J Med Syst (2006) 30:309–315
DOI 10.1007/s10916-006-9019-y

ORIGINAL ARTICLE

Personal Health Record Systems and Their Security Protection

Khin Than Win · Willy Susilo · Yi Mu

Received: 17 December 2005 / Accepted: 7 February 2006 / Published online: 28 June 2006

Abstract The objective of this study is to analyze the security protection of personal health record systems. To achieve this we have investigated different personal health record systems, their security functions, and security issues. We have noted that current security mechanisms are not adequate and we have proposed some security mechanisms to tackle these problems.

Keywords Personal health record · Electronic health record · Privacy · Security · Information protection

Introduction

The focus of healthcare has been shifted from healthcare providers' paternalistic approach to the consumer-oriented approach. It is noted that consumers that are well informed about their illnesses tend to understand and follow instructions and ask more insightful questions [1]. Allowing patients to access their own records will encourage patients to be involved in their own healthcare and that will strengthen the patient–provider relationship and will enhance the effective healthcare management. Healthcare institutions around the world are encouraged to develop the electronic health record system and personal health record system can be seen as one of the means that can empower patients in their own healthcare. However, security of electronic health record has been a major concern in healthcare industry [2–4]. A health record system could be under various common attacks including [56]:

- *Masquerading*: the pretence of one entity to be another entity. By masquerading, an entity can get hold of privileges, which it is not authorized to have in the first place. Within a health record system, a user or process might masquerade as another to gain access to a file or memory to which it is not authorized, while over a network, a masquerading user or host may deceive the receiver about its real identity.
- *Unauthorized use of resources*: This includes unauthorized access to both resources on the networks as well as a computer system. For instance, within a computer system, this threat corresponds to users or processes accessing files, memory, or processor without authorization. Over a network, the threat may be in the form of accessing a network resource. This may be a simple network component such as a printer or a terminal, or a more complex one such as a database, or some applications within the database.
- *Unauthorized disclosure and flow of information*: This threat involves unauthorized disclosure and illegal flow of information stored, processed, or transferred in a networked system, both internal and external to the user organizations. Within a system, such an attack may occur in the form of unauthorized reading of stored information, while over the network, the means of attack might be wiretapping or traffic analysis.
- *Unauthorized alteration of resources and information*: Unauthorized alteration of information may occur both within a system (by writing into memory) and over the network (through active wiretapping). The latter attack may be used in combination with other attacks such as replay whereby a message or part of a message is repeated intentionally to produce an unauthorized effect. This threat may also involve unauthorized introduction (removal) of

K. T. Win · W. Susilo · Y. Mu
University of Wollongong,
New South Wales, Australia

K. T. Win (✉)
e-mail: win@uow.edu.au

resources into (from) a distribution system. Unauthorized use of resource may also lead to theft of computing and communications resources, or to the unauthorized destruction, modification, disclosure of information related to the business. That will impair the data integrity of health data. Destruction or modification of data can have serious impact on patients' health.

- *Repudiation of actions*: This is a threat against accountability in organizations. For instance, a repudiation attack can occur whereby the sender (or the receiver) of a message denies having sent (or received) the information. For instance, a healthcare consumer requesting an appointment with a healthcare provider for a certain service, but later denies having sent the message. A similar attack can occur at the receiving end; for instance, an organization denying the receipt of a particular request even though it actually did receive that. This kind of incident will be a significant problem in patient booking or scheduling of task.
- *Unauthorized denial of service*: Here, the attacker acts to deny resources or services to entities, which are authorized to use them. For instance, within a computer system an entity may lock a file thereby denying access to other authorized entities. In the case of the network, the attack may involve blocking the access to the network by continuous deletion or generation of messages so that the target is either depleted or saturated with meaningless messages. This will disrupt the workflow of the healthcare process as an authorized person would not be able to access the required data.

In this paper, we will investigate some existing personal health record systems, their security functions, and security issues. As the countermeasure to those issues, we will propose some security mechanisms to tackle those problems. It is envisaged that our proposal will make health record systems more secure.

