無線虛擬私有網路環境下群體導向安全機制之研究

劉彥含、曹偉駿

E-mail: 9121389@mail.dyu.edu.tw

摘 要

21世紀知識與數位經濟已經來臨，企業無不利用虛擬私有網路來保護內部資訊的傳遞。然而透過無線傳輸交易，達成隨時、隨地進行電子交易已經越來越被企業所重視。故如何在無線環境功能諸多限制下，設計出既安全又有效率的無線虛擬私有網路安全機制，是為本論文所要探討的課題。 傳統數位簽章機制，往往以單一簽名者為考量，然而在真實的電子商務中，我們也須考慮個人與群體之間的關係。故而本研究整合橢圓曲線密碼系統、群體導向簽章、自我認證公開金鑰密碼系統與群體導向鑑別加密法，使無線虛擬私有網路封包的傳輸能更具安全性，進而打造一個無線群體導向電子商務的安全環境。 本論文因植基於橢圓曲線密碼系統，較現存其他公開金鑰密碼系統可以更少位元數來達到相同的安全等級，相對地金鑰的儲存空間也大幅減少，因此非常適合應用於資源短缺的無線虛擬私有網路環境下。至於在計算複雜度與通訊傳輸量方面也大幅降低，遠少於其他公開金鑰系統。此外，本論文所提出之群體導向鑑別加密法，能使接收者在不需花費額外計算成本之情況下，將鑑別加密訊息轉換成一般具訊息回復的數位簽章。故本論文所提出的方法在實際應用方面，是非常適合於無線虛擬私有網路的環境。

關鍵詞 : 橢圓曲線密碼系統 ; 自我認證公開金鑰密碼系統 ; 群體導向簽章 ; 群體導向鑑別加密法 ; 無線虛擬私有網路

目錄

封面內頁 簽名頁 授權書 iii 中文摘要 v 英文摘要 vi 誌謝 viii 目錄 ix 圖目錄 xi 表目錄 xii 第一章 緒論 1 1.1 研究背景與動機 1 1.2 研究目的 3 1.3 研究架構 4 第二章 文獻探討 6 2.1 虛擬私有網路 6 2.1.1 簡介 6 2.1.2 主要採用技術 6 2.1.3 安全需求 8 2.2 無線虛擬私有網路(MVPN) 9 2.2.1 行動位址(Mobile IP) 9 2.2.2 無線虛擬私有網路簡介 10 2.2.3 建構以IPSec為基礎的MVPN所產生的問題 11 2.2.4 運作原理 11 2.3 橢圓曲線密碼系統(ECC) 21 2.4 自我認證公開金鑰系統 23 2.5 群體導向簽章機制 28 2.6 門檻式群體鑑別加密法 33 2.7 討論 38 第三章 適用於MVPN的群體導向安全機制之設計 40 3.1 群體導向簽章機制 40 3.1.1需要TKAC之協助 40 3.1.2不需要TKAC之協助 44 3.2 門檻式群體鑑別加密法 48 3.2.1 系統設置階段 48 3.2.2 註冊階段 49 3.2.3 鑑別加密階段 50 3.2.4 鑑別解密階段 51 3.2.5 簽章驗證階段 52 第四章 安全性分析 53 第五章 效能分析 56 5.1 計算時間複雜度 56 5.2 通訊傳輸量 59 第六章 結論與建議 61 參考文獻 62

參考文獻

[1] 胡國新, 「設計植基於自我驗證公開金鑰系統之安全線上電子拍賣機制」, 大葉大學資訊管理研究所碩士論文, 民國89年。

[2] 陳宗保, 「行動電子商務環境下安全協定之研究」, 大葉大學資訊管理研究所碩士論文, 民國90年。

[3] 許建隆, 「適用於群體導向應用之鑑別加密法」, 國立台灣科技大學資訊管理研究所博士論文, 民國91年。

[4] 張真誠、韓亮、賴溪松, 「近代密碼學及其應用」, 松崗圖書資料公司, 民國88年8月。

[5] 楊慶隆, " 從密碼技術談資訊安全 " , 無線網路暨網路安全研討會, 2001年十一月。 URL: http://www.ndhu.edu.tw/~comput/computer_c/net/wireless.htm [6] A. Inoue, M. Ishiyama, A. Fukumoto and T. Okamoto, " Secure Mobile IP Using IP security Primitives, " Enabling Technologies: Infrastructure for Collaborative Enterprises, 1997.

[7] A. Jurisic and A. Menezes, " Elliptic Curves and Cryptography, " Dr. Dobb ' s Journal, 1997, pp. 26-35.

