FILE TRANSFER PROTOCOL(FTP) MANAGER

Devashish Tomar[1], Devesh Shukla[1] , Harshit Kumar[1], Ravi Gupta[2]

[1]UG STUDENT, Information Technology, IMSEC ,UTTAR PRADESH , INDIA
[2] Faculty Information Technology Departm , IMSEC,UTTAR PRADESH , INDIA

ABSTRACT

File Transferring Protocol (FTP) has been extensively used for many years. Despite, there occur some vulnerability in the protocol. For Example, the passwords, files, and other confidential data are transmitted in unencrypted form that is in plaintext. Albeit some new FTPs like FTPS (File Transfer Protocol Services) have been recommended and are been used to overthrown the known vulnerabilities, there are many flaws, such as lack of tractability in use, unable to meet unequivocal security requirements. Given these fact, the FTP and its prerequisite requirements are studied rooted and a new 'SCSN'(Secure Client Server Network) system. A modern SCSN system is recommended upon combination of dynamic password, face recognition, thumb recognition technology as well as hash function and symmetric key algorithms and etc. to obtain its high efficiency and security. The security level selection mechanisms ratify to meet each and its own security requirements. The resource access control mechanism is used to prevent server from unauthorized access attacks. Analysis shows that compared with previous and existing FTP systems, the new system makes not only data transmission but also system in use user friendly, more tactile and efficient.

Watchwords: FTP, SCSN, Face recognition, SSL, TLS, SSH, SFTP

1. INTRODUCTION

The Secure Client Server Network in FTP adds best security in client server network. The main idea behind this project is providing security. There are many security assurance policies are used as face recognition, thumb recognition, dynamic password mechanism and cipher text and plain text techniques, as well as access of only particular drive or folder is given by server to user. The server keeps information of sender at the time of registration in the database which contains Password, Face image and thumb impression. The system grants authenticated users in the network, for authentication intent, Server allow user to sign in in the network if his password, face image and thumb impression match with the face image and thumb impression in the database. So no other unauthorized user cannot access the network. After login data transmission operated in the encrypted manner. Client (sender) sends data in encrypted manner through applying encryption algorithm and another end client (receiver) receives that encrypted data and transforms it into the original massage through applying given decryption algorithm. In order to prevent data alteration in the network easily by any other user.

2.RELATED STUDY

The description in FTP [1] is an utterly insecure way of transferring files because there is no method specified for transferring data in an encrypted manner. This means that on the underneath of most user names, passwords, network configurations, FTP instructs and transmit files that can be tapped and stole by anyone that can harm the integrity of file on the same network using a packet sniffer. The most obvious and laically solution is to use either FTP over SSH (Secure Shell) protocol which brings SSH encryption into FTP system, or FTPS (FTP over SSL) which induces SSL encryption into FTP system [2]. Albeit they can overthrow the fatal weakness of data transmission in plaintext, there are still some disadvantages, such as data connections security, system cost and pricing, meeting specific security requirements etc. FTP over SSH uses multiple TCP connections, which is particularly difficult to tunnel over SSH [3]. For SSH clients, endeavouring to set up a tunnel as the control connection will only protect that connection; when data are transmitted, the FTP software at either end will establish new TCP connections (data connections) which will intern outflank the SSH connection, thus further enhancing confidentiality, integrity protection and etc. FTPS is an expansion to FTP that enumerate the backing for Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.

However, it entrusts on TLS and SSL security protocol at the transport layer, which cannot meet unequivocal security requirement, such as tactile security level selection and resource access control and etc. And secure authentication and information transmission implemented by a trustworthy third-party, certificate and public key cryptography will add more complexity and hardship to the system. At present, the reference material on safety of FTP is limited. Reference [4] and [5] proposed a secure FTP system, which ratified the public key cryptography mechanisms to clarify the secure certification and transmission. In most cases asymmetric key algorithms are much more computationally comprehensive than symmetric key algorithms, which are hundreds to thousands of times lethargic than symmetric key algorithms in practice; it takes a much higher and unreasonable computational cost to resolve their solutions. We introduce a new 'SCSN in FTP' (Secure Client Server Network in FTP) system based on consolidation of dynamic password, face recognition, thumb recognition as well as the hash function and symmetric key algorithms and etc. to resolve its high security and efficiency.

