行政院國家科學委員會補助專題研究計畫成果報告

網際網路上高效率之安全促成工具(Ⅱ)

計畫類別：□個別型計畫　■整合型計畫

計畫編號：NSC 89－2213－E－002－081

執行期間：88 年 8 月 1 日至 89 年 7 月 31 日

計畫主持人：國立台灣大學電機工程學系　雷欽隆教授

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份

□出席國際學術會議心得報告及發表之論文各一份

□國際合作研究計畫國外研究報告書一份

執行單位：國立台灣大學電機工程學系

中　華　民　國　89 年 10 月 20 日

行政院國家科學委員會專題研究計劃成果報告

網際網路上高效率之安全促成工具(Ⅱ)
Efficient IP-based Security Enablers for Internet(Ⅱ)

計劃編號：NSC 89-2213-E-002-081
執行期限：88 年 8 月 1 日至 89 年 7 月 31 日
主持人：雷欽隆　國立台灣大電機工程學系教授

一、中文摘要

隨著網際網路及電子商務的快速成長，如何在網際網路上提供一個安全的網路通訊環境已成為一迫切的課題。然而，現有的網路安全解決方案，大多將安全機制設計於應用層，因此針對各個不同的應用程式，必須做個別的修改，方能達到保密及認證的功能，十分不便，且需耗費許多額外的人力物力。有鑑於此，本計畫提出網際網路安全促成工具的概念，作為一有效的網際網路安全解決方案。網際網路安全促成工具的概念，在於提供一個可彈性運用，擴充性高的網路安全介面，讓所有網路應用程式，毋須做任何修改，即可使用，並立即享有認證，保密，使用權控制等網路安全服務。

本計畫所提出的網際網路安全促成工具之系統架構設計分為三大部分：認證及密鑰管理部分、網路層協定加密部分以及安全策略部分。我們已將此系統實作於 FreeBSD 2.2.8 作業系統上。

本計畫所提出之網路安全促成工具，提供使用者一個強健的網路安全架構，以及多種的網路安全服務，並具有系統設定容易，適用於區域網路及企業內部網路，且可適用於低計算能力的行動計算裝置等優點。

此外，我們的系統亦將 Public Key Kerberos 的觀念整合進來，使得系統具有相當良好的擴充性。對於近來日漸受到重視的電子商務，本計畫亦提出 SET Enabler 的安全服務，讓使用者在網路上進行電子交易時，能有一個既安全又方便的電子付款解決方案。

關鍵詞：網路安全，網際網路，電子商務，網際網路安全協定，身份認證，密鑰管理，隱私性，安全促成工具，網路付款。

Abstract

With the fast growth of Internet and electronic commerce, how to provide a secure communication environment on the Internet has become an urgent issue. However, Most of the network security solutions place their security mechanisms at the application layer. Therefore, they must modify each application individually to accomplish the purposes of security and authentication. This is very inconvenient and requires much time and work. In this project, we propose the concept of IP-based security enablers to be an efficient Internet security solution. The concept of IP-based security enablers is to provide a flexible and extensible network security interface for

network programs. Network programs can enjoy network security services such as authentication, confidentiality, access control immediately without any modification.

The system architecture of the proposed IP-based security enablers contains three components: an authentication and key management component, a network protocol encryption component, and a security policy component. The implementation is carried out on FreeBSD 2.2.8 operation system.

IP-based security enablers provide a robust network security infrastructure and various security services to users. It has advantages such as: does not need PKI, suitable for Local Area Network (LAN) and Intranet of an enterprise, easy to install, and suitable for low-computation power mobile computing devices.

In addition, our system integrates the concept of Public Key Kerberos; therefore, it has good scalability. Owing to electronic commerce is getting more and more important recently, we also propose a SET Enabler to be a secure and convenient Internet payment mechanism.

Keywords: Network Security, Internet, Electronic Commerce, IP Security, Authentication, Key Management, Privacy, Security Enablers, Internet Payment.

