行政院國家科學委員會專題研究計劃成果報告

個人化網路教學系統上安全與收費管理之研究與製作(II)
Security and Billing Management for Personalized Networked Education Systems (II)

計劃編號：NSC 89-2213-E-002-034
執行期限：88 年 8 月 1 日至 89 年 7 月 31 日
主持人：雷欽隆　台大電機系教授

一、中文摘要

本計畫的目的主要是提供整體系統之安全機制並開發出一套可靠而高效率的帳單管理與付款架構。本計畫所完成的帳單管理系統將包含帳號管理、用戶身分確認、帳目沖銷管理與查詢服務、以及電子化帳單、收據與發票等功能。另外，在付款方面，本計畫將設計出一組彈性的付款方式，例如信用卡，智慧型 IC 卡，電子資金轉移，電子貨幣等，讓用戶可以依照個別的情況選擇適當的方式安全地進行付費。此外，為了保護個人的隱私性，除了基本的付款方式外，我們也將研究開發出匿名的電子付款技術，使得用戶身分在付款時受到安全的保護，不虞曝光。本計畫將運用可靠且高效能安全技術為磐石，例如高效率的加密法，數值簽章，盲目簽章，與存取管制等，來發展所提出的系統功能。

在配合總計畫與其它子計畫的原則下，本計畫將完成整體系統中與系統安全、帳單管理及付款相關的功能，並且提供具彈性的銜接界面，使得本計畫能夠充分且容易地與其它子計畫進行整合。

關鍵詞：網路教學、帳單管理、電子付款、電子貨幣、網路安全、網際網路。

Abstract

The main goals of this project are to build the security infrastructures of the networked education system, to develop reliable bill management tools, and to construct efficient electronic payment protocols. The proposed bill management consists of several components, such as digitized bills, authentication tools, and accounts management. Our payment systems will provide a set of different payment protocols such that every user can choose a way suitable for himself to pay, for example credit card, IC card, or digital cash payment. Furthermore, we will also develop anonymous electronic payment techniques to protect the privacy of payers. In this project, we will take secure and high-performance security primitives, such as efficient encryption, digital signatures, and blind signatures, as the foundations to construct all the functions we propose.

This project will support the necessary components of billing, payment, and other security mechanisms in this networked education system, and we will provide a friendly method for integration with other subprojects. After the completion of the proposed project, we will deliver a practical networked education system, which can provide secure and personalized services with secure and robust billing management.

Keywords: Networked Education, Bill Management, Electronic Payment, Electronic Cash, Network Security, Internet.

二、緣由與目的

由於網際網路技術的快速發展以及網路使用的日益普及，許多資訊服務正由傳統的紙張傳播方式朝向網路導向的電子傳播方式發展。藉由網際網路無遠弗屆與高速傳輸的特性，分佈於各地的用戶可隨時透過資訊服務提供者快速地獲得其所想要的資訊。將這些先進的通訊技術應用在教學上，不僅用戶可以透過網路方便地接受到教學服務，更可以讓學習時間彈性化，這種新型態網路教學模式將可以突破傳統教學系統所受的時空限制。

基於使用者付費的原則，用戶必須在接受教學服務後依據事先所協定好的價格付費，當然，教學服務提供者也應提供安全且方便的收費付款方式，讓使用者可以在安全確保的前提下方便地進行付費。此外，教學系統本身也應有一套健全的帳單帳目管理機制，使其能夠正確而有效率地管理龐大的使用者帳戶與帳單業務以及其它相關的資料。

本計畫的目的主要是提供整體系統之安全機制並開發出一套可靠而高效率的帳單管理與付款架構。本計畫所完成的帳單管理系統將包含帳號管理、用戶身分確認、帳目沖銷管理與查詢服務、以及電子化帳單、收據與發票等功能。另外，在付款方面，本計畫將設計出一組彈性的付款方式，例如信用卡，智慧型 IC 卡，電子資金轉移，電子貨幣等，讓用戶可以依照個別的情況選擇適當的方式安全地進行付費。此外，為了保護個人的隱私性，除了基本的付款方式外，我們也將研究開發出匿名的電子付款技術，使得用戶身分在付款時受到安全的保護，不虞曝光。本計畫將運用可靠且高效能安全技術為磐石，例如高效率的加密法，數值簽章，盲目簽章，與存取管制等，來發展所提出的系統功能。

