CSE471 Information Systems Security (2020 Spring)

Report of the Project:

Prototype of Encrypted File Storage System on Cloud with Authentication Support

Main idea of the project is all encryption and decryption processes are made on client side. Therefore, server can never see content of file stored.

As no student project can compete with a real-world security project, this one can be considered as just prototype too, with many flaws and missing features.

Project has been developed on C# language. 1 visual studio solution consist of 3 projects which means 3 executables: client, authentication server and file server.

Servers have got multi-client support, but ports must be configured manually.

Usernames and passwords are held as hashed (SHA256) on authentication server.

Each user has got private space in file server. Considering, encryption password should be generated from user password, leak of encrypted files is not a big worry.

Even if 'logIn' form is bypassed, still files on file server cannot be accessed. Because, file server will validate authentication through authentication server. Therefore, if client has not got valid authentication TokenId, access to file server will not be possible.

Standard TCP sockets are used. That means, connections can be easily sniffed by an eavesdropper. Identity of any party (client and servers) can be copied and session hijacking can be done easily. In a nutshell, **TLS protocol with a secure implementation** is a must in a real-world implementation.

A static password is used for all encryptions. In a real-life project, encryption password should be generated from both user log-in-password and hardware-based password generator. Any kind of software-based password generation is not secure.

To sum up, this is just a prototype. You may see the result of work from user side in the links below:

Multi-Client Support Demo: https://www.youtube.com/watch?v=K7b9gbDSHZo
Encryption, Decryption Demo: https://www.youtube.com/watch?v=yNo9w3pNCfc

Tahir Özdilek