The rest of this paper is arranged as follows. In the section on Review of Personal Health Record Systems, we will describe personal health record systems. Access and security of personal health record systems and enhancing security mechanism will be described in the sections titled Access and Security of Personal Health Record Systems and Enhancing Security in Health Record Systems, respectively.

Review of personal health record systems

Personal health record systems

The PHR (Personal Health Record) could be seen as the solution for better management of an individual's health, and as the tool that will empower the patient in correlation with healthcare providers through the ability to provide his/her own medical history [7–9]. The Australian Medical Council stated that, patient access to their own record is important as clinicians should respect patient's autonomy and disclose to their patients relevant information regarding their diagnosis, prognosis, or the implications of diagnostic tests [10]. In the United States, the Health Insurance Privacy and Portability Act 1996 also stated that "patients must be able to see and get copies of their records and request amendments" [11].

Waegemann 2002 has categorized different types of personal health record systems, which include, Offline personal health records; web-based Commercial/Organizational personal health records; functional or purpose-based personal health record; provider-based personal health records and partial personal health records [9]. Commercial PHRs offer fee for service such as annual fees and allow consumers/patients to store their health information which can be accessed by users anywhere in the world. Organizational PHRs are hosted by the healthcare organization or insurance company such as Kaiser Permente. Purpose-based personal health records are widely available currently which cater to a group of individuals with specific illness or diseases, for example, health record systems for people with AIDs, chronic diseases such as diabetes and cardiovascular diseases.

It can be seen that except for offline PHRs, personal health record systems are available in different forms such as PHR in web kiosk, smart cards, and web-based PHRs.

Web-based personal health record systems

The web-based PHRs have great potential to influence healthcare in the 21st century by creating a single source of health information that is accessible from anywhere in the world and people's health information could be under the shared control of the individual and their healthcare provider [12, 13]. There are different opnions regarding how PHRs should be implemented. There is a strong opinion in one part of the healthcare professional community that web-based PHRs should be entirely separated from institutional EHRs because there is great doubt that individuals can accurately describe/report on their own medical condition. Others argue that there is no reason why Internet-based PHRs cannot have exactly the same record architecture as the records maintained by institutional EHR systems. However, there is a security concern over these PHRs, if they will be integrated with institutional EHRs as this will allow more users to access these systems and the system will be more vulnerable to unscrupulous users. Furthermore, they argue that implementation of standardized architecture will enable fully operational interoperability of health data among healthcare providers and the Internet-based PHRs where appropriate and approved by an individual [14]. It can be seen that there are commercial-based and organizational-based web-based PHRs available for healthcare consumers. It is noted that to ensure patient safety, web-based personal health record [15].

should support functionalities such as health information and data, results management, order entry/management, decision support, electronic communication and connectivity, patient support, administrative processes, reporting [8], privacy, unique patient identification, and interoperability [15]. Again, there is a divided opinion regarding how much information should be included and what functionalities these PHRs should have. However, the security of PHR should not be overlooked. With Institutional electronic health record systems these can be in local area network or within intranet but web-based personal health record systems will be on the Internet, able to be accessed anywhere in the world.

Health kiosks

Health kiosks offer an alternative platform for patients to manage their own health. Patients will be able to make updates to their medical records through an ATM-style interface. These updates may also include address information, insurance updates, appointment scheduling, and payments [16]. The Health Kiosks also have a portal for patients to insert an USB disk for information retrieval, and card scan for user authentication and payment entry. The USB disk, allows patients to retrieve any information for further access in other locations (i.e., computers or other Health Kiosks) [16] Touch-screen kiosks have long been in existence to deliver health information to the general public. Health kiosks have proved to be a one-stop center for those who do not have access to the Internet or even a computer [17]. The main objectives for installing health kiosks in healthcare institutions were to automate appointment-booking, registration, and payment processes. However, with the push for patient empowerment, systems have been designed to allow patients to access and update their own medical records. Patients can now review their health information prior to their consultations while sitting in the waiting room. This will enable them to have a clearer picture of their health conditions during the consultation itself [18].

