

Secure Design of Client Server Network in FTP

Swapnil S. Jagtap¹ Nakul A. Mali²

^{1,2}Department of Computer Science & Engineering

^{1,2}Dr. Daulatrao Aher College of Engineering, Karad – 415110

Abstract— The File Transferring Protocol (FTP) has already been widely used for many years. However, there exist some secure vulnerability in the protocol. For example, both passwords and files are transmitted in plaintext. Although some new FTPs such as FTPS (File Transfer Protocol Services) have been proposed and applied to overcome these vulnerabilities, there are many drawbacks such as lack of flexibility in use, failing to meet specific security requirements. Given these facts, the FTP and its requirements are studied deeply and a new ‘SCSN’ (Secure Client Server Network) system. A new SCSN system is proposed based on combination of dynamic password, face recognition, thumb recognition technology as well as the hash function and symmetric key algorithms and etc. to achieve its high security and efficiency. The security level selection mechanism is adopted to meet individual security requirements. The resource access control mechanism is used to keep the server from unauthorized access attacks. Analysis shows that compared with existing FTP systems, the new system makes not only data transmission securer but also system in use easier, more flexible and efficient.

Key words: FTP, SCSN, face recognition

I. INTRODUCTION

The Secure Client Server Network in FTP provides best security in client server network. The main idea behind this project is providing security. There are several security policies are used as face recognition, thumb recognition, dynamic password mechanism and encryption and decryption techniques, as well as access of only particular drive or folder is given by server to user. The server stores information of clients at the time of registration in the database which contains Password, Face image and thumb impression.

The system allows only authenticated users in the network, for authentication purpose Server allow user to login in the network if and only if his password, face image and thumb impression match with the face image and thumb impression in the database. So unauthorized user cannot enter in the network.

After user login is completed data transmission performed in the encrypted format. Client (sender) sends data in encrypted format by using encryption algorithm and another client (receiver) receives that encrypted data and converts it into the original message with the help of decryption algorithm. So data cannot be modified in the network easily by any other user.

II. RELATED STUDY

The original specification in FTP [1] is an inherently insecure method of transferring files because there is no method specified for transferring data in an encrypted fashion. This means that under most network configurations, user names, passwords, FTP commands and transferred files

can be captured by anyone on the same network using a packet sniffer (particular types of network).

The general solution is to use either FTP over SSH (Secure Shell) protocol which brings SSH encryption into FTP system, or FTPS (FTP over SSL) which brings SSL encryption into FTP system [2]. Although they can overcome the fatal weakness of data transmission in plaintext, there are still some disadvantages, such as data connections security, system cost and meeting specific security requirements etc. FTP over SSH uses multiple TCP connections, which is particularly difficult to tunnel over SSH [3]. For SSH clients, attempting to set up a tunnel as the control connection will only protect that connection; when data are transferred, the FTP software at either end will set up new TCP connections (data connections) which will bypass the SSH connection, thus saving no confidentiality, integrity protection and etc. FTPS is an extension to FTP that adds the support for Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.

However, it relies on TLS and SSL security protocol at the transport layer, which cannot meet specific security requirement, such as flexible security level selection and resource access control and etc. And secure authentication and information transmission implemented by a credible third-party, certificate and public key cryptography will add more complexity and burden to the system. At present, the reference material on safety of FTP is limited. Reference [4] and [5] proposed a secure FTP system, which adopted the public key cryptography mechanisms to solve the secure certification and transmission. Asymmetric key algorithms are generally much more computationally intensive than symmetric key algorithms, which are typically hundreds to thousands of times slower than symmetric key algorithms in practice; it takes a more expensive computational cost to achieve their solutions.

We propose a new ‘SCSN in FTP’ (Secure Client Server Network in FTP) system based on combination of dynamic password, face recognition, thumb recognition as well as the hash function and symmetric key algorithms and etc, to achieve its high security and efficiency.

III. LITERATURE SURVEY

Now a day there are many protocols available in the network for the transmission of data but they does not provide the sufficient security for the transmission of data. As well as detecting authorized users is quite difficult in the network, there are no any specific way for the detection of authorized users.

Survey of papers given as in reference, the data is not secure in transmission because data is transmitted in the form of plain text & that’s why unauthorized person easily access the data. Any person who knows the password can login into the network and can do misuse of the information.

To provide the security to the data transmission and user authentication a system needs Secure Client Server Network in FTP (SCSN in FTP).

A review of literature indicates that Secure Client Server Network in FTP (SCSN in FTP) can be required now a days.

