A Study on Group-Oriented Security Schemes in Mobile Virtual Private Network Environments

劉彥含、曹偉駿

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

ABSTRACT

When knowledge and digital economy have been coming in the twenty-first century, most enterprises protect the transmission of internal information using virtual private networks. However, transactions through wireless transmission anytime and anywhere have been paid much attention by enterprises. In this thesis, we focus on how to design secure and efficient schemes suitable for mobile virtual private networks subject to many restrictions of functions in mobile environments. Traditional digital signature schemes often consider single signature. Nevertheless, we must think about the relationship between an individual and groups in the real electronic commerce. Consequently, this study integrates the elliptic curve cryptosystems (ECC), group-oriented signature, self-certified public key cryptosystems and group-oriented authenticated encryption scheme so that the transmission of packets in mobile virtual private networks can be more secure. Also, we can develop further a secure environment of mobile group-oriented electronic commerce based on our proposed security schemes. Based on ECC, the proposed security schemes can possess fewer bits achieving the same security degree as other public key cryptosystems, and the key space needed can be also greatly reduced. Thus, ECC is very fit for applying in resource-limited mobile virtual private networks. As to the computing complexity and communication cost, they are also substantially decreased. Moreover, the proposed group-oriented authenticated encryption scheme can transform authenticated encryption message into a general digital signature with message recovery without requiring extra computing cost. Hence, in this thesis our proposed schemes are quite suitable for mobile virtual private networks in practical applications.

Keywords : Elliptic curve cryptosystems ; Self-certified public key cryptosystems ; Group-oriented signature ; Group-oriented authenticated encryption scheme ; Mobile virtual private networks

Table of Contents

REFERENCES

[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.