Smart cards

Smart cards are commonly used as storage for patient records or also for identification purposes in the healthcare industry. In fact, smart cards are more commonly used on a larger scale as compared to web-based PHRs. Shelfer and Procaccion [19]. cited that over 80 million smart cards are currently in use in the German healthcare system. Other countries which have also introduced smart cards in their health systems on a national level are notably Canada [20]. and Taiwan [21]. One main reason why smart cards are commonly used in the healthcare industry is the ability to store both text and image-based medical records. Chan *et al*. [22]. also recognize that the smart card technology is the solution to universal access to medical information. Nevertheless, Tobacman *et al*. [25]. noted that usage of smart cards as PHRs do not promote patients, healthcare providers' relationship as there is limited information available on the smart card. However, with the introduction of optical memory embedded into smart cards, a much higher storage capacity of digital data can be stored in the smart card and that could alleviate the limitation.

Access and security of personal health record systems

Patients access to their own health information

Currently PHRs have been implemented or are being implemented in healthcare institutions throughout the world [4,14,23,24]. There are potential benefits from patients' access to their own health information. Studies indicated that patients' access to their health record can promote communication between patients and their healthcare providers, for example, patient being able to participate more in discussing treatment options [14]. A cross-sectional study conducted in 2001 involving 4500 adults who had a recent clinic visit documented that patients would like to see their health information because they would like to be more involved in their own healthcare, understand the condition better, see if they are getting better or worse, and jog their memory about medical history [26]. Therefore, appropriate information available to patients will benefit patients as they will be better informed of their health conditions. There are also concerns regarding the information available to patients. A study conducted by Cimino *et al*. 2002 noted patients involved in their studies understood the information in their records [14]. and recommended that vital information should be included in PHRs [14,25]. Confidentiality of personal information should not be overlooked when granting patients' access to the PHRs. Consumers were worried that their health information stored in the commercial web sites will be used for other purposes. Healthcare providers have the ethical responsibilities to maintain the patient's confidentiality. However, information stored on the server can be accessed by different individuals and it is a concern of information security. Information protection of PHR will be discussed in detail in the following section.

Information protection of personal health record systems

Health record systems include patients' sensitive health information and web-based PHR allows patients to access their records from anywhere in the world. Vulnerability of health data in history was reported such as the incident of a hacker infiltrating the University of Washington Medical Center's Computer System and stealing at least 5000 cardiology and

rehabilitation medicine patients' records [3,27,28]. and the incident of a Hacker pointing out the vulnerabilities of the system because he had penetrated an unidentified medical center in New York and another in Holland [3,28].

Previous work on evaluation of information protection of personal health record system included user authentication through password mechanisms, audit controls, privacy and confidentiality statements, documented secure transmission, and secure messaging system [4]. Web-based PHRs use a secure HTTPS protocol and encrypts content, which provide security of information on the openly-accessed Internet, and is therefore subject to eavesdropping or interferences. Like most secured websites, a 128-bit strong encryption is used to make interpretation and interference of information extremely difficult. Implementing a firewall and antivirus protection through security policies will further provide a secure Internet connection [29]. In smart card systems, a Personal Identification Number (PIN) is assigned to each card for first-level access. Since only the card owner will know the PIN, nobody else will be able to access the owner's health records without his/her permission. Other user authentication methods include biometric scans (fingerprint, face, hand, and retina) [30]. The next level of security is the implementation of cryptographic mechanisms within the smart card or through specialized security modules. Public key cryptography, in which each card has its own private key, is a common method deployed. Both sender and receiver need to share a common secret key in order to encipher/decipher the data. The microprocessor chip also offers significant resistance to any physical tampering [2].

As confidential information is stored and transmitted across networks, it is important that all web-based PHRs provide protective measures. Security of web-based PHRS have been reviewed [15]. and it was indicated that those sites have privacy statements which ensure users that their information is in good hands by explaining how information is being handled while always maintaining the anonymity of an individual's identity. All websites also use a Secure Socket Layer (SSL) connection to encrypt information that is being exchanged across networks.

