105 學年度
專題製作成果發表

專題題目

Linux 時變加密系統
Time-varying Encryption System for Linux

內容摘要

本專題將簡易通訊架構套用至 Linux 系統上，伺服器與用戶端透過 Socket 傳遞訊息，且伺服器與用戶端會進行時間同步，並提取相同的時間因子進行時變加密與解密，以確保訊息在網路間傳遞的安全性，即便傳送的訊息遭他人竊取，也無法取得時間因子進行解密，雙方還會建置資料庫，用來記錄帳戶資訊或歷史訊息，展現一個安全性高的資料傳遞系統。

專題成果

用戶端透過無線網路連接伺服器，便可發送訊息或指令至伺服器，伺服器確認接收到訊息會回覆告知用戶端，雙方會將訊息儲存至訊息資料表，若發送的是指令，則雙方處理指令內容。

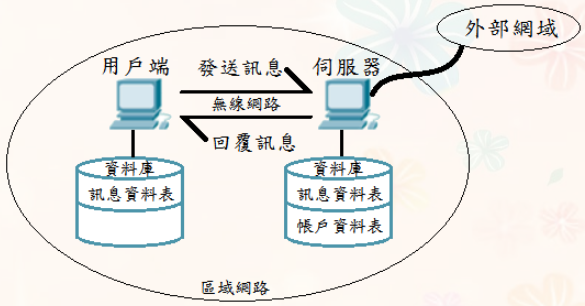

圖 1 系統架構圖

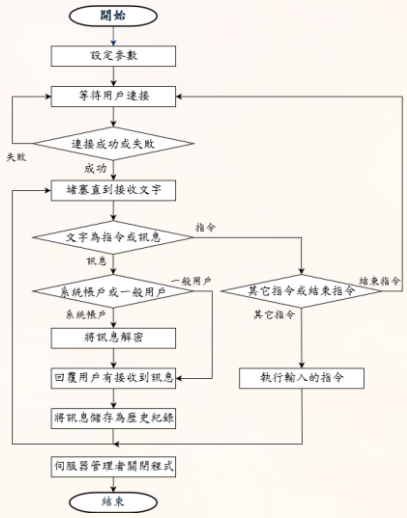

圖 2 伺服器流程圖

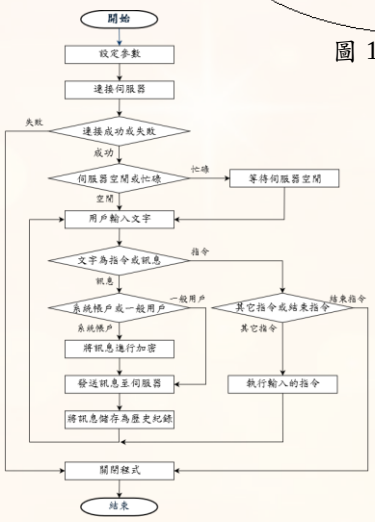

圖 3 用戶端流程圖

通訊過程大致分為四階段，依序為 Socket 連接、用戶發送訊息至伺服器、處理訊息或指令、結束程式，伺服器流程圖如圖 2 所示，用戶端流程圖如圖 3 所示。

電機工程系

學號：U02127109　學生：林　新　澔
學號：U02127130　學生：彭　希　銘

指導老師：邱　機　平

明志科技大學
MING CHI UNIVERSITY OF TECHNOLOGY