A Study on Security Schemes for Community HealthCare Information System

賴惠美、曹偉駿

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

ABSTRACT

The problems, such as industry migration, aging of population, successively rising rate of suffering from the chronic disease ,etc., are getting seriously day by day in recent years. Therefore, every hospital actively plunges into community''s medical treatment, builds community''s healthy life and implements the idea of “ prevention is better than therapy ” . And the Community HealthCare Information System (CHIS), combines the information technology and personnel''s professional knowledge of medical treatment, offers medical member''s omni-directional medical care to the community. The system can promote the convenience of patient''s health management effectively, let the members of community look-after network condense the common consensus, and achieve purpose of sharing resources. The operations of CHIS are divided into three ways at present: The first way is in written form, recording the patient ’ s information of the doctor''s advice, then taking back the written information and inputing into the medical information system; The second way is transferring the patient''s basic materials to the notebook computer, then carrying to the community by the user, inquiring or modifying the information in the notebook computer if necessary, taking back the notebook to the hospital and upload the information to the host computer afterward; the third way is through VPN. The user first logins the host computer by inputting ID and password, and the user can then inquire about patient''s information. Among them, the shortcomings of the first way are: difficult to recognize the data (for instance: hasty and careless handwriting), unable to examine the content ’ s accuracy immediately and the written files easy to be lost or defiled, etc.; the shortcomings of the second way are: the data are easy to be lost or distorted, or revealed the patient''s personal secrets, etc. Although the third way offers the medical personnel''s convenient operation interface real-time, it is unable to satisfy patients when they want to inquire their health information at home. It also can not offer more extensive and more convenient information when the doctors engaged in the service-at-home in the community. For this reason, the thesis is to focus on the environment of World Wide Web, based on the information security management standard (BS7799-2), to analyze and arrange the security requirement that exists in the community ’ s health-care information system. In addition, we also propose user authentication, data encryption/decryption, digital signature, authenticated encryption, role-based access control schemes to secure the CHIS. Furthermore, we implement the proposed CHIS to achieve pratical application indeed.

Key Words : Community Healthcare、Electronic Medical Record、BS7799、Role-Based Access Control、Self-certified public key cryptosystems、 Elliptic curve cryptosystems.

Keywords : Community Healthcare ; HL7 ; BS7799

Table of Contents

REFERENCES

[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,周伯鋥,「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.