It can be seen that the most common authentication mechanism seen in current electronic health record systems including personal health record systems are an "identifier" together with a "Password." [31]. However, programs with common password protection use subroutines that check against a hashcode of the password. Debuggers and disassemblers can reverse engineer the binary program code to the human readable form and execute program instructions. This can search the subroutine that decides acceptance or rejection of the password [32]. In addition, there are security concerns over passwords mechanism for protection of personal health information as commented in a GP interview "Although each individual GP has his own password, it is collected by one of the practice staff and then written on a piece of paper that hangs up in the back of the office area" [33].

To prevent external access, most healthcare organizations have implemented firewall. Information protection of personal health record should be beyond these measures as these PHRs will be available on the Internet. Audit trails have been used as an important tool for data security in web-based personal health record systems [15]. Nevertheless, it was noted that audit trails often can exceed the size of the original file by orders of magnitude [34]. and it is not practical.

In Web Kiosk, in GE healthcare system, and in patients using the Patient Access Electronic Record System the patients are not able to make changes themselves but can send requests or comments to practitioners to point out errors in their health records. When logging into the kiosk systems, patient authentication is required either in the form of user ID/password log-in ("System") or fingerprint scanning [23].

With the advancement of wireless and handheld devices and connectivity to Internet through mobile phones accessibility of information has increased and it is important to ensure the security of these devices. A scenario presented by Sax *et al*. (2005) clearly demonstrated usage of these devices by healthcare consumers to access personal health information [33]. Their model used the mobile authentication service through using the directory service. Then the mobile device needs to answer the challenge. After that, a mobile authentication service sends an SMS (Short Message Service) to the user's phone and the user will key in the personal identification number. The authentication process relies on the RSA algorithm [35]. It can be seen that security is a main concern for securing personal health information and different healthcare organizations have provided different security mechanisms. Gritzalis and Lambrinoudakis have proposed a security architecture for interconnecting health information systems through security agents. The system ensures confidentiality through data exchange, content integrity and access control, single sign-on authentication services, role-based access control, and auditing [3]. It can be seen that security mechanisms for health record systems have been emphasizing on the user authentication. However, these security mechanisms are not sufficient for protecting personal health information. The following section will demonstrate why these are not sufficient and propose to enhance security in health record systems.

Enhancing security in health record systems

Stronger authentication

PIN or password-based authentication system provide *very weak* security protection to the system. A PIN can be broken

easily since normally a PIN consists of a series of string/digit, which is easy to remember. Hence, this is due to a brute force attack. Consider a PIN that contains of 4 digits, then it only requires 10^4 combinations for the attacker to break into it. A weak password is as bad as a PIN and can be cracked easily. Therefore, it is an obvious need for introducing stronger authentication than PIN or password-based system. A better solution to user authentication is a credential system, where only the user who holds a *legitimate credential* issued by the associated authority can have access to the record. A credential system is a system where users obtain credentials from organizations and demonstrate possession of these credentials, either implicitly or explicitly. A user who obtained a credential can perform some cryptographic operations, such as signing or decryption. Since the credential is digitally signed by the authority, it is unforgeable under some complexity assumption. Compared with the PIN and password-based systems, the credential-based is much secure since it cannot be found by guessing for example. Therefore, this will prevent others to access personal health information in consumers' personal health record.

Confidentiality

Confidentiality can be somehow achieved by authentication mechanisms. A system protected by an authentication scheme such as the credential scheme introduced above can ensure confidentiality by allowing only legitimate users to access. However, once a user logs in the system, he or she can then do anything. In particular, when the personal health information is transmitted in a computer network, it can be approached by anyone who does not have the legitimate access rights. Therefore, a proper encryption scheme must be introduced in order to achieve confidentiality in a health record system.

Although an encryption scheme is the key in providing confidentiality to a health record system, it is still not perfect. Consider the situation that a legitimate user accidentally (or even intentionally) distributes a confidential record to other illegal parties, the encryption scheme will fail. The example will be the incident of Kaiser Permanente accidentally sending the private correspondence of over 850 of its members to approximately 19 people in August 2000 [36]. We introduce a scheme where the health records can be accessed in some designed device such as a handheld device or a laptop computer. The device is assigned a cryptographic key, which can be used to decrypt some specific records; therefore, only the owner of the device can access the record. Clearly, the user (owner of the device) cannot illegally distribute the records he or she has, to any other illegal users since they are in an encrypted form.