三、結果與討論

本子計劃的執行與研究，大致已完成系統架構的設計與規劃，並且完成部分子系統的實作與測試，以下將主要結果條列之，並加以討論：

(一) 網路傳輸的安全措施

系統的安全措施的第一步，便是資料傳輸過程中，完整性、隱密性、與對方身份的確認。我們已建立一套安全函式庫，包含 RSA、DES、IDEA、MD5 等等常用的密碼學機制。另外，本實驗室中已完成一套針對網路底層架構的安全致能器，將可被應用到本子計畫中，就這方面我們也完成評估與整合測試。

(二) 以 Kerberos 為基礎的收費與記帳架構

我們提出了以 Kerberos 為基礎的收費與記帳的架構，使用者透過收費主機，付費的同時，取得憑證，藉由憑證進入網路教學的伺服器擷取所需的教學服務。另一方面，記帳系統也同時紀錄該筆交易。

我們已經完成了 Kerberos 5 的架設與測試，並且可以整合到伺服器，作為其認證的工具。

(三) 收費方式的研究與開發

網際網路的使用者，皆是透過網路取得教學服務，因此必須設計出便利的付款管道，使得使用者可以在安全無虞的環境下，透過網際網路就可以輕鬆完成付款的動作。

我們不僅涉略目前已發表的收費系統，也提出許多有效率的電子貨幣系統，例如用戶端高效能的電子貨幣系統、公平電子付款系統(Fair E-Cash Systems)、可分割之電子付款系統（Divisible E-Cash Systems）等等[1-3]。其中可分割之電子付款系統可以把電子貨幣分解成數個較小面額的貨幣獨立分開使用，例如 100 元面額的電子貨幣可以分解成二個 50 元或四個 25 元或是更小面額的電子貨幣分開使用。可分割之電子付款系統可以讓電子貨幣的使用更方便更彈性。我們利用二次剩餘與離散對數理論來研究開發出高效率可分割之電子付款系統。

四、計劃成果自評

在過去一年中，我們已完成整體安全系統架構設計並開發完成有效率之電子貨幣協定及付款機制，本計劃之部分研究成果獲得第八屆全國資訊安全會議論文獎、1999 年龍騰論文獎及資訊學會博士論文獎。在計劃的最後一年，我們將在配合總計畫與其它子計畫的原則下，完成整體系統中與系統安全、帳單管理及付款相關的功能，並且提供具彈性的銜接界面，使得本計畫能夠充分且容易地與其它子計畫進行整合。藉由本計畫的執行，整體系統不僅能夠在可信賴的環境下有效率地管理大量的用戶帳單業務，更可以讓使用者透過網路安全地進行付款作業。以下分別就前一節中所列舉的結果，一一提出自評：

(一) 網路傳輸的安全措施

密碼學的工具是所以安全措施的基礎，因此不論採用何種安全架構，加解密、數位簽章、雜湊函數等等都是必備的工具。而我們所完成的安全函式庫，就包含了目前具有公信地位的諸多密碼學演算法的程式庫，可以供往後系統實作時使用。所以在這部分的工作，雖然從外在看不出成果，卻是基礎建設的重要部分。

(二) 以 Kerberos 為基礎的收費與記帳架構

Kerberos 並不需要使用到非對稱式加解密或數位簽章、因此在目前數位憑證建置不完善亦不普及的環境下，Kerberos 極適合作為系統的認證與金匙分配的架構。而我們所提出的收費與記帳架構，即以 Kerberbos 為基礎，可以兼顧安全性與效率，並且簡化系統實作所需要的成本。

(三) 收費方式的研究與開發

目前的網路商場多是利用信用卡收費，但是信用卡的交易成本較高，而網路上的資訊服務多是小額付費為多，並不適合使用信用卡付款。因此電子貨幣不但具有匿名性，且交易成本比信用卡小，將有利於網際網路上電子商務的推展。我們提出了若干用戶端高效能的電子貨幣系統，不但可以大量降低使用者端的運算負擔[2]，並且可以符合社會公平正義、降低銀行資料庫負擔[1]，還可以使電子貨幣有效率的分割[3]，使電子貨幣的使用各具有效能與彈性。

(四) 其他

最近網路與系統安全越來越受到普遍的重視，然而網路交易所衍生的糾紛也層出不窮，本系統除了著眼於安全性的保障外，也致力於交易公平性的研究，同時讓商家取得貨款、而消費者也能獲得預期的服務，若有任何一方無法履行義務，公正的第三者也能正確的根據交易資訊做出公正的判決。

五、參考文獻

[1] C. L. Lei, and C. I. Fan, "Low Computation Partially Blind Signatures for Electronic Cash," IEICE trans. On Fundamentals of Electronics, Communications and Computer Sciences, Vol. E81-A, No. 5, pp.818-824, 1998.

[2] C. I. Fan, and C. L. Lei, "User Efficient Blind Signatures, "IEE Electronics Letters, Vol. 34, No.6, pp.544-546, 1998.

[3] C. I. Fan, C. L. Lei, C. Y. Chang, and P. L. Yu, "An Efficient Divisible Blind Signature Scheme," Proceddings of the 8th Conference on Information Security, pp. 215-224, 1998.

[4] C. L. Lei, W. S. Juang, and C. I. Fan, "Anonymous Channel and Authentication in Wireless Communication," Proceedings of International Conference on Networking and Multimedia, pp. 227-234, Kaohsung, 1996.

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

[6] 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.

[7] 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.

[8] 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.

[9] Chin-Laung Lei, Wen-Sheng Juang, and Pei-Ling Yu, "Provably Secure Blind Threshold Signature Based on Discrete Logarithm," Proceedings of NCS'99, Volume III, pp198-205, 1999.

[10] AES homepage: http://www.nist.gov/aes

[11] R. Atkinson, "Security Architecture for the Internet Protocol," RFC 1825, Naval Research Laboratory, 1995.

[12] S. M. Bellovin, "Security Problems in the TCP/IP Protocol Suite," ACM Computer Communications Review, Vol. 19, No. 2, 1989.

[13] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, and M. Waidner, "iKP – A Family of Secure Electronic Payment Protocols," Extended Abstract, USENIX Workshop on Electronic Commerce. July 11-12, 1995.

[14] R. Braden, D. Clark, S. Crocker and C. Huitema, "Security in the Internet Architecture," RFC 1636, 1994.

[15] B. Cox. "Maintaining Privacy in Electronic Transactions," Information Networking Institute Technical Report TR 1994—8, Fall 1994.

[16] B. Cox, J. D. Tygar, and Marvin Sirbu, "NetBill Security and Transaction Protocol," Proceedings of the First USENIX Workshop in Electronic Commerce, pp. 77~88, 1995.

[17] E. B. Hickman and T. Elgamal, "The SSL Protocol, " Internet Draft. June 1995.

[18] R. Housley, W. Ford, W. Polk and D. Solo, "Internet Public Key Infrastructure, X.509 Certificate and CRL Profile," RFC [tbd], 1997.

[19] J. Ioannidis and M. Blaze, "Architecture and Implementation of Network-layer Security Under Unix," Proceedings of the USENIX Security Symposium, Santa Clara, Internet Draft, IP Encapsulating, November 1997.

[20] G. Jennifer, B. Steiner, C. Neuman and J. I. Schiller, "Kerberos: An Authentication Service for Open Network Systems," USENIX Winter Conference, pp. 191-202, February 1988.

[21] Mastercard International and Visa International, *Secure Electronic Transaction (SET) Specification*, June 1996, http://www.visa.com or http://www.mastercard.com.

[22] Mastercard International and Visa International, "Business Description.Draft for Public comment," Secure Electronic Transaction (SET) Specification, Book1, February 23, 1996.

[23] M. Sirbu and J. D. Tygar. "NetBill: an Internet Commerce System Optimized for Network Delivered Services," IEEE Personal Communications, pp. 34-39, August 1995.

[24] J. D. Tygar. "Atomicity in Electronic Commerce," the 21st ACM Principles of Distributed Computation, 1996.