be used as data file. We will set up all kinds of authority check when doing every operation to make sure that every user can do what they are allowed to do.

4.2 Experiments

How do you plan to do or design the experiments?

- We will try to delete infromation from data file and see if we can restore it from sync file
- We will try to ask permission as one member and use the permitted code as the other member.
- We will test if the username, password system can be hacked

4.3 Results

What are the results?

- All the test were passed.

4.4 Analysis

What do these results mean?

- It means that the attacker can only login to the system with paired Username and Password, and it is hard to guess the password. When he/she is logged in, they can only do what they are allowed. Even if the attacker find a username and password of coleader and randomly edit the data file, we can still restore it from the sync file.

5 Group and Artifacts

- Group members and each of their contributions in %.
  - Leader
    - Xijun Huang(xh195): Program: 37% Bug: 40%
  - Member
    - Qihan Lu(ql169): Program: 37% Bug: 40%
    - Le Tao(lt457): Program: 26% Bug: 20%
- Project repository address.
  - https://github.com/QihanLu/CS419.git
- Video Link
  - `https://drive.google.com/file/d/1Kdo_CXkOT5KhOPuBMovksZE7THbDSBdv/view?usp=sharing`
- What is proud part of this project, for each of you?
  - Everyone is using what they know trying to make the work done.

6 Bug Hunting

- Issue Links

Repo	Owner	Issue
https://github.com/sagjig/secure-image-vault	sagjig	https://github.com/sagjig/secure-image-vault/issues/2
https://github.com/sagjig/secure-image-vault	sagjig	https://github.com/sagjig/secure-image-vault/issues/3
https://github.com/sagjig/secure-image-vault	sagjig	https://github.com/sagjig/secure-image-vault/issues/4