行政院國家科學委員會專題研究計劃成果報告

ATM 網路安全管理之研究(III)

Security Management for ATM Networks (III)

計劃編號：NSC 87-2213-E-002-049
執行期限：86 年 8 月 1 日至 87 年 7 月 31 日
主持人：雷欽隆　台大電機系教授

一、中文摘要

由於網際網路的快速發展促成了網路上大量資訊流通與資源共享之需求，並勾勒出電子商務之無限遠景。為了有效的應用與管理日趨龐大複雜的網路資源，發展智慧型網管系統是刻不容緩的工作。而網路安全則是網管的重要課題之一。舉凡秘密通訊、訊息確認、資源授權、與存取管制等都是網路安全管理的範圍。

本計劃針對 ATM **網路安全管理之各項技術作深入探討，並提供總計劃之網管系統所須之安全管理支援。預定之進度與相關研究工作業已完成，包含安全訊息代理人、安全管理工具、一個擴充** SNMPv2 **安全能力的認證模型、數個有效率的網路服務協定、與相關網路安全協定的架設與測試。**

關鍵詞：ATM **安全管理、隱私性與正確性、安全的** ATM **服務、**SNMP

Abstract

Due to the fast progress of Internet, the demand of data transmission and information sharing grows dramatically. Therefore, the development of high speed networks attracts the attentions of both academic and industrial societies. To manage the ever-growing and complicated networks efficiently, an intelligent network manage-ment system is in urgent need. Meanwhile, the demand of ubiquitous information sharing makes the security consideration one of the major concerns in a network management system. In an open network, it is necessary to preserve data privacy, authentication and integrity.

In this project, we focus on the security issues of managing ATM networks. We have designed and implemented the underlying security mechanisms and provide security management tools for the whole system of this integrated project. We have finished all components proposed, including Secure Message Agent, a set of security management tools, some secure network service protocols, and an authentication model for SNMPv2.

Keywords: ATM Security Management, Privacy & Authentication, Secure ATM, Services, SNMP.

二、緣由與目的

為了能有效的應用與管理在高速網路環境下日趨龐大複雜的網路資源，發展智慧型網管系統是刻不容緩的。也由於資訊無遠弗屆的傳輸與共享，網路安全已成了

網管中重要的一環。在開放式的網際網路中，一者傳輸的資料容易被竊取、竄改，傳輸資料的隱私性與完整性相當重要；再者電腦病毒與電腦蟲可能藉由某些管道破壞網路中的資源，所以安全的網路存取管制也有其必要。基於上述原因，在網管系統中一套完整的安全管理工具是迫切需要的。

而安全的網路管理系統是既複雜且困難的，其癥結如下：

- 網路與通訊的安全問題，遠非單純的加密解密就可達成。
- 任何安全機制或演算法設計時，都必須仔細考量，思索對手所可能採取的攻擊對策。
- 所發展出來的安全機制，必須妥善規劃如何使用、用在何處。
- 通常在安全機制中，都會同時涉及許多不同的演算法與協定。
- 在安全管理機制的實作中，不僅要縝密考量安全性之外，也必須兼顧其執行效率與系統所增加的負擔。

在本計劃中，我們的研究重心在於 ATM 網路管理的安全性。我們將為整體計劃中的 ATM 網管系統設計一套底層的安全機制，並提供有效率的安全管理工具。

為了防止網路資源被非法存取與訊息被竄改，在我們的網管系統中必須有相對的安全保護架構。首先，我們會把一個特別為 ATM 網管設計的安全訊息代理人(Secure Messaging Agent)加進 NetView 中。而此代理人不僅與 SNMPv2 相容，並且提供其他子計劃基本的安全架構。此外，為了降低管理上的複雜性，我們將提供易於使用之安全管理工具給系統管理者與其他子系統的軟體使用。我們也設計了幾個安全而有效率的 ATM 網路服務協定，例如安全的電子會議系統、安全的電子投票系統與安全的電子貨幣系統等。

三、結果與討論

本子計劃經過兩年的執行與研究，在網管系統之安全訊息代理人、安全管理工具、安全的網路服務協定等方面都有相當的成果，分項討論如下：

(一)安全訊息代理人：

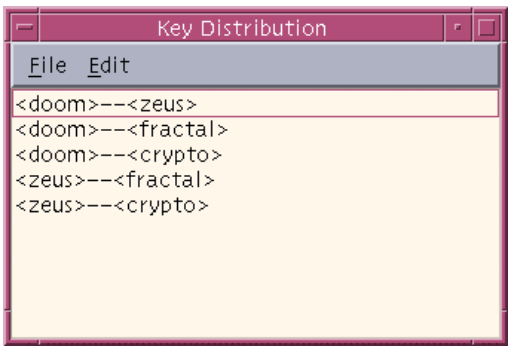
此代理人的目的是欲使整個網管系統免於安全上的顧慮。且必須與 SNMPv2 相容，並對其他子計劃與系統使用者是透明的(transparent)的。在去年度中，我們利用一些密碼學的工具來架構我們的安全機制；而在本年度中，則重於系統的整合與跨平台的測試工作，以期本代理人系統有高度的相容性與可攜性。