Normal client server network in FTP transmits passwords and files in plaintext, which lacks an effective identity authentication and a secure transmission mechanism. Once the important information is leaked out, it will result in great damage and harm to users, especially for such users as government and enterprises who need higher security.

SCSN in FTP system combines dynamic password mechanism, secure transmission mechanism, face and thumb recognition and resource access control mechanism to achieve a secure and more efficient FTP communication system.

IV. PROPOSED WORK

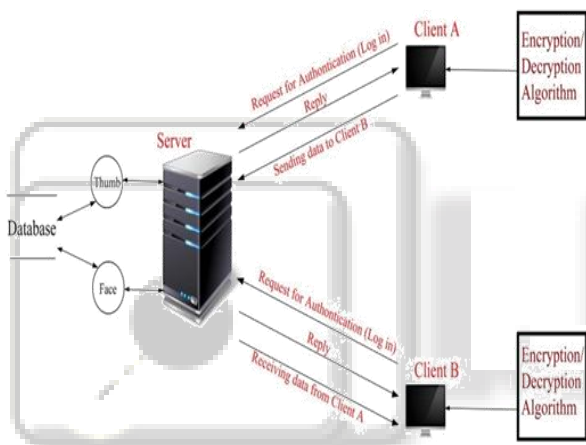


Fig. 1: Architecture Diagram

Before logging into the system, one user needs go to a trusted authority center to submit personal registration information, then the authority center will give the user a user ID, password face image, thumb impression, etc. When a registered user logs into the system, he enters the user ID, password, face image, thumb impression, then waiting for authentication. If his identity is legitimate, the system will provide him service.

A. Registration Process:

- User submits his personal registration information to authority center.
- Authority center verifies the information and stores it in the database if it is unique. Among this information, password is stored as hash password instead of itself, which makes it more difficult for an intruder to get the real passwords.
- Authority center will generate a user account on the server.
- User ID, password will be given to the user.

B. Authentication Process:

When a registered user logs into the system, he needs to insert the user ID, password, face image, thumb impression.

Then the system starts the FTP client software and begins a mutual authentication. The process is as follows:

- Client sends user ID, password and other information to the server to log into the system.
- All the information of the client is send to the server in encrypted format.
- Server compares the information of the user to the information stored in the database.
- If the user's identity is verified successfully, then the user session is started.
- If the user's identity is mismatched, the system will warn the user that this authentication has failed and break the session.

C. Secure Transmission Process:

After the mutual authentication, the session goes to the secure transmission process by using data compression, data confidentiality and data integrity mechanisms.

D. Comparative Study:

1) File Transfer Protocol (FTP):

- In FTP Username & Password is subsequently transmitted in plaintext format.
- In FTP the connection transferred data is could not intended final destination securely.
- Low speed in file transfer.
- End-to-end connectivity but low security.

2) Secure Client Server Network (SCSN) in FTP:

- In SCSN user name & password is subsequently transmitted in encrypted format.
- In SCSN the connection transferred data intended the final destination and to provide the higher security.
- High speed in file transfer.
- End-to-end connectivity and high security.

V. CONCLUSIONS

We introduce the disadvantages of traditional FTP communication systems and compare the related work. Then we propose a new SCSN (Secure Client Server Network in FTP) system by using dynamic password mechanism, security level selection mechanism, resource access control mechanism and face and thumb recognition. The security and efficiency analysis shows that the new system makes not only data transmission secure but also system in use easier, more flexible and efficient.

REFERENCES

- [1] RFC-959 J. Postel, J. Reynolds, ISI, "File Transfer Protocol (FTP)" Oct 1985. Available: <http://www.ietf.org/rfc/>
- [2] RFC 4217: P. Ford-Hutchinson, IBM UK Ltd, "Securing FTP with TLS" Oct 2005. Available: <http://www.ietf.org/rfc/>
- [3] RFC 4251: T.Ylonen, T. and C. Lonvick, Ed. Cisco Systems, Inc, "The Secure Shell (SSH) Protocol Architecture" Jan 2006. Available: <http://www.ietf.org/rfc/>
- [4] Y Ma, H. T. Liu, B. Y Cai, "Design and implementation of a secure FTP system" Applications and Software, Aug 2007.

- [5] W C. He, Y. Y. Zhang, P. H. Liu. "Research and design of a computer encryption communication system based on secure FTP" Network Security Technology and Application, Jan 2007.
- [6] B. Wang, Y. Y. Zhang, "Analysis and amendment of one-time password authentication scheme" Computer Engineering, July 2006.
- [7] N. Wang, X D. Qiu, P Luo, "One-time password scheme based on hash function and public key encryption" Application Research of Computers, Feb 2009