3. LITERATURE SURVEY

In modern era, many protocols are available in the network for the successful transmission of data but they do not administer the required and enough security for the transmission of data. As well as identifying authorized users is quite troublesome task in the network, there are no any recognized way for the identification of authorized users. Inspection of papers given as in reference, the data is not secure in transmission because data is transferred in unencrypted manner(plaintext) & that's why unauthorized user can easily approach and access the data. Any user who knows the password can sign in into the network and can alter and misuse the information.

To grant the security to the data transmission and authentication, a system requires Secure Client Server Network in FTP (SCSN in FTP). A review of literature demonstrates that Secure Client Server Network in FTP (SCSN in FTP) can be needed now some days. Normal client server network in FTP transfers passwords and files in unencrypted manner(plaintext), which deficits a reliable and good identity authentication and a secure transmission mechanism. Once the important information is compromised, it will do vast damage and loss to users, notably for such users as government and enterprises who requires higher security. SCSN in FTP system bind dynamic password mechanism, secure transmission mechanism, face and thumb recognition and resource access control mechanism to obtain a secure and more adequate FTP communication system.

3.1 PROPOSED WORK

Before logging into the system, one user needs go to a trusted authority center to submit personal registration Before logging into the system, the user needs go to a credible authority centre to acknowledge personal registration information, then the authority centre will give the user a user ID, password face image, thumb impression, etc. When a registered user logs in, he enters the user ID, password, face image, thumb impression, then downtime for authentication. If his identity is verified and legitimate, the service will be granted to that user.

3.1. 1. **Registration Process**:

– User submits his personal registration information to authority centr

– Authority centre certify the information and loads it in the database if it is solitary. Amidst this information, password is converted (encryption through hash function) to hash password instead of plaintext, which makes it more difficult for an intruder to get the real passwords.

– Authority centre will setup a user account on the server.

– User ID, password will be provided to the user.

3.1.2.Authentication Process:

When a registered end user signs in into the system, he needs to insert the user ID, password, face image, thumb impression that is which type of authentication process the user had chosen.

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

– Client transmits user ID, password and auxiliary information to the server to log into the system.

– All the information of the client is transmitting to the server in encrypted manner (format).

– Server correlate the information of the user to the information exists in the database.

– If the user's identity is authenticated successfully, then the user is logged in and session is started.

– If the user's identity is does not authenticate, the system will warn the user that this authentication has resulted into failure and terminates the session.

3.1.3. Secure Transmission Process:

After the collective authentication, the session goes to the secure transmission operates by using data compression, data confidentiality and data integrity mechanisms. D. Comparative Study:

File Transfer Protocol (FTP):

– In FTP Username& Password is sequence by sequence transmitted in unencrypted (plaintext) manner.

– In FTP the connection transmit information and data is could not expected final destination securely.

– Slow speed in file transfer.

– Less Secure.

3.1.4. Secure Client Server Network (SCSN) in FTP:

– In SCSN user name & password is transmitted in encrypted manner (encryption process may depend upon the protocol).

– In SCSN the connection transmitted data designated the end destination and to dispense the higher security. – High speed in file transfer.

– High Security and reliable end to end connectivity.

4. CONCLUSIONS

We discuss the demerits of traditional FTP communication systems and correlates the work. Then we propose a new SCSN (Secure Client Server Network in FTP) system by applying dynamic password mechanism, security level selection mechanism, resource access control mechanism and face and thumb recognition. The security and efficiency analysis shows that the modern system makes data transmission secure, apparent, more tactile and efficient. Now we are developing a Client and Server which will be used the FTP, and as for security we have developed an additional module which uses the Encryptions and Decryptions and image embedding (Stenographic Process) which will be used for security purposes. Overall, it will enhance the security over file transfers.

5. REFERENCES

[1] RFC-959 J . Postel, J . Reynolds, lSI, "File Transfer Protocol (FTP)" Oct 1985. Available: http://www.ietforg/rfc/

[2] RFC 4217: P. Ford-Hutchinson, IBM UK Ltd, "Securing FTP with TLS" Oct 2005. Available: http://www.ietforg/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.ietforg/rfc/ [4] Y Ma, H. T. Liu, B. Y Cai, "Design and implementation of a secure FTP system" Applications and Software, Aug 2007.

[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.