而這些安全函式所需要的金匙，必須由金匙分配中心來產生與分配。我們也設計了一個安全而有效率的金匙分配中心。

(二)安全管理工具

在去年度已完成的安全管理工具包括金匙管理視窗與安全函式庫管理視窗。今年度我們利用這些工具對於安全函式庫與各種網路安全協定進行跨平台的測試。

使用者可以透過金匙管理視窗執行金匙分配、安全參數設定、建立安全鏈結等功能。金匙管理的主視窗如圖(一)所示，使



圖(一)金匙管理視窗之主視窗

用者可以看到目前已有的鏈結，並且可以

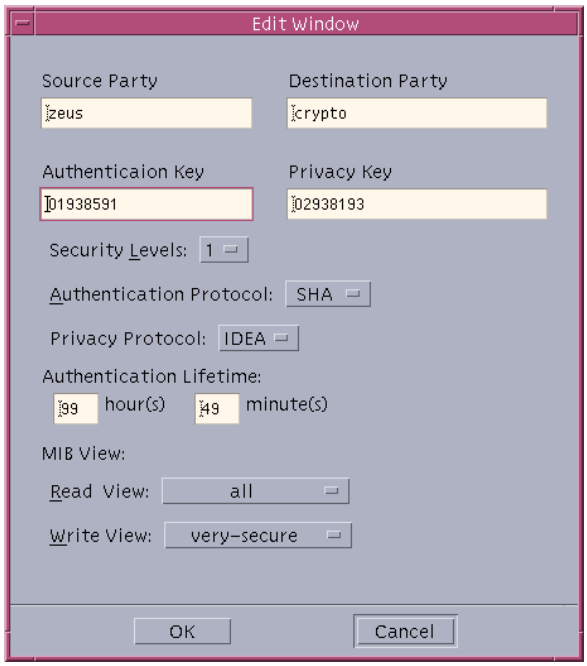
編輯功能來增加、刪除、或修改。並可執行金匙分配來供這些鏈結使用。使用者也可以透過視窗設定各個鏈結所需的安全等級與參數如圖(二)。

在安全函式庫管理視窗方面，主要的功能是提供一個視窗用來測試已完成之安全函式庫中的各項安全功能與函數，同時提供便於使用者參考的函式庫說明。其主視窗如圖(三)所示。目前已含括的函式包括 DES、SHA、MD5、RSA 與 Diffie-Hellman 等。

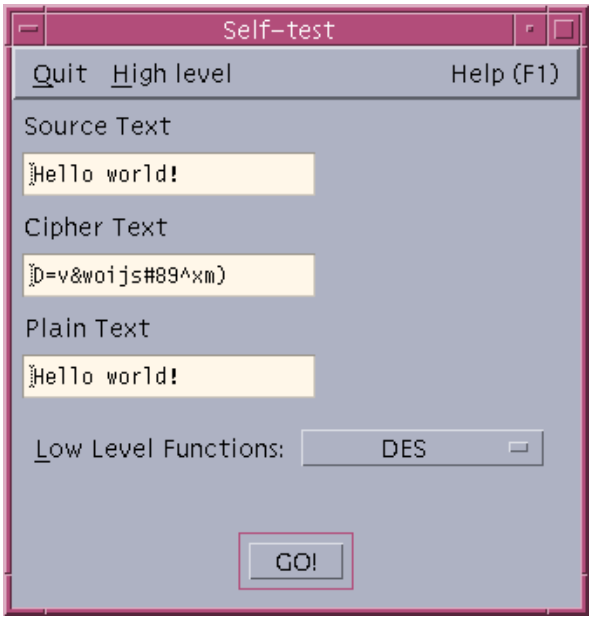
(三)ATM 上安全的網路服務協定

這方面的研究成果，包括電子投票、電子貨幣、數位簽章、匿名轉信系統等。

電子商務成功與否的最大關鍵，莫過於安全性與方便的付款方式，而電子貨幣正是電子商務中理想的付款方式。故我們陸續提出了一些有效率的協定，包括可分割的電子貨幣，使得電子貨幣能像真實貨幣一樣可以找零；可加時戳的電子貨幣，以減輕發行銀行資料庫必須無限制擴張的壓力；公平公正的匿名簽章，可使電子貨



