URN etd-0407109-183720-1652
Author Ming-Huai Kang
Author's Email Address No Public.
Statistics This thesis had been viewed 55 times. Download 0 times.
Department
Year 2005
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title Intelligent and Secure File Transfer System
Date of Defense 0000-00-00
Page Count 71

Keyword
FTP
Stolen verifier
Keylogger
Trojan horse program

Abstract
Due to the rapid development of network technology, the security of data transmission over Internet becomes more and more important. Among all data transmission protocols, the File Transfer Protocol (FTP) is the most popular. However, FTP systems transmit data in plaintext form, so an adversary can easily obtain the user's critical secrets (e.g. ID, password, file content) by eavesdropping. Therefore, FTP systems do not provide message confidentiality.
In order to secure file transmission, we will design have proposed a Stolen Verifier Resistant File Transfer System. In our system, the user and the server can authenticate each other and establish a session key. Thus, they can encrypt the transmitted files using the session key. In addition, our system can also resist the stolen verifier attack. That is, even an adversary steals the password-verifier file from the server, he/she still cannot login to the server.
Moreover, a kind of Trojan Horse program called a keylogger has been spread out over Internet unconsciously. A keylogger can log a user's ID and password from his/her typing, and then sends these secrets to an adversary. To disable keyloggers, we plan to design and implement an Intelligent Variable Password System and integrate it to the Stolen Verifier Resistant File Transfer System. The new system can intelligently transform a real password into a One Time Password. Therefore, an adversary cannot gain any useful information even he embeds a keylogger to the client side.
Advisory Committee Narn-Yih Lee - advisor

Files No Any Full Text File.
Date of Submission 2006-07-24