

資工系實務專題研究計畫成果報告

研究計畫成果摘要報告

專題編號：097CSIE-S012

執行期限：96 年 1 學期至 97 年 1 學期

指導教授：梁文耀

專題計劃參與人員：賴育聖、蔡明諺

一、中文摘要

本專題目標是實作出一個可攜式的網路傳輸加密裝置，是利用Creator XScale-PXA270開發板[1]實現，此開發板適用於發展可攜式裝置，符合題目可攜式的訴求。再藉由撰寫自動化程式、驅動程式[2]與金鑰傳輸程式以及建置所需軟硬體服務達到目標。此外，在驗證系統的正確性上將分成三部分來執行：分別是交換金鑰、安全連線建立和最後的雙方傳輸。在驗證是否可靠部分，我們使用封包擷取、分析軟體來查證經由本裝置對外網路的無線網路封包是否經過加密，以確保系統的正確性與可靠度。

關鍵詞：加密網路 零設定 交換金鑰 網路安全 虛擬私有網路 公眾無線網路 可攜式裝置。

二、緣由與目的

在今日網路盛行的時代，人與人之間藉由網路交流已是生活中不可或缺的一部份。尤其在現今公眾無線網路日漸普及的情形下，有心人士可以透過簡易的管道擷取公眾無線網路封包，從中竊取出重要的隱私資訊。有鑑於此，本組提出一智慧型，易操作之安全隨身罩(Security Taken with Yourself, STY)系統，讓使用者可在不改變網路設備的前提下，藉由具有加密保護的安全網路來讓可攜式裝置(例如筆記型電腦或PDA)做網路存取的服務。

三、功能與構想

我們提出零設定(Zero Configuration)的行動加密裝置 — 「安全隨身罩(Security Taken with Yourself, STY)」，讓使用者幾乎不需任何知識背景、繁雜的手動設定、改變網路設備的前提下，藉由有加密保護的安全VPN(Virtual Private Network) [3]通道讓可攜式裝置(如筆記型電腦或PDA)做網路存取的服務。

四、系統軟硬體平台簡述與資源運用

表格 1-使用的軟硬體平台

硬體	
Platform	Creator XScale-PXA270
Microprocessor	Intel XScale-PXA270
USB Interface	USB Rev. 1.1 compatible
USB 無線網卡	D-Link DWL-G122 Wireless USB Adapter (802.11g)
軟體	
Fedora Core 5.0-Linux :Kernel 2.6.15	
DHCP Server 3.1.0	
Iptables 1.4.0	
Open VPN 2.0.9	
OpenSSL 0.9.7	
Thttpd 2.21b	
Php 4.4.8	

我們使用 Creator XScale-PXA270 開發板，XScale-PXA270 是專為高效能、低功耗、移動性手持裝置設計之SOC(System On Chip)。我們將使用 RJ45 Connector 來與使用者 PC 建立區域連線，再藉由無線網卡透過無線網路來建立無線網路下的安全連線。除硬體平台外，其技術核心尚包含VPN、VPN 設定自動化、密碼學、NAT、DHCP、驅動程式與 Web-base 設定。

五、實作內容簡述

如下頁圖 1 所示。STY 是成對使用的簡易裝置，經過交換金鑰(Key)後，使用者僅需將 PC 與 STY 的一端連線，透過 DHCP



圖1.系統概念圖

讓使用者不需設定網路卡即可自動取得 IP，並藉由 NAT 令內部網路與外部網路溝通。此外我們提供網頁介面(PHP) [4]的方式來進行些許的設定，像是 Wireless、有線網路的固定 IP 或 ADSL 等等的網路環境設定。最後是將其中一個 STY 裝置裝設於通訊目的端(通常為有線網路環境)，而另一 STY 裝置則與可攜式裝置隨身攜帶至其他地方透過網際網路(公眾無線網路)來建立安全的網路連線。

六、設計創意

零設定的操作模式和可攜式的便利，對於不了解網路安全或是 VPN 的使用者，只需將 STY 隨身攜帶，並於使用時做簡單的接線動作即可達到安全的網路通訊，尤其是在公眾無線網路的環境之下，能夠安全的進行網路存取的動作，提升其使用價值。此外，交換金鑰的部份只需將兩個 STY 裝置藉由 USB、RJ45 Connector、通用型之輸入輸出 (General Purpose I/O)、或是近距離無線通訊(Near Field Communication, NFC)等方式來實現，避免交換金鑰時被人竊取的風險，確保整個系統是安全無虞的。

七、衍生應用

本裝置可以應用在許多需要安全傳輸的資訊交換場合上。例如在校園的公眾無線網路環境。若校方的基地台與使用者雙方在這種環境下加裝STY，將封包經由 VPN技術加密來保護資料，避免帳密被他人竊取的問題。因此STY也可如右上圖2所示，使用於行動辦公室的應用上(例如、IBM的行動辦公室)。

若今天某位員工需長期在公司外部工作，且必需跟公司內部網路做資料的存取，

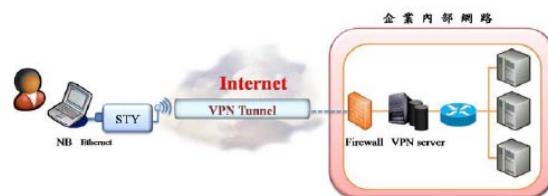


圖2. STY行動辦公概念圖

也可透過加裝STY來避免封包在外部網路連線到公司時，資料遭到竊取的風險。因此在現今社會對商業機密越加重視的情形下，更彰顯出STY的應用性。

此外，網路遊戲在全球很多地方都很普遍，但由於網路遊戲中的虛擬代幣與物品可依一定的比例來兌換真實的金錢。因此帳密常常被有心圖利的人士竊取。雖然遊戲廠商提供多種軟體保護的方法；但顯然效果不彰。因此若在遊戲伺服器端與玩家電腦之間如下圖來使用STY，就可以避免帳密的資訊在傳輸過程被截取到它處的可能性，藉此解決帳號被盜取的問題。

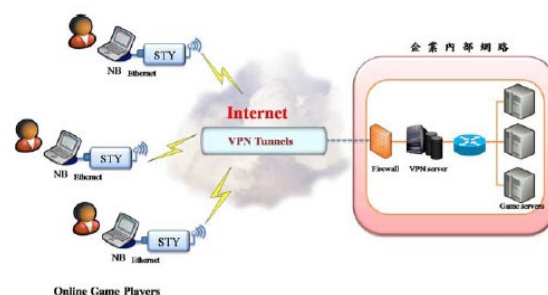


圖3. STY網路遊戲概念圖

八、參考文獻

- [1] Microtime-Creator-XScale-PXA270 User's Guide V2.02 (for Linux)
- [2] Linux 驅動程式 3e/Jonathan Corbet, Alessandro Rubini, Greg Kroah-Hartman. /O'REILLY 出版
- [3] VPN architectures/ Pepelnjak, Ivan, Guichard, Jim /旗標
- [4] PHP5 程式設計教學/吳佳諺/成大資訊