圖(二) 金匙分配之安全參數設定視窗



圖(三) 安全函式庫管理視窗

幣的匿名性不會成為金融犯罪的工具。

在電子投票方面，我們也提出了一次領票多次選舉的協定，可以減輕網路負荷與發票的次數。

在數位簽章方面，我們則提出了門檻式匿名數位簽章，可以分散簽證權力，避免潛在的缺失與弊端。

而匿名轉信系統則是許多網路應用所需的基本機制之一。因此我們對此做了深入的探討與實作，並建立了一套可以相容 MIME、PGP 等電子郵件標準的匿名轉信系統。

(四)網路安全管理協定之相關研究

雖然近幾年 IETF 提出的 SNMPv2 為下一代的 Internet 網路管理協定，但以嚴格的安全管理角度而言，SNMPv2 上的安全協定在一些重要的方面缺乏完整的定義。例如，如何建立使用者認證訊息和認證有效時間的設定。因此我們提出了一個適用於 SNMPv2 的使用者認證模型[5]，以擴充 SNMPv2 的安全管理能力。由嚴謹的安全管理觀點而言，此模型能提供一個更容易管理和易於擴充新功能的網路管理環境，同時也能維持與現有 SNMPv2 的相容性。

四、計劃成果自評

在本計劃的最後一個年度中，我們的工作目標著眼在未來性。除了將預定的進度完成外，也希望我們的開發成果能夠應用在其他的系統中，尤其面對新世代網際網路的革命性發展，更是不敢鬆懈。以下將本年度的研究成果分項茲述：

(一)安全管理代言人

此部份是整個網路系統安全的核心之一。除了在此網管系統中扮演安全守門神的角色外，也可以推廣到其他的系統上。

(二)安全管理工具

安全管理的複雜度，隨著網路上節點的數量而迅速增加，加上各個節點間的通訊所需的安全等級不同，複雜的安全參數設定，對管理者而言，必然需要有效率的管理工具來輔助。而我們所發展的管理工具，即能提供方便的設定視窗與有效率的管理程式。

(三)安全的網路服務協定

我們所提出的數個網路服務協定，包括了數篇已發表的論文。這些協定我們都可證明其效率遠優於其它系統，能夠符合 ATM 高速網路下的應用。

雖然目前這些協定僅完成理論部份，但這些電子商務、電子投票、與電子會議在現實生活中的應用，已是不可抵擋的趨勢與潮流，如果能夠獲得更多的支援，將這些協定付諸實作，相信會有更進一步的成果。

(四)網管安全之相關研究

針對 SNMPv2 安全性上的缺失，我們提出了相對的解決方法。在這方面，我們鑽研並分析 SNMPv2 在安全性上面的設計與可能面臨的攻擊，並且謀求解決之道，因此提出了一個適用於 SNMPv2 的使用者認證模型。在未來的工作中，如果能加以實作與測試，便可以驗證其成效。

(五)其他

匿名轉信系統的建置，並且相容於 MIME、PGP 等協定，提供了諸多應用程式一個簡易的整合介面，因而增加了這個轉信系統的可行性。

其他的認證協定、安全傳輸協定、安全付款機制等等，也都在我們的探討對象中，我們以蓄勢待發來自評。

五、參考文獻

[1] C. I. Fan, and C. L. Lei, “A Multi-Recastable Ticket Scheme for Electronic Elections,” Proceedings, ASIACRYPT’96, 1996.

[2] W. S. Juang and C. L. Lei, “Blind threshold signatures based on discrete logarithm,” Proc. of Second Asian Computing Science Conference on Programming, Concurrency and Parallelism, Networking and Security, LNCS 1179, pp. 172-181, 1996.

[3] W. S. Juang and C. L. Lei, "A collision free secret ballot protocol for computerized general elections, Computers & Security, Vol. 15, No. 4, pp. 339-348, 1996.

[4] W. S. Juang and C. L. Lei, "A secure and practical electronic voting scheme for real world environments," IEICE Trans. On Fundamentals, Vol. E80-A, No. 1, pp. 64-71, January, 1997.

[5] 周天人，一個適用於 SNMPv2 的使用者認證模型，台大電機所碩士論文，八十六年六月。

[6] William Stallings, Network and Internetwork Security. Pretice Hall International editions, 1995.

[7] Daniel Stevenson, Nathan Hillery, Greg Byrd and Dan winkelstein, “Design of a Key Agile Cryptographic System for OC-12c Rate ATM,” Internet Society Symposium on Network and Distributed Systems Security, Feb, 1995.