Availability

A networked health record server could suffered from denial of service (DoS) attacks. The attacker in such attacks does not aim on the information provided in the system, rather it aims on denying legitimate rights of others. How does it work? There are various DoS methods, but most of the existing attacks tried to consume the given resources (memory, CPU, etc.) on the server by sending a number of data packets to the server. A consequence of such attacks is crash of the system.

One of the solutions to this problem is the *client puzzle* mechanism, which is described as follows. The server prepares a lot of small digital puzzles for potential users. If everything is normal or users are logging in the system in order, the server will handle the system normally. However, when the server detects a potential DoS attack (too many access requests have been received), the server will send a digital puzzle to each of the users. Since all users are now required to solve their puzzles, the server can gain precious time to allocate its resource properly. If the user cannot answer the provided puzzle correctly, then the resources will not be allocated to the user. This is to protect against DoS attacks.

We have developed two unique and efficient client puzzle techniques [37,38]. which are applicable for this purpose. In our testbed implemented, we have included this work and we show that DoS attacks can be prevented.

Challenges

We have described various mechanisms for securing health records, and PHR in particular. However, we must point out that the current and existing technologies may not be adequate to provide a satisfactory level of protection. For instance, one can think that encrypting the personal health information in the database may solve all the problems, but indeed, this is not true. Consider the situation where the record owner is retrieving his personal health information from the database, then normally the record will be transmitted over the air in a plaintext form, which is subject to a *sniffing* attack. Additionally, a straightforward solution may be incorporated by using the encrypted version of Wireless LAN as a media for transmitting the data from the database to the owner's handheld device, as the current existing Wireless LAN technology itself is also known to be insecure (e.g. Wired Equivalent Privacy (WEP) protocol has been broken, meanwhile the latest TKIP in WPA (Wired Protection Access) is known to be insecure due to the use of *Michael* hash function [37,38].

To address the WEP vulnerabilities, the IEEE 802.11 Task Group i (TGi) provides a short-term solution and a long-term solution. The short-term solution has adopted the Temporal

Key Integrity Protocol (TKIP). TKIP is a group of algorithms that wraps the WEP protocol to address the known weaknesses. TKIP includes three components: a message integrity code called *Michael*, a packet sequencing discipline, and a per-packet key mixing function. TKIP is considered as a temporary solution, and it is designed for legacy hardware. For the long-term solution, the IEEE 802.11 TGi recommends two modes of operations: WRAP (Wireless Robust Authenticated Protocol) and CCMP (Counter-Mode-CBC-MAC Protocol). Michael is the message integrity code (MIC) of TKIP in the IEEE 802.11i draft. Michael is a keyed hash function, whose inputs are a 64-bit Michael key and an arbitrarily long message, and output is a 64-bit Michael value.

We have shown in Ref [39]. that having Michael hash function included in the WPA will result in an inadequate protection for the Wireless LAN. Very recently, we extended this work to show that TKIP is also insecure [37]. The long-term solution using AES (Advanced Encryption Standard) is still not yet available, and before this long-term solution is available, wireless LAN is considered as an insecure environment [40].

Our future work will be in the area of finding an alternative means for securing health records where they cannot be achieved with the current and existing technologies. It is the challenge that will advance the security of health records to be used in practice.

Conclusion

Information security of personal health information has been a growing concern in healthcare industry. Personal health record systems and electronic health record systems which allow patients to access their health information can be seen in today's healthcare arena. Legislations and policies have been in place in different countries to protect information privacy. Security measures also need to be adequate to ensure the information protection. As discussed in this paper, it is noted that there still are gaps in current security protection mechanisms and these need to be addressed to enhance protection of personal health information.

