電子付費系統安全之研究

梁道一、顏嵩銘

E-mail: 8809489@mail.dyu.edu.tw

摘 要

如果妳想要買一樣東西，妳可以帶著現金與商家面對面的交易，也可以利用郵購或是電話訂購的方式來完成一項交易買賣，當然，妳亦可以利用網路來進行交易，不過，網路交易與前述幾項不同，它所背負的職責不只是純粹的交易而已，還包括了交易進行時的各種安全與效益問題。 相信擁有信用卡的人應該都有一種相同的經驗，那就是每次都必須在信用卡上簽名之後才能完成一筆交易，因此，就延伸出兩種問題，一、妳的每一筆交易都在別人的掌控之中，二、妳買一瓶飲料時無法使用信用卡；或許有些人對這些沒什麼感覺，但是以隱私與便利性的觀點來看，似乎就有些問題了。 因此，在本文中，我們將提出一個以電子現金的方式來完成的匿名系統，匿名的範圍包括商家與銀行，而這種完全性的匿名功能中，我們加入了託管的功能在裡面，便於日後發生買賣糾紛或是蓄意詐時的管理。另外，對於只買一瓶飲料而又必須使用付費系統時，這就必須借助於小額付費的方式了，所以，我們也將討論有關於小額付費的效率，以及一些因效率而言伸出來的一些問題。

關鍵詞 : 小額付費 ; 電子現金 ; 匿名 ; 託管 ; 錢幣

目錄

參考文獻

[1] J. Abad Peiro, N. Asokan, M. Waidner, "Payment Manager-Overview," IBM Zurich Research Lab, 21 March 1996, SEMPER Activity Paper 212ZR054, http://www.zurich.ibm.com/ [2] P. Janson, M. Waidner, "Electronic Payment over Open Networks -A Technology Overview-," IBM Zurich Research Laboratory, CH-8803 Ruschlikon, Switzerland, Version 5/8/1995, http://www.ibm.com/crypto/ [3] N. Asokan, Pbillipe A. Janson, Michael Waidner, "The State of the Art in Electronic Payment Systems," IBM Zurich Research Lab., September 1997, http://www.zurich.ibm.com/ [4] N. Asokan, Phil Janson, Michael Waidner, "Electronic Payment Systems," IBM Research Division, Zurich Research Laboratory, CH-8803 Ruschlikon, Switzerland, ftp://ftp.cl.cam.ac.uk/users/rja14/ [5] Birgit Pfitzmann, Michael Waidner, "Properties of Payment Systems : General Definition Sketch and Classification," IBM Research Report RZ 2823(#90126), 05/06/1996, http://www.zurich.ibm.com/Technology/Security/ [6] Gerard Lacoste, "A Security Framework for the Global Electronic Marketplace," IBM France, August 1997, http://www.semper.org.

[7] Matthias Schunter, Michael Waidner, "Architecture and Design of a Secure Electronic Markerplace," 1996, ftp://ftp.cl.cam.ac.uk/users/rja14/ [8] Micheal Waidner, "Development of a Secure Electronic Marketplace for Europe," IBM Zurich Research Laboratory, September 1996, ftp://ftp.cl.cam.ac.uk/users/rja14/ [9] Dorothy E. Denning and Miles Smid, "Key Escrow Today," IEEE Communications Magazine, pp.58~68, September 1994.

[10] Thomas, Hans-Joachim Knobloch, Marcus Otten, Gustavus J. Simmons, Peer Wichmann, "Towards Acceptable Key Escrow Systems,"

Karlsruhe University Europen Institute fo System Security Am Fasanengarten 5 76128 Karlsruhe Germany.
[11] Ross Anderson, "Ueps - A Second Generation Electronic Wallet," Proceedings of ESORICS 92, Springer LNCS v 648 pp 411~418.
[12] D Chaum, "Security without Identification: Card Computers to make Big Brother Obsolete,"in Commun. ACM;28(10) October 1985, 1030-1004. http://digicash.support.nl/news/archive/ [13] Ronald L. Rivest and Adi Shamir, "PayWord and MicroMint: Two simple micropayment schemes," MIT Laboratory for Computer Science 545 Technology Square, May 7 1996.
[14] Ross Anderson, Charalampos Manifavas and Chris Sutherland, "NetCard - A Practical Electronic Cash System," Computer Lab. 1996.
[15] Anonymous, "Electronic Cash System," 1996.
[16] Mihir Bellare, Juan A. Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Michael Waidner, "iKP-A Family of Secure Electronic Payment Protocols," Working Draft, May 8 1995,
http://www.zurich.ibm.com/Technology/Security/publications/1995/ [17] Mihir Bellare, Juan A. Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Michael Waidner, "iKP-A Family of Secure Electronic Payment Protocols," Extended Abstract, July 12 1995, http://www.zurich.ibm.com/Technology/Security/publications/1995/ [18] Ralf Hauser, Michael Steiner, Michael Waidner, "Micro-payment based on iKP," IBM Zurich Research Laboratory, CH-8803 Ruschlikon Switzerland, August 21 1996
http://www.zurich.ibm.com/Technology/Security/publications/1995/.
[19] J. P. Boly, A. Bosselaers, A. Cramer, R. Michelsen, S. Mjolsnes, F. Muller, T. Pedersen, B. Pfitzmann, P. de Roij, B. Schoenmarkers, M. Schunter, L. Vallee, and M. Waidner, "The ESPRIT Project CAFE-High Security Digital Payment Systems," ESORICS '94, LNCS 875, Springer-Verlag, Berlin, 1994, pp. 217~230.
[20] H. Burk and A. Pfitzmann, "Digital Payment Systems Enabling Security and Unobservability," Computer & Security, Vol.9, No.5, 1989, pp.399~416. http://www.semper.org/sirene/publ/BuePf_89.ps.gz [21] David M. Kristol, Steven H. Low, Nicholas F. Maxemchuk, "Anonymous Internet Mercantile Protocol," AT&T Bell Lab., Murray Hill, NJ07974, March 17 1994.
[22] Steven H. Low, Nicholas F. Maxemchuk and Sanjoy Paul, "Anonymous Credit Cards," ACM Conference on Computer and Communication Security, November 2-4, 1994.
[23] Ronald L. Rivest, "Electronic Lottery Tickets as Micropayments," MIT Lab. for Computer Science. Available from rivest@theory.lcs.mit.edu.
[24] Sung-Ming Yen, P.Y. Kuo, "Improved Micro-Payment System," Proc. Of the 8th National Conference on Information Security, May 1998.
[25] Stanislaw Jarecki and Andrew Odlyzko, "An efficient micropayment system based on probabilistic polling," Proceedings 1997 Financial Cryptography Conference(Springer, 1997).
[26] R. L. Rivest, A. Shamir, and L. Adleman. "Amethod for obtaining digital signatures and public-key cryptosystems." Communications of ACM, 21, February 1978.
[27] Peter Wayner, "Digital Cash-Communication on The Net", Harcourt Brace & Company Asia Pte Ltd, 1998.
[28] Gennady Medvinsky, B. difford Nenuman, "NetCash : Adesign for practical electronic currency on the Internet" , ACM Conference on Computer and Communications Security, November 1993.