於車載網路之多伺服器密碼認證機制

王常力、曹偉駿

E-mail: 322094@mail.dyu.edu.tw

摘 要

近年來，由於無線網路設備的普及，使得車載網路(vehicular ad hod network)應用的發展也慢慢受到了大家的重視。在這注重個人隱私的社會上，資訊安全也同樣的備受矚目，所以為了能有效地確保網路通訊的安全，在車載網路的環境下建構一個兼具隱私保護的身分認證機制，已是必需的。而在這麼多種的身分認證機制中，又以通行碼是最為普遍的，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最廣被大眾所接受的一種方式。近年來已有學者提出在車載網路的環境下，以橢圓曲線密碼系統(elliptic curve cryptosystems, ECC)建構一套單伺服器密碼認證機制，然而，其運算量較大且並未考慮多伺服器的應用環境，導致降低建置伺服器時所浪費的成本，特別是在車載網路這種流動性大的環境下，因此，本研究基於雙線性配對(bilinear pairing)且結合牛頓內插法建構出一個適用於車載網路環境下的多伺服器(multi-server)密碼認證機制，其主要特色兼顧運算量與安全性，特別是在新增及刪除伺服器時能節省建置成本。

關鍵詞 : 車載網路、多伺服器、雙線性配對、密碼認證

目錄

參考文獻

一、英文部份 Adler, P. S. (1993). Time-and-motion regained. Harvard Business Review, 71(1), 97-108. Bernardos, C. J., Soto, I., & Calderon, M. (2007). Vaton: vehicular ad hoc route otimisation for NEMO. Computer Communication, 30 , 1765-1784. Boneh, D., & Franklin, M. (2001). Identity-based encryption from the weil pairing. Lecture Notes in Computer Science, 2139 , 213-229. Boneh, D., Lynn, B., & Shacham, H. (2001). Short signatures from the Weil pairing. Lecture Notes in Computer Science, 2248 , 514-532. 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, 18 , 936-942. Chang, J., & Lee, S. J. (2004). An efficient and secure multi-server password authentication scheme using smart cards. Proceedings of the International Conference on Cyberworlds (pp. 417-422). Tokyo, Japan: Tokyo Institute of Technology. Das, M. L., Saxena, A., Gulati, V. P., & Phatak, D. B. (2006). A novel remote user authentication scheme using bilinear pairings. Computers & Security, 25 , 184-189. 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. Lecture Notes in Computer Science, 2248 , 495-513. Green, M., & Hohenberger, S. (2008). Blind identity-based encryption and simulatable oblivious transfer. Lecture Notes in Computer Science, 4833 , 265-282. 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, 31(1), 24-29. Hwang, R. J., & Shiau, S. H. (2007). Provably efficient authenticated key agreement protocol for multi-servers. The Computer Journal, 50(5), 602-615. Jinyuan, S., & Yuguang, F. (2009). Defense against misbehavior in anonymous vehicular ad hoc networks. Ad Hoc Networks, 7 , 1515-1525. Joux, A. (2002). The Weil and Tate pairings as building blocks for public key cryptosystems. Lecture Notes in Computer Science, 2369 , 20-32. Juang, W. S. (2004). Efficient multi-server password authenticated key agreement using smart cards. Transactions on Consumer Electronics, 4(1), 251-255. Klaus, P., & Hannes, F. (2008). A privacy aware and efficient security infrastructure for vehicular ad hoc networks. Computer Standards & Interfaces, 30 , 390-397. Lee, N. Y., Wu, C. N., & Wang, C. C. (2008). Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings. Computers and Electrical Engineering, 34 , 12-20. Li, C. T., Hwang, M. S., & Chu, Y. P. (2008). A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. Computer Communications, 31 , 2803-2814. Li, L., Lin, I., & Hwang, M. (2001). A remote password authentication scheme for multi-server architecture using neural networks. IEEE Transaction on Neural Networks, 12(6), 1498-1504. Liao, Y. P., & Wang, S. S. (2009). A secure dynamic id based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces, 31(1), 24-29. Lin, C. Y., Wu, T. C., Zhang F., & Hwang, J. J. (2005). New identity-based society oriented signature schemes from pairings on elliptic curves. Mathematics and Computation, 160 , 245-260. Lin, I. C., Hwang, M. S., & Li, L. H. (2003). A new remote user authentication scheme for multi-server architecture. Future Generation Computer Systems, 19(1), 13-22. Menezes, A., Okamoto, T., & Vanstone, S. (1993). Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transaction on Information Theory, 39 , 1639-1646. Mohammed, E., Emarah, A. E., & Ei-Shennawy, K. (2001). Elliptic curve cryptosystems on smart cards. 2001 IEEE 35th International Carnahan Conference on Security Technology (pp. 213-222). London: IEEE. Paterson, K. G. (2002). Id-based signatures from pairings on elliptic curves. Electronics Letters, 38(18), 1025-1026. Purdy, P. G. (1974). A high security log-in procedure. Communications of the Association for Computing Machinery, 17(18), 442-445. Raya, M., & Hubaux, J. P. (2005a). The security of vehicular ad hoc networks. Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (pp. 11-21). Alexandria, Virginia: Association for Computing Machinery. Raya, M., & Hubaux, J. P. (2005b). Security aspects of inter-vehicle communications. Proceedings of the 5th Swiss Transport Research Conference. Ascona, Switzerland: Swiss Transport Research Conference. Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. Journal of Computer Security, 15 , 39-68. Raya, M., Jungels, D., Papadimitratos, P., Aad, I. & Hubaux, J. P. (2006). Certificate revocation in vehicular networks. Laboratory for Computer Communications and Applications (LCA-Report-2006-006). Lausanne, Switzerland: Swiss Federal Institute of Technology. Sauer, T. (2005). Numerical Analysis. Reading, Massachusetts: Addison-Wesley. Smart, N. P. (2002). Identity-based authenticated key agreement protocol based on Weil pairing. Electronic Letters, 38 , 630-632. Tsaur, W. J. (2005). Several security schemes constructed using ECC-based self-certified public key cryptosystems. Applied Mathematics and Computation, 168 , 447-464. Tsuar, W. J., Wu, C. C., & Lee, W. B. (2001). A flexible user authentication for multi-server internet services. Lecture Notes in Computer Science, 2093 , 174-183. 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(1), 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, 19(2), 285-302. Tzeng, W. G. (2002). Efficient 1-out-n oblivious transfer schemes. Lecture Notes in Computer Science, 2274 , 359-362. Wang, N. W., Huang, Y. M., & Chen, W. M. (2007). A novel secure communication scheme in vehicular ad hoc networks. Computer Communications, 31(12), 2827-2837. Wang, S. B., Cao, Z., Raymond, C. K. K., & Wang, L. (2009). An improved identity-based key agreement protocol and its security proof. Information Sciences, 179(3), 307-318. Yang, C. C., Tang, Y. L., Wang, R.C., & Yang, H. W. (2005). A secure and efficient authentication protocol for anonymous channel in wireless communications. Mathematics and Computation, 169(2), 1431-1439. Zhang, J., Ma, L., Su, W., & Wang, Y. (2007). Privacy-preserving authentication based on short group signature in vehicular networks. Proceedings of the The First International Symposium on Data, Privacy, and E-Commerce (pp. 138-142). Washington, District of Columbia: IEEE Computer Society.