[8] A. Marie, " Virtual Private Network Security, " Network Vol. 2000, No.7, Jul. 2000, pp. 11-14.

[9] A. Shamir, " How to Share a Secret, " Communications of the ACM, 1997, Vol. 22, pp. 612-613.

[10] B. Hancock, " Virtual Private Networks: What, Why, Where and How, " Network Security, Aug. 1997, pp. 8-11.

[11] C. C. Lin and C. S. Laih, " Cryptanalysis of Nyberg-Ruppel ' s message recovery scheme, " IEEE Communications Letters, Vol. 4, No.7, 2000.

[12] C. E. Perkins, " Mobility IP Support, " IETF RFC 2002, Oct. 1996.

[13] C. E. Perkins, " Mobile IP, " IEEE Communications Magazine, Vol. 35, No. 5, May 1997, pp. 84-99.

[14] C. E. Perkins, " Mobile IP: Design Principles and Practices, " Addison-Wesley Wireless Communications Sries, 1998.

[15] C. L. Hsu, and T. C. Wu, " Authenticated encryption scheme with (t, n) shared verification, " IEE Proceedings Computers and Digital Techiques, Vol. 145, No. 2, 1998, pp. 117-120.

[16] C. P. Schnorr, " Efficient Identification and Signatures for Smart Cards, " Advances in Cryptology, Proceedings of Crypto ' 89,

Springer-Verlag, 1990, pp. 339-351.

[17] C. Perkins, “ IP Encapsulation within IP, ” IETF RFC 2003, Oct. 1996.

[18] C. Perkins, “ Minimal Encapsulation within IP, ” IETF RFC 2004, Oct. 1996.

[19] D. Chaum and E. V. Heyst, “ Group Signature, ” Advances in Cryptology, Proceedings of Eurocrypt ’ 91, Springer Verlag, 1991, pp. 257-265.

[20] D. Chaum and M. E. Pedersen, “ Transferred cash grows in size, ” Advances in Cryptology, Proceedings of Crypto ’ 92, Springer-Verlag, 1992, pp. 390-407.

[21] D. F. Knuth, “ Seminumerical Algorithms, ” The Art of Computer Programming, Second Edition, Addison-Wesley, Reading, MA, Vol. 2, 1981.

[22] F. Bao and R. H. Deng, “ A signcryption svheme with signature directly verifiable by public key, ” Workshop on Public Key Cryptography, Spring-Verlag, 1998, pp. 55-59.

[23] FIPS 180-1, “ Secure Hash Standard, ” Federal Information Proceeding Standards Publication 46, U.S. Department of Commerce, 1995.

[24] G. R. Blakley, “ Safeguarding Cryptographic Keys, ” AFIPS 1979 National Computer Congerence, 1979, pp. 313-317.

[25] H. Petersen, and P. Horster, “ Self-Certified Keys Concepts and Applications, ” Proceedings of Communications and Multimedia Security ’ 97, 1997, pp. 102-116.

[26] Infonetics Research, “ Virtual Private Networks — A Partnership between Service Providers And Network Managers, ” The Networking Information Source, 1997.

[27] ISO 10118-3, “ Information technology — Security techniques — Hash functions — Part 3: Dedicated hash-functions, ” Internation Organization for Standardization, 1998.

[28] ISO/IEC 9796-3, “ Information technology — Security techniques — Digital signature schemes giving message recovery — Part3: Discrete logarithm based mechanisms, ” International Organization for Standardization, 2000.

[29] ISO/IEC 9796-4, “ Information technology — Security techniques — Digital signature schemes giving message recovery — Part4: Methods based on the discrete logarithm, ” International Organization for Standardization (draft), 1998.

[30] J. Postel, “ Internet Protocol, ” IETF RFC 791, Sep. 1981.

[31] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little and G. Zorn, “ Point-to-Point Tunneling Protocol, ” ITEF RFC 2637, Jul. 1999.

[32] L. Harn, ” Group-Oriented (t, n) Threshold Digital Signature Scheme and Digital Multi-signature ” , IEE Proceedings Computers and Digital and Digital Techiques, 1994, Vol. 141, No. 5, pp. 307-313.

[33] M. Abe and T. Okamoto, “ A signature scheme with message recovery as secure as discrete logaritm, ” IEICE Transactions on Fundamentals of Electronic Communications and Computer Science, Vol. E84-A, No. 1, 2001, pp. 197-204.

[34] M. Reid and S. Botzko, “ Control Protocol for Multimedia Communication, ” ITU-T Recommendation H. 245, 1998.

