社區醫療資訊系統之安全機制研究

賴惠美、曹偉駿

E-mail: 9422443@mail.dyu.edu.tw

摘 要

近年來隨著產業外移、人口老化、罹患慢性病比率節節上升等問題日益嚴重，因此各醫院均積極投入社區醫療，營造社區健康生活，落實預防勝於治療的理念。而社區醫療資訊系統（Community HealthCare Information System，CHIS）在於結合了資訊科技與醫療從事人員的專業知識，提供社區醫療成員全方位的醫療照顧。可以有效提昇病患健康管理的便利性，同時讓社區照護網絡成員得以凝聚共識，達到資源分享的目的。 目前CHIS運作方式共分為三種：第一種利用書面方式，記錄該病患之醫囑資料，將帶回的書面資料統一輸入至醫療資訊系統；第二種則是將病患基本資料轉檔至筆記型電腦中，由使用者攜帶至社區，依實際需要查詢或異動至筆記型電腦，事後帶回醫院端再上傳至主機；第三種則是透過VPN，由使用者輸入ID及密碼後登入醫院端主機，查詢病患相關資料。其中，第一種作法之缺點為：資料辨識不易（如：筆跡潦草）、無法即時檢核內容正確性、書面文件容易遺失或污損等問題；第二種之缺點則有：資料容易遺失或遭篡改、洩露病人隱私等問題。第三種作法雖提供醫療人員方便又即時的操作介面，但卻無法滿足病患在家即可查詢健康資訊、以及醫師到社區從事居家服務時，提供更廣泛且方便的資訊。因此，本研究針對在網際網路的環境中，根據資訊安全管理標準（BS7799-2）分析及整理社區醫療資訊系統存在的安全需求，並針對身份辨識、資料加解密、存取控制提出可行的安全機制。此外，本論文亦進一步實際開發CHIS，真正做到兼具管理面、技術面與實務應用面。 關鍵字：社區醫療、電子病歷、BS7799、角色存取控制、自我驗證公開金鑰密碼系統、橢圓曲線密碼

關鍵詞 : 社區醫療 ; 角色存取控制 ; 自我驗證公開金鑰密碼系統 ; 電子病歷

目錄

參考文獻

[1] 林昇豪，「台灣地區醫療電子商務實施現況初探」，國立陽明大學醫務管理研究所碩士論文，民國八十九年（指導教授:黃松共） [2] 吳依凡，「醫療資源可近性對個人醫療制用的影響——台灣地區的實證研究」，中央大學產業經濟研究所碩士論文，民國九十二年（指導教授:蔡偉德） [3] 洪國寶,周伯錕,「以智慧卡為基礎之遠端使用者身分認證」,Communications of the CCISA,vol.9,no.3,June 2003 [4] 郭年真，「醫院應用網站現況與影響因素研究」，國立臺灣大學醫療機構管理研究所碩士論文，民國九十年（指導教授:鍾國彪、楊銘欽） [5] 陳宗保，「行動電子商務環境下安全協定之研究」，大 葉 大 學資訊管理學系研究所碩士論文，民國九十年（指導教授:曹偉駿）

