適用於多伺服器環境之兼具效率與安全的身分認證機制

謝燦榮、曹偉駿

E-mail: 9422452@mail.dyu.edu.tw

摘 要

為達到系統安全，一般常用身份認證機制，驗證使用者的合法性。傳統的身份認證機制中，系統存有使用者通行碼驗證資訊，易遭受偷竊及竄改的攻擊。目前免儲存通行碼驗證資訊的身份認證的作法，均需使用smart card，並結合公開金鑰密碼技術或赫序函數。雖然公開金鑰密碼技術所提供的安全性較高，但其建置成本及運算量也較高，然而赫序函數運算量則較低。在多伺服器環境中，使用者常需重複註冊及記憶多組密碼，造成使用上不便及管理不易，尤其當伺服器數量增加時，維護成本更高。本論文提出一個基於smart card，以橢圓曲線密碼系統結合牛頓內插法建構多伺服器登入認證機制，本機制具有以下特點：（1）使用者只需註冊一次，（2）系統不用儲存使用者密碼，（3）達到使用者與伺服器雙向認證，（4）使用者可自由選擇及變更密碼，（5）系統可自動刪除過期使用者，（6）新增伺服器時，系統不需整個重新建置，只需異動少部份，（7）在登入驗證後可同時產生使用者與伺服器間的交談金鑰。因此，本論文所提出之兼具效率與安全的身份認證機制是非常適用於真實環境中。

關鍵詞 : Smart card ; 公開金鑰密碼系統 ; 赫序函數 ; 身份認證 ; 多伺服器

目錄

參考文獻

[1] 洪國寶,周伯錕,＂以smart card為基礎之遠端使用者身分認證,＂Communications of the CCISA,vol.9, no.3, June 2003.

[2] 曾志光，巫坤品 譯＂密碼學與網路安全:原理與實務第二版＂.

[3] 賴溪松, 韓亮, 張真誠著，＂近代密碼學及其應用＂, 92 [4] A. Jurisic, and A.J. Menezes,＂Elliptic Curves and Cryptography,＂Dr. Dobb＇s Journal, pp. 26-35, 1997.

[5] A. Shamir,＂Identity-Based Cryptosystems and Signature Schemes,＂Proceedings of CRYPTO＇84, pp. 47-53, 1985.

[6] B. Ingu et al.,＂Online Fingerprint Verification System using Direct Minutia Extraction,＂Proceeding ISCA 13th Int. Conf. Computer Applications in Industry and Engineering, pp. 120-123, 2000.

[7] C. C. Chang and S. J. Hwang,＂Using Smart Cards to Authentication Remote Passwords,＂Computer Mathematics with Applications, vol. 26, no. 7, pp. 19-27, 1993.

[8] C. H. Lin and Y. Y. Lai,＂A Flexible Biometrics Remote User Authentication Scheme,＂Computer Standards and Interfaces vol: 27, no. 1, pp. 19-23, November, 2004.

[9] C. K. Chan and L. M. Cheng,＂Cryptanalysis of A Remote User Authentication Scheme Using Smart Cards,＂IEEE Transactions on Consumer Electronics, vol. 46, no. 4, pp. 992-993, November 2000.

[10] C. K. Chan and L. M. Cheng,＂Remarks on Wang-Chang＇s Password Authentication Scheme,＂Electronics Letters, vol. 37, no. 1, pp. 22-23, 2001.

[11] C. K. Chan and L. M. Cheng,＂Cryptanalysis of a Timestamp-Based Password Authentication Scheme,＂Computers and Security, vol. 21, no. 1, pp. 74-76, 2002.

[12] D.E. Knuth,3rd edition, The Art of Computer Programming ,vol. 2,1998.

