動態的多伺服器密碼認證機制

王興翰、曹偉駿

E-mail: 9806264@mail.dyu.edu.tw

摘 要

隨著網際網路的蓬勃發展，資訊安全議題已被大家所重視，為了能有效地確保網路通訊的安全，各式各樣的安全機制被提出且應用在各個不同的環境中。這些安全機制大都必須滿足兩項基本的安全需求，如使用者的身份認證和傳輸資料的保密。要達成使用者的身份認證有許多方法，其中，通行碼具有簡單、容易記憶、成本低廉等特性，因此使用通行碼來進行身份認證是目前廣被大眾所接受的一種方式。然而，將傳統的身份認證機制應用在多伺服器環境中，系統須保存著使用者通行碼等資訊，致使通行碼易遭受偷竊及竄改的攻擊，使得免儲存通行碼驗證資訊的身份認證方法被提出，其藉助智慧卡(smart card)，並結合公開金鑰密碼技術或赫序函數來達成。但在這些機制當中，皆未提及如何有效地新增伺服器。因此，本研究提出一個基於智慧卡，並以雙線性(Bilinear Pairing)密碼系統結合牛頓內插法(Newton Interpolating Polynomial)，來建構動態多伺服器密碼認證機制，其主要特色兼顧運算量與安全性，特別是在新增與刪除伺服器時能節省建置成本。

關鍵詞 : 多伺服器、雙線性配對、密碼認證、智慧卡

目錄

參考文獻

Boneh, D., & Franklin, M. (2001). Identity-based encryption from the weil pairing. Crypto 2001, LNCS , 2139, 213-229.Boneh, D., Lynn, B., & Shacham, H. (2001). Short signatures from the Weil pairing. Crypto 2001 LNCS, 17(4), 297-319.Chang, C. C., & Hwang, S. J. (1993). Using smart cards to authenticate remote passwords. Computers and Mathematics with Applications, 26(7), 19-27.Chang, C. C., & Wu, T. C. (1995). Remote scheme for password authentication based on theory of quadratic residues. Computer Communications , 936 – 942.Chang, C. C. & Lee, S. J. (2004). An efficient and secure multi-server password authentication scheme using smart cards. Proceedings of the 2004 International Conference

on Cyberworlds (pp. 417-422).Du, H., & Wen, Q. (2009). Efficient and provably-secure certificateless short signature scheme from bilinear pairings. Computer Standards & Interfaces, 31(2), 390-394.Galbraith, S. (2001). Supersingular curves in cryptography. Proc. Of Asiacrypt' 01,LNCS (pp. 495-513).Galbraith, S. D., Paterson, K. G., & Smart, N. P. (2008). Pairings for cryptographers. Discrete Applied Mathematics. 156(1), 3113-3121.Geng, J., & Zhang, L. (2008). A dynamic ID-based user authentication and key agreement scheme for multi-server environment using bilinear pairings. Workshop on Power Electronics and Intelligent Transportation System, 35(1), 33-37.Hsiang, H. C., & Shih, W. K. (2009). Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces , doi:10.1016/j.csi.2008.11.002.Hwang, R. J., & Shiau, S. H. (2007). Provably efficient authenticated key agreement protocol for multi-servers. The Computer Journal Advance Access published , 50(5), 602-615.Joux, A. (2002). The weil and tate pairings as building blocks for public key cryptosystems. LNCS (pp. 20-32).Juang, W. S. (2004). Efficient multi-server password authenticated key agreement using smart cards. IEEE Transactions on Consumer Electronics, 50(1), 251-255.Lee, N. Y., Wu, C. N., & Wang, C. C. (2008) Authenticated multiple key exchange protocols basedon elliptic curves and bilinear pairings. Computers and Electrical Engineering, 34(1), 12-20.Li, L., Lin, I., & Hwang, M. (2001). A remote password authentication scheme for multi-server architecture using neural networks. IEEE Trans, (pp. 1498-1504). Neural Netw.Liao, Y. P., & Wang, S. S. (2009). A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces, 24-29.Lin, I. C., Hwang, M. S., & Li, L. H. (2003). A new remote user authentication scheme for multi-server architecture. Future Generation Computer Systems, 13-22.Menezes, A., Okamoto, T., & Vanstone, S. (1993). Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transaction on Information Theory, 1639-1646.Menkus, B. (1989). Understanding the use of passwords. Computer sand Security 7, 132-136.Mills, D. J. (1991). Internet time synchronization: The network time protocol, IEEE Transactions on Communications, 39(10), 1484-1493.Mohammed, E., Emarah, A. E., & El-Shennawy, K. (2001). Elliptic curve cryptosystems on smart cards. 2001 IEEE 35th International Carnahan Conference, (pp. 213-222).Paterson, K. G. (2002). ID-Based signatures from pairings on elliptic curves. Electronics Letters , pp. 1025-1026.Pfleeger, C. P. (1997). Security in computing. (2nd edition), PrenticeHall. NJ.Purdy, P. G. (1974). A high security login procedure. Communications of the ACM 17, (pp. 442-445).Sauer, T. (2005). Numerical Analysis. Addison-Wesley .Scott, M. N. Costigan & Abdulwahab, W. (2006). Implementing cryptographic pairings on smartcards. In Cryptology ePrint Archive. Available: http://eprint.iacr.org/2006/144.pdfSmart, N. P. (2002). Identity-based authenticated key agreement protocol based on Weil pairing. Electronic Letters, 38(13), 630-632.Tsaur, W. J. (2005). Several security schemes constructed using ECC-based self-certified public key cryptosystems. Applied Mathematics and Computation, 168(10), 447-464.Tsaur, W. J., Wu, C. C., & Lee, W. B. (2004). A smart card-based remote scheme for password authentication in multi-server Internet services. Computer Standards & Interfaces, 27(4), 39-51.Tseng, Y. M., Wu, T. Y., & Wu, J. D. (2008). A Pairing-based user authentication scheme for wireless clients with smart cards. Institute of Mathematics and Informatics, Vilnius, 19(2), 285-302.Tsuar, W. J., Wu, C. C., & Lee, W. B. (2001). A flexible user authentication for multi-server internet services. Networking-JCN2001LNCS , (pp. 174-183).Wang, S. B., Cao, Z., Raymond Choo, K. K., & Wang, L. (2009). An improved identity-based key agreement protocol and its security proof. Information Sciences, 179(30), 307-318.