[6] 陳慶穎，「以角色定義為基礎之社區醫療人力資源管理系統」，暨南大學資訊管理研究所碩士論文，民國九十二年 （指導教授:俞旭昇） [7] 陳祥輝，「資訊系統的安全管理與鑑識軌跡設計－基於ＭＩＢ與資料庫之探討」，中國文化大學資訊管理研究所碩士論文，民國八十八年（指導教授:蔡敦仁） [8] 陳源昌，「網路醫療新紀元」，醫望，vol34, 2001，pp..67-72 [9] 葉相妤，「運用BS7799檢測醫療院所資訊安全管理作業文件之研究」，國立陽明大學衛生資訊與決策研究所碩士論文，民國九十一年（指導教授:郭旭崧、王大為） [10] 趙咸欣，「應用於社區醫療資訊的結構化表單管理系統」，暨南大學資訊管理研究所碩士論文，民國九十二年（指導教授:俞旭昇） [11] 劉益成，「院際醫療資訊交換平台之設計－以轉診為例」，長庚大學資訊管理研究所碩士論文，民國九十二年（指導教授:蔡榮隆） [12] 劉廷楷，「電子病歷分享系統中安全技術之設計與實作」，東海大學資訊工程與科學系碩士論文，民國九十二年（指導教授:林祝興）
[13] 賴溪松，「醫療資訊安全之發展與未來趨勢」，建構優質之醫療體系資通安全管理機制研討會，2004 [14] 賴溪松、韓亮、張真誠，「近代密碼學及其應用」，松崗圖書資料公司，民國八十八年八月。
[15] 謝清佳、吳琮璠，「資訊管理理論與實務」，智勝文化事業有限公司，民國八十九年五月。
[16] 中華民國醫療資訊協會網站， http://www.hl7.org.tw，2002 [17] 中央健康保險局網站， http://www.nhi.gov.tw [18] 行政院衛生署，http://www.doh.gov.tw [19] 行政院衛生署醫療憑證管理中心， http://hca.doh.gov.tw/HCA/default.jsp [20] A.E. Hutt, ” Management ’ s Approach to Effective Information Technology Risk Analysis and Management, ” Information Management & Computer Security,Vol. 4-1,pp.27-28,1995 [21] A. Jurisic, A.J. Menezes, “ Elliptic curves and cryptography, ” Dr. Dobb ’ s Journal, 1997, pp. 26-35.
[22] A. Shamir, “ Identity-Based Cryptosystems and Signature Schemes, ” Proceedings of CRYPTO ’ 84, pp.47-53， 1985 [23] B. Blobel,R. Francis , “ A systematic approach for analysis and design of secure health information systems, ” Internation Journal of Medical Information ,Vol. 62 ,pp.51-78,2001 [24] B. Dixie, et al. ” PCASSO:a design for secure communication of personal health information via the internet, ” International Journal of Medical Informatics, Vol. 54,pp.97-104,1999 [25] C. Gunther, “ An identity-based key-exchange protocol, ” Advances in Cryptology EuroCrypt ’ 91, Lecture Notes in Computer Science, Vol. 547, Springer-Verlag, 1991, pp.29-37.
[26] C.H. Lin, Y.Y. Lai, “ A flexible biometrics remote user authentication scheme， ” Computer Standards & Interfaces 27,pp.19-23,2004 [27] C.P. Schnorr, “ Efficient identification and signatures for smart cards, ” Advances in Cryptology: Crypto ’ 89, Springer-Verlag,1990, pp.339-351.
[28] D. Ferraiolo, et al. “ Proposed NIST Standard for Role-Based Access Control, ” ACM Transactions on Information and System Security, Vol 4,No. 3,August 2001,224-274 [29] D. Gritzalis, C. Lambrinoudakis , “ A security architecture for interconnecting health information systems， ” International Journal of Medical Informatics ,Vol. 73,pp.305-309,2004 [30] D.B. Parker, ” Information Security in a Nutshell, ” Information Systems Security,1997 [31] D. Hunter , “ Managed card:Disease management, ” British Medical Journal ,Vol.315:50-3,1997 [32] F. Cao,H.K. Huang,and X.Q. Zhou, ” Medical image security in a HIPAA mandated PACS environment, ” Computerized Medical Imaging and Graphics ,Vol.27,pp.185-196,2003 [33] G. Schadow, “ HL/7 V3.0 Data Type, ” Regenstrief Institute for Health Care,1999 [34] H. Petersen, P. Horster, “ Self-certified keys concepts and applications, ” Proceedings of Communications and Multimedia Security ’ 97, 1997, pp. 102-116.
[35] H. Takeda, et al. “ An assessment of PKI and networked electronic patient record system: lessons learned from real patient data exchange at the platform of OCHIS (Osaka Community Healthcare Information System), ” International Journal of Medical Informatics, Vol.73, pp.311-316,2004 [36] 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 [37] 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 [38] K.S.Carrison et al. “ Implementation of ISO17799 and BS7799 in picture archiving and communication system: local experience in implementation of BS7799 standard, ” International Congress Series,Vol.1256 , pp.311-318,2003 [39] M. Girault, “ Self-certified public keys, ” Advances in Cryptology:EuroCrypt ’ 91, Lecture Notes in Computer Science, Vol. 547, Springer-Verlag, 1991, pp. 491-497.
[40] M. S. Hwang , 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 [41] M. van der Haak, et al. “ Data security and protection in cross-institutional electronic patient records, ” International Journal of Medical Informatics, Vol. 70,pp.117-130,2003 [42] N. Koblitz, “ Elliptic curve cryptosystems, ” Mathematics of Computation, Vol. 48, No. 17, 1987, pp. 203-209.
[43] P. Ruotsalainen, ” A cross-platform model for secure Electronic Health Record communication, ” International Journal of Medical Informatics ,Vol.73,pp.291-295,2004 [44] P. Thomas, ” Implementing BS7799 in the UK National Health Service, ” ,Computer Fraud & Security Vol.2003,Issue. 5,2003,pp.10-13.
[45] R. Bhatti, et al. “ Access Control in Dynamic XML-based Web-Services with X-RBAC, ” International Conference on Web Services, Las Vegas, June 2003.
[46] 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.120-126.1978 [47] S. Kim, S. Oh, S. Park, and D. Won, “ On saeednia ’ s key-exchange protocols, ” KICS (Korean Institute of Communication Sciences) Conference, Vol. 17, No. 2, Korea, 1998, pp.1001-1004.
[48] S. Saeednia, “ Identity-based and self-certified key-exchange protocols, ” Information Security and Privacy: ACISP ’ 97, 1997, pp. 303-313.
[49] S. Saeednia, “ A note on Girault s self-certified model, ” Information Processing Letters 86 ,2003, pp. 323 – 327.
[50] 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.
[51] T.C. Wu, Y.S. Chang and T.Y. Lin, “ Improvement of saeednia ’ s self-certified key exchange protocols, ” IEEE Electronic Letters,Vol 34,

