Ransom-Aware

Ransomware-resistant remote documents

Group A37:
Diogo Ravasco - 89434
João David - 89471
Daniel Gonçalves - 91004

Motivation

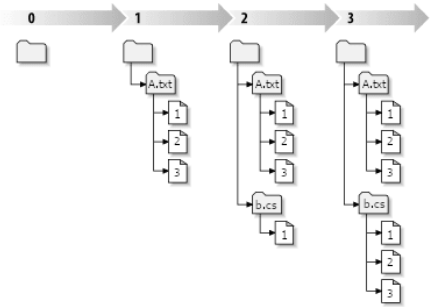
Collaborative application that allows:

- Storing files remotely through a unsecure network and a untrusted server in a secure manner
- Granting and revoking access to other users
- Resistance to Ransomware attacks

Goal

As such we need a document sharing application that ensures:

- User authentication and authorization
- File confidentiality and integrity
- Version history with backups to protect against threats to the main server



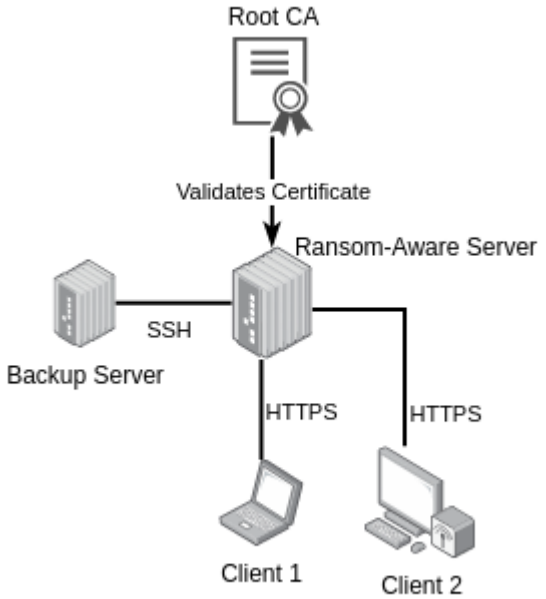
Architecture Overview

Four main components:

- Root CA
  - A simple self-signed certificate
- Server
  - Handles clients' requests
- Backup server
  - Defense against threats to the main server
- Client

Communication channels:

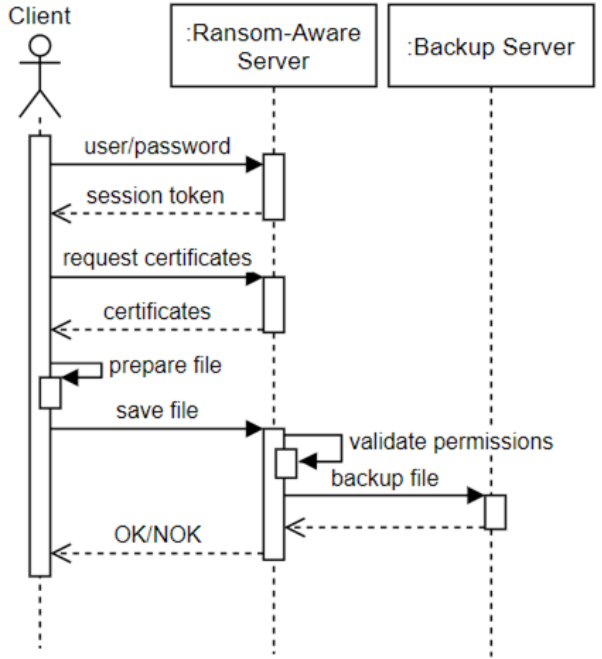
- Client-Server over HTTPS, user and password
- Server-Backup over SSH, public key authentication



Usage Example

Typical interaction between client and server, login and save file command:

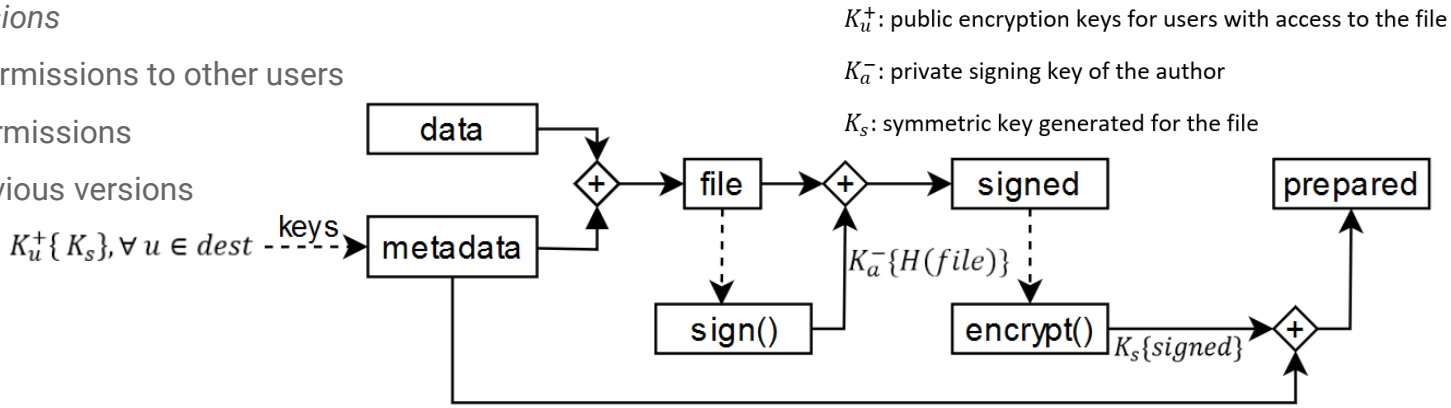
- Client sends login request
  - If authenticated, receives a session cookie
- Requests the certificates of all users with file access
- Sends ciphered file alongside ciphered symmetric keys
- Server validates user
  - If validated save file to backup server
  - Return to user