[13] D.L. Mills, Internet time synchronization: the network time protocol, IEEE Transactions on Communications 1482 – 1493, 1991.
[14] G. Horng, “ Password Authentication without Using Password Table, ” Information Processing Letters 55, pp. 247-250, 1995.
[15] G. B. Purdy, “ A High Security Log-in Procedure, ” Communications of the Association for Computing Machinery, vol. 17, no. 8, pp. 442-445, August 1974.
[16] H. K. Lee, J. O. Chio, C. O. Kim and J. S. Song, “ Password Based Strong Authentication Protocol for Remote User Access using Public Key cryptosystem, ” IEICE Trans.Fundamentals/Commun./Electron./Inf.&Syst.,vol.E85-A/B/C/D, no. 1, pp. 1-11, September , 2004.
[17] H. Y. Chien, J. K. Jan and Y. M. Tseng, “ A Modified Remote Log In Authentication Scheme Based on Geometric Approach, ” Journal of Systems and Software, vol. 55, pp. 287-290, 2001.
[18] H. Y. Chien, J. K. Jan and Y. M. Tseng, “ An Efficient and Practical Solution to Remote Authentication: Smart Card, ” Computers and Security, vol. 21, no. 4, pp. 372-375, 2002.
[19] H. M. Sun, “ An Efficient Remote User Authentication Scheme using Smart Cards, ” IEEE Transactions on Consumer Electronics, vol. 46, no. 4, pp. 958-961, November 2000.
[20] H. M. Sun, “ Cryptanalysis of Password Authentication Schemes with Smart Cards, ” The 11th Conference on Information Security, pp. 221-223, May, 2001.
[21] IEEE P1363 working Group, “ IEEE P1363 standard specifications for public key cryptography ” [22] I. Lin, M. Hwang and L. Li, “ A New Remote User Authentication Scheme for Multi-server Architecture, ” Future Generation Computer Systems, ” vol. 19, pp. 13-22, 2003.
[23] J. J. Shen, C. C. Lin and M. S. Hwang, “ A Modified Remote User Authentication Scheme using Smart cards, ” IEEE Transactions on Consumer Electronics, vol. 49, no. 2, pp. 414-416, May 2003.
[24] J. K. Jan and Y. Y. Chen, “ ‘ Paramita Wisdom ’ Password Authentication Scheme without Verification Tables, ” Journal of Systems and Software, vol. 42, pp. 45-57, 1998.
[25] J. K. Lee, S. R. Ryu and K. Y. Yoo, “ Fingerprint-Based Remote User Authentication Scheme using Smart Cards, ” Electronics Letters, vol. 38, no. 12, pp. 554-555, 2002.
[26] L. Harn, D. Hwang and C. S. Laih, “ Password Authentication using Public-Key Cryptography, ” International Journal of Computer and Mathematics with Applications, vol. 18, no. 12, pp. 1001-1017, 1989.
[27] L. Fan, J. H. Li and H. W. Zhu, “ An Enhancement of Timestamp-Based Password Authentication Scheme, ” Computers and Security, vol. 21, no. 7, pp. 665-667, 2002.
[28] L. Lamport, “ Password Authentication with Insecure Communication, ” Communications of ACM, vol. 24, pp. 770-772, 1981.
[29] MD5 Collisions, （http://free.tnc.edu.tw/modules/news）.
[30] M. Girault, “ Self-certified public keys, ” Advances in Cryptology:EuroCrypt ’91, Lecture Notes in Computer Science, vol. 547,Springer-Verlag, pp. 491-497, 1991.
[31] M. Kumar, “ New Remote User Authentication Scheme using Smart Cards, ” IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 597-600, May 2004.
[32] M. S. Hwang and L. H. Li, “ A New Remote User Authentication Scheme using Smart Cards, ” IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp. 28-30, February 2000.
[33] M. S. Hwang, C. C. Lee and Y. L. Tang, “ A Simple Remote User Authentication Scheme, ” Mathematical and Computer Modeling, vol. 36, pp. 103-107, 2002.
[34] N. K. Ratha and A. K. Jain, “ A Real-Time Matching System for Large Fingerprint Databases, ” IEEE Transactions Pattern Anal. Mach. Intell., vol. 18, pp. 799-813, 1996.
[35] N. Koblitz, A. Menezes, S. Vanstone, The state of elliptic curve cryptograph, Designs, Codes and Cryptography, 173-193,19(2000).
[36] N. Koblitz, “ Elliptic curve cryptosystems, ” Mathematics of Computation, vol. 48, no. 17, pp. 203-209 , 1987.
[37] P. Peyret, G. Lisimaque and T. Y. Chua, “ Smart Cards Provide very High Security and Flexibility in Subscribers Management, ” IEEE Transactions on Consumer Electronics, vol. 36, no. 3, pp. 744-752, 1990.
[38] R. E. Lennon, S. M. Matyas and C. H. Meyer, “ Cryptographic Authentication or Time-Invariant Quantities, ” IEEE Transactions on Communications, vol. com-29, no. 6, pp. 773-777, June 1981.
[39] R. Riverst, A. Shamir and L. Adleman, “ A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, ” Communications of the ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978.
[40] S. J. Wang and J. F. Chang, “ Smart Card Based Secure Password Authentication Scheme, ” Computers and Security, vol. 15, no. 3, pp. 231-237, 1996.
[41] 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, pp. 78-87,1997.
[42] T. Y. Hwang, “ Passwords Authentication Using Public-Key Encryption, ” Proceedings of 1983 International Carnahan Conference on Security Technology Zurich, Switzerland, pp. 35-38, October, 1983.
[43] T. Hwang, Y. Chen and C. S. Laih, “ Non-Interactive Password Authentication without Password Tables, ” 1990 IEEE Region 10

Conference on Computer and Communication Systems, Hong Kong, pp. 429-431, September 1990.
[44] T. ElGamal, “ A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms, ” IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, July 1985.
[45] T. H. Chen, W. B. Lee and G. Horng, “ Secure SAS-like Password Authentication Schemes, ” Computer Standards and Interfaces vol. 27, mo. 1, pp. 25-31, November, 2004.
[46] The status of MD5 after a Recent Attack RSA Lab ’ s 1996.
[47] V.S. Miller., “ Use of Elliptic Curves in Cryptography, ” Advances in Cryptology:Crypto ’ 85, Springer-Verlag,1986, pp. 417-426.
[48] W. H. Yang and S. P. Shieh, “ Password Authentication Schemes with Smart Cards, ” Computers and Security, vol. 18, no. 8, pp. 727-733, 1999.
[49] W. J. Tsaur, C. C. Wu and W. B. Lee, “ A Smart Card-Based Remote Scheme for Password Authentication in Multi-Server Internet Services, ” Computer Standards and Interfaces, vol. 27, no. 1, pp. 39-51, November, 2004.
[50] W. J. Tsaur, “ Several security schemes constructed using ECC-based self-certified key cryptosystems, ” Applied Mathematics and Computation, Available online 2004.
[51] W. S. Juang, “ Efficient Multi-server Password Authenticated Key Agreement using Smart Cards, ” IEEE Transactions on Consumer Electronics, vol. 50, no. 1 pp. 251-255 February 2004.