No 11, May 1998, pp. 1094-1095.
[52] T.C. Wu, “ Digital signature/multi signature schemes giving public key verification and message recovery imultaneously, ” Computer Systems Science and Engineering, 2001.
[53] T. ElGamal, ” A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms, ” IEEE Transactions on Information Theory,Vol.31,No.3,pp.469-472,1985 [54] T. Finne, ” Information Systems Risk Management:Key Concepts and Business Processes, ” Computers & Security,Vol. 19,pp.234-235,2000 [55] V.S. Miller., “ Use of elliptic curves in cryptography, ” Advances in Cryptology:Crypto ’ 85, Springer-Verlag,1986, pp. 417-426.
[56] W.B. Lee and C.C. Chang, “ Authenticated encryption scheme without using a one way function, ” Electronics Letters, Vol.31,No.19, 1995, pp. 1656-1657.
[57] W. Diffie, and M.E. Hellman, “ New directions in cryptography, ” IEEE Transactions on Information Theory, Vol. IT-22, No. 6, 1976, pp. 644-654.
[58] W.J. Tsaur, ” Several security schemes constructed using ECC-based self-certified public key cryptosystems, ” Applied Mathematics and Computation ,article in press, 2004 [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 System and Software, 2000, pp. 99-105.
[60] IBM, IBM Data Security Support Programs, USA.1984 [61] British Standards Institution, BSI, http://www.bsi-global.com/index.xalter
[62] British Standards Institution,BSI, http://asia.bsi-global.com/Taiwan/index.xalter.