Client Overview

Client allows the user to:

- *List files*
- *Save* a file in the server
- *Get* a file from the server
- *List file permissions*
- *Grant* author permissions to other users
- *Revoke* said permissions
- *Rollback* to previous versions



Server Overview

When a client registers:

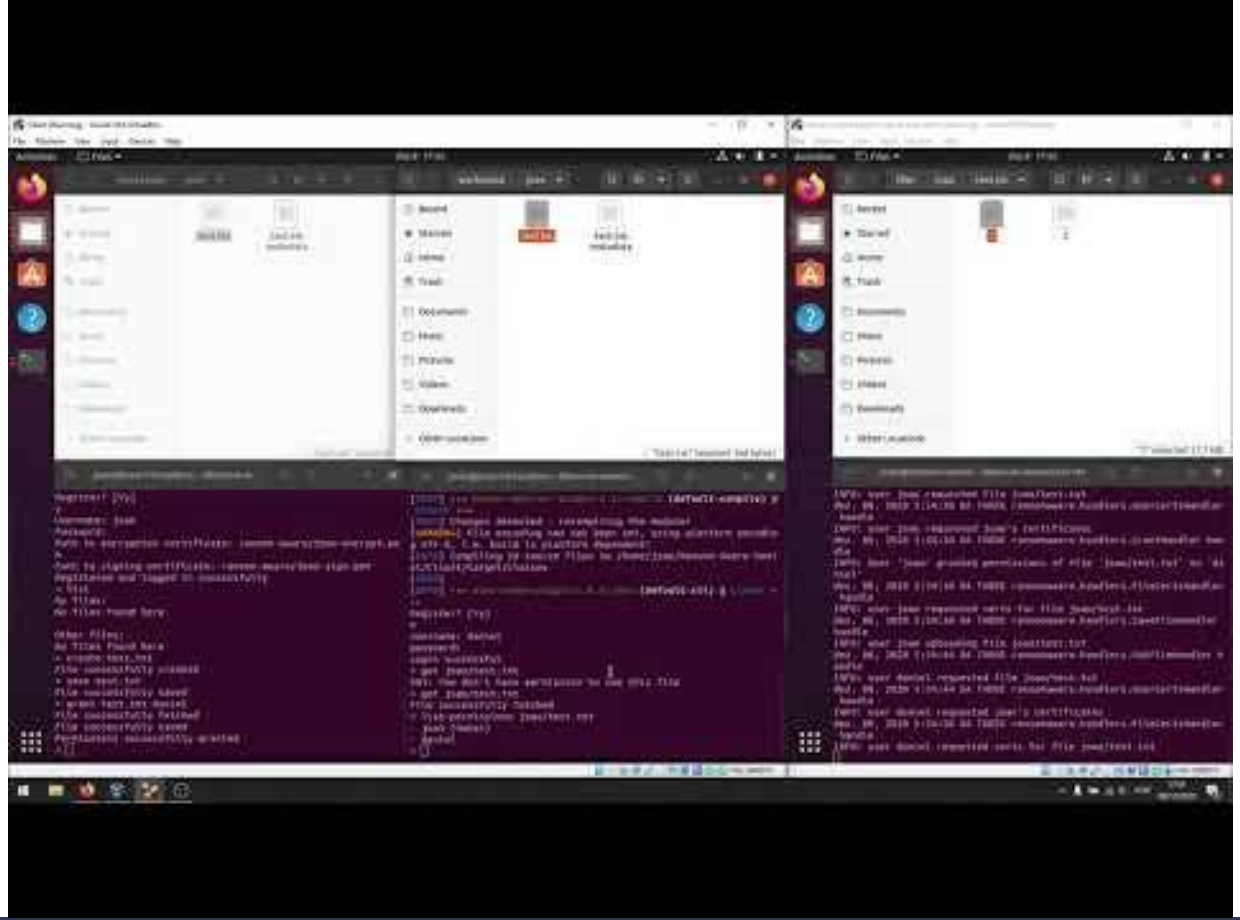
- His password is salted and hashed and kept in a database
- His username and certificates, encryption and signing, are kept in a database as well

Server issues a random token when a client logs in, in order to manage their session, and authenticate further requests

Files are stored in the local filesystem, with the structure on the figure


```
{
    "data":"Y1UNJxIL5Nib...",
    "info":{
        "keys":{
            "daniel":"ilIyIZypn...",
            "joao":"g4NFtcaEdJu..."
        },
        "iv":"bHFecN4UrLbfZN6nfW0G/w==",
        "author":"daniel",
        "timestamp":"2020-12-10T17:36:58.791707Z"
    }
}
```


How a file is stored in the server file system



Video Demonstration