References

1. Eysenbach, G., Consumer health informatics: Recent advances *Br. Med. J.* 320:1713–1716, 2000.
2. Gritzalis, D., and Lambrinoudakis, C., A security architecture for interconnecting health information systems. *Int. J. Med. Inf.* 73:305–309, 2004.
3. Lemos, R. 2000, Medical Privacy Gets CPR, December. Available at http://www.zdnet.com/zdnn/stories/news/0,4586, 2667243,00.html accessed May 17, 2001.
4. Win, K. T., A review of security of electronic health records. *Health Inf. Manage. J.* 34(1):13–18, 2005.
5. Stallings, W., *Cryptography and Network Security: Principle and Practices*, 4th edn., Prentice-Hall, Englewood Cliffs, NJ, 2006.
6. Varadharajan, V., and Mu, Y., Design of secure end-to-end protocols for mobile systems. In Encarnacao, J. L., and Rabaey, K. M. (eds.), *Mobile Communications*, Chapman and Hall, London, pp. 258–266, 1996.
7. Waegemann, C. P., Status Report 2002: Electronic Health Records, Medical Records Institute, available at www.medrecinst.com/, 2002.
8. Committee on Data Standards for Patient Safety, *Key Capabilities of an Electronic Health Record System*, Institute of Medicine, The National Academies, Washington, DC, 2003.
9. NSW Ministerial Advisory Committee on Privacy and Health Information, ANACEA OR PLACEBO? Linked Electronic Health Records and Improvements in Health Outcomes, December, 2000.
10. Australian Medical Council 2003, Legal, ethical and organisational aspects of the practice of medicine. In Marshall, V. C. et al. (ed.), Anthology of Medical Conditions, Australian Medical Council, Inc., Barton, ACT, Australia.
11. Ross, S., and Chen, T. L., The effects of promoting patient access to medical records. *J. Am. Med. Inf. Assoc.* 10:129–138, 2003.
12. Sittig, D. F., Middleton, B., and Hazlehurst, L. B., Personalized Health Care Record Information on the Web, Proceedings of the Quality Healthcare Information on the "Net'99 Conference, October 13, 1999 in New York. Available at: http://www.informatics-review.com/thoughts/personal.htm, 1999.
13. Treseder, P., Keeping Your Health on Record, ISO/TC 215, Health Informatics. Available at; http://www.iso.ch/iso/en/commcentre /pdf/Health0011.pdf, (Accessed: February 2, 2004), 2000.
14. Cimino, J. J., Patel, V. L., and Kushniruk, A. W., The patient clinical information system (PatCIS): Technical solutions for and experience with giving patients access to their electronic medical records. *Int. J. Med. Inf.* 68:113–127, 2002.
15. Win, K. T., Web-based personal health record systems evaluation, *Int. J. Healthc. Technol. Manage.* 7(3/4):208–217, 2006.
16. Galvanon, News and Events: GE Healthcare's Health Kiosks Enable Easy "ATM style" Access to Electronic Medical Records [Online]. Available URL: http://www.galvanon.com/healthcare/whitepapers/ge_kiosks.htm, [Accessed 25 May 2005], 2005.
17. Nicholas, D., Huntington, P., and Williams, P., An evaluation of the use of NHS touch-screen health kiosks: A national study, *Aslib Proc.* 54(6):372–384, 2002.
18. Briggs, B., Patients Step Up to Kiosks—Warily. *Health Data Manage.* 13(6):88–90, 2005.
19. Schattner, P., and Plteshner, C., The GPCG Computer Security Project: Final Report. Monash University, The Department of General Practice in Affiliation with the Dept of Rural Health, The University of Melbourne, Monash Division of General Practice, 2004.
20. Benoit, A., and Hamel, G., Adoption of Smart Cards in the Medical Sector: The Canadian Experience. *Soc. Sci. Med.* 53(7):879–894, 2001.
21. Smart Card Alliance, *The Taiwan Health Care Smart Card Project* [Online]. Available URL: http://www.smartcardalliance.org/pdf/about_alliance/user_profiles/Taiwan_Health_Card_Profile.pdf [Accessed 24 March 2005], 2005a.
22. Chan, A., Cao, J., Chan, H., and Young, G., A web-enabled framework for smart card application in health services. *Commun. ACM* 44(9):77–82, 2001.
23. PAERS, *Patient Access to Electronic Medical Record and Automatic Arrival System* [Online]. Available URL: http://www.bromba.com/download/PAERSsystem_detailed.pdf, [Accessed 5 October 2005], 2004.

24. Kim, M., and Johnson, K., Personal health records