二、緣由與目的

在早期的網際網路發展中，網路安全並未受到太大的重視。然而，隨著電子商務的快速發展，越來越多的商業應用軟體及商業交易使用網際網路為媒介，網路安全已成為一亟待解決的問題。然而，現有的網路安全解決方案大多將安全機制設計於應用層，因此針對各個不同的應用程式，必須做個別修改，方能達到保密及認證的功能，十分不便。有鑑於此，本計畫提出網際網路安全促成工具的概念，作為一有效的網際網路安全解決方案。

網際網路安全促成工具的概念，在於提供一個可彈性運用，擴充性高的網路安全介面，讓所有網路應用程式，毋須做任何修改，即可使用，並立即享有認證，保密，使用權控制等網路安全服務，且使用者可視其需要隨時加入新的安全功能。由於網路應用程式必須透過 IP 層發送封包來傳送資料，而所接收的資料也必須經由 IP 層方能往上送達位於應用層的網路程式。因此，我們在網路層做適當的修改，以達成網際網路促成工具的功能。我們並且融入了網際網路安全協定（IP Security）及 Public Key Kerberos 的概念到我們所設計的網際網路安全促成工具之中。

另外，對目前相當熱門的電子商務，在本計畫中，我們也加入了 SET Enabler。我們認為現有的網路付款系統，在使用的方便性與不可否認性等方面，及保障消費者付款資料的保密性及私密性上，仍有改進的空間。所以我們提出了架構在 SSL 層上的 Secure Information Layer (SIL)，作為提供安全付款的機制。

三、結果與討論

本子計劃經過一年的執行與研究，我們已設計並實作出幾種基本的網際網路安全促成工具（包含認證、加密、密鑰管理及安全策略促成工具），我們另外提出了兩種安全促成工具之設計，一為安全通道促成工具（Tunnel Enabler），其設計目的

在提供無法安裝網際網路安全促成工具的使用者，可以經由一個安裝網際網路安全促成工具的閘道器或路由器，間接得到網際網路安全促成工具之保護。另一為公開密鑰促成工具（Public-Key Enabler），其設計目的在引入公開密鑰的機制，以加強本促成工具之認證功能，同時能夠讓系統的擴充性能夠更加的良好。

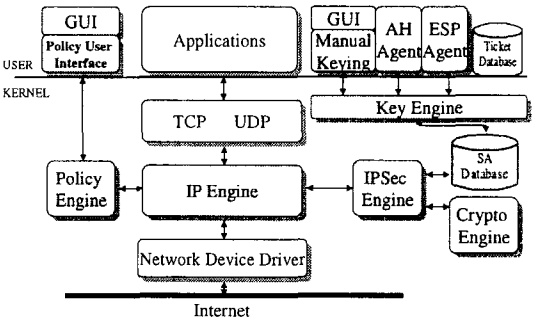
我們所提出的網際網路安全促成工具的系統架構設計分為三個主要的部分：認證及密鑰管理部分、網路層協定加密部分以及安全策略部分。在認證及密鑰管理部分，我們自行設計出了一個基於 Public Key Kerberos 認證服務的密鑰管理協定，稱為通行票式密鑰管理協定。在網路層協定加密部分，我們採用網際網路安全協定（IP Security），用來做 IP 封包的加密，在安全策略部分，我們利用過濾封包的輸出及輸入做分析，將之歸納成四種安全策略。

在實作方面，我們的實作平台為 FreeBSD 2.2.8 作業系統。網際網路安全促成工具的網路架構如圖(一)所示。其系統架構如圖(二)所示。圖(三)展示我們在 X-Windows 上所實作的網際網路安全促成工具圖形使用者介面。圖(四)是 Public Key Kerberos 的運作過程。我們亦對我們的系統做實際測試，圖三為我們我們利用協定分析儀捕捉 IP 封包，以顯示測試結果。

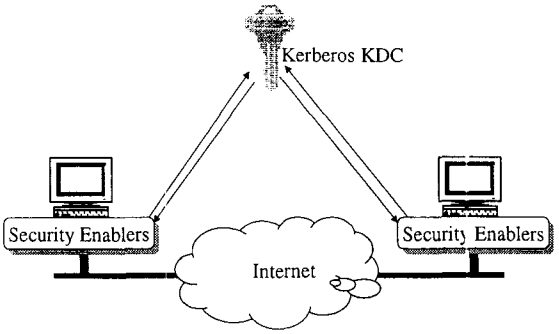
而在網路付款機制方面，我們利用公鑰與對稱金鑰演算法混合加密系統，提供如同公鑰系統的功能且更有效率的加密系統。另一方面利用我們所提出的傳輸協定達到保障消費者付款資料不會為網路商店所取得，而消費者所購買商品的隱私權亦可獲得保障，另外，亦可提供消費者足夠資料作為網路商店及付款系統不可否認的證據。

四、計劃成果自評

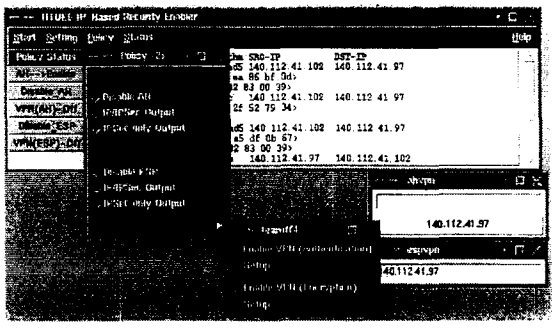
本計畫提出一個在網際網路上高效率的安全促成工具，做為一個有效的網際網路安全解決方案。網際網路安全促成工具提供使用者一個具彈性且擴充性高的安全機制與介面，讓使用者在毋須修改應用程式的情況下，即可達成其所要求的安全功能。使用者可視其需要隨時加入新的安全功能。另外，本促成工具對於網際網路



圖(二) 安全促成工具之系統架構

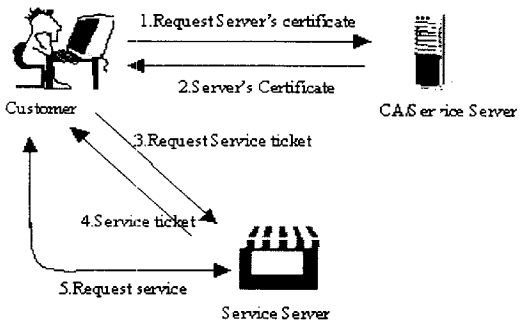


圖(一) 安全促成工具之網路架構



圖(三) 安全促成工具圖形使用者介面

應用程式而言是透通的（Transparent）。我們所設計的網際網路安全促成工具提供使



圖(四) Public Key Kerberos

用者包含身份認證、加密、資料完整性、密鑰管理、存取控制等基本安全功能。我們另外公開密鑰促成工具（Public-Key Enabler），其設計目的在引入公開密鑰的機制，以加強本促成工具之認證功能，同時讓系統的擴充性能夠更加的提升。在實作方面，我們已在 FreeBSD 2.2.8 作業系統上完成基本網際網路安全促成工具的實作。在網路付款的部分，我們亦完成了實作並進行測試。

未來，我們將繼續完成安全通道促成工具之實作，設計新的促成工具以擴充網際網路安全促成工具的功能，並加強整個系統安全性與執行效能。

五、參考文獻

[1] 張譽鐘，網際網路安全促成工具之設計與實作，台大電機所碩士論文，八十八年六月。

[2] P. C. Cheng, J. A. Garay, A. Herzberg, H. Krawczyk, "A Security Architecture for the Internet Protocol," IBM Systems Journal, Vol. 37, No.1, 1998.

[3] B. Cox, J. D. Tygar, Marvin Sirbu, "NetBill Security and Transaction Protocol," Proceedings of the 1st USENIX Workshop on Electronic Commerce, pp. 77-88, July, 1995.

[4] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, Nov. 1998.

[5] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998.

[6] S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402, Nov. 1998.

[7] S. Kent and R. Atkinson , "IP Encapsulating Security Payload (ESP)," RFC 2406, Nov. 1998.

[8] J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)," RFC 1510, Sep. 1993.

[9] C. Neuman and J. Wray, "Public Key Cryptography for Initial Authentication in Kerberos," draft-ietf-cat-kerberos-pk-init-03.txt, 1997.

[10] W. Stallings, Cryptography and Network Security, 2nd Edition, Prentice-Hall, 1999.