[35] M. Girault, “ Self-Certified Public Keys, ” Proceedings of EuroCrypt ’ 91, Lecture Notes in Computer Science, Vol. 547, Springer-Verlag, 1991, pp. 491-497.

[36] N. Koblitz, “ Elliptic Curve Cryptosystems, ” Mathematics of Computation, Vol. 48, No. 17, 1987, pp. 203-209.

[37] K. Nyberg and R. A. Ruppel, “ A new signature scheme based on the DSA given message recovery, ” Proceedings of the First ACM Conference on Computer and Communications Security, 1993, pp. 58-61.

[38] K. Nyberg and R. A. Ruppel, “ Message recovery for signature scheme based on the discrete logarithm problem, ” Designs Codes and Cryptography, Vol. 7, No. 1/2, 1996, pp. 61-81.

[39] R. L. Rivest, “ The MD5 message digest algorithm, ” Request for Comment RFC 1321, 1992.

[40] R. Kalakota and A. Whinston, “ Electronic Commerce — A Manager ’ s Guide, ” Addison Wesley, 1997.

[41] R. Rivest, A. Shamir, and L. Adleman, “ A Method for Obtaining Digitalsignatures and public-key cryptosystems , ” Communications of the ACM, Vol. 21, No. 2, 1978, pp. 120-126.

[42] S. Kent and R. Atkinson, “ IP Authentication Header, ” IETF RFC 2402, Nov. 1998.

[43] S. Kent and R. Atkinson, “ IP Encapsulating Security Payload, ” RFC 2406, Nov. 1998.

[44] S. Kent, R. Atkinson, “ Security Architecture for the Internet Protocol, ” IETF RFC 2401, Nov. 1998.

[45] S. Saeednia, “ Identity-Based and Self-certified Key-Exchange Protocols, ” Information Security and Privacy: ACISP ’ 97, 1997, pp. 303-313.

[46] S. Vanstone, “ Elliptic Curve Cryptosystem - the Answer to Strong, Fast Public-key Cryptography for Securing Constrained Environments, ” Information Security Technical Report, Vol. 2, No. 2, Elsevier, 1997, pp. 78-87.

[47] T. C. Wu, “ Digital Signature/Multisignature Schemes Giving Public Key Verification and Message Recovery Simultaneously, ” Computer Systems Science and Engineering, 2001.

[48] T. ElGamal, “ A public key cryptosystem and a signature scheme based on discrete logarithms, ” IEEE Transactions on Information Theory, Vol. IT-31, No. 4, 1985, pp. 469-472.

[49] T. P. Pedersen, “ A threshold cryptosystem without a trusted party, ” Advances in Cryptology , Proceedings of Crypto ’ 91, Springer-Verlag,

1991, pp. 522-526 [50] T. P. Pedersen, “ Non-interactive and information-theoretic verifiable secret sharing, ” Advances in Cryptology, Proceedings of Crypto ’ 91, Springer-Verlag, 1991, pp. 129-140.

[51] V. Varadharajan and Y. Mu, “ Preserving Privacy in Mobile Communications: A Hybrid Method, ” Personal Wireless, IEEE, April 1997 pp. 532-536.

[52] V. Tzvetkov and E. Sanchez , “ Mobile Virtual Private Network, ” Internet Draft, IETF, Sep. 2000. URL: http://search.ietf.org/internet-drafts/draft-sjostrand-mobileip-vpn- problem-stat-00.txt.

[53] V. S. Miller, “ Use of Elliptic Curves in Cryptography, ” Advances in Cryptology, Proceedings of Crypto ’ 82, Springer-Verlag, 1986, pp. 417-426.

[54] W. Caelli, E. Dawson, and S. Rea, “ PKI, Elliptic Curve Cryptography and Digital Signatures, ” Computer & Security, Vol. 18, No. 1, 1999, pp. 47-66.

[55] W. Simpson, “ PPP Challenge Handshake Authentication Protocol (CHAP), ” IETF RFC 1994, Aug. 1996.

[56] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn and B. Palter, “ Layer Two Tunneling Protocol "L2TP", ” IETF RFC 2661, Aug. 1999.

[57] Y. Desmedt and Y. Frankel, “ Shared Generation of Authenticators and Signatures, ” Advances in Cryptology , Proceedings of Crypto ’ 91, 1991, pp. 457-469.

[58] Y. Zhang, “ The Implication of End-to-End IPSec, ” Internet Draft, Mar. 2000.

[59] Y. S. Chang, T. C. Wu and S. C. Huang, “ ElGamal-Like Digital Signature and Multisignature Schemes Using Self-Certified Public Keys, ” The Journal of Systems and Software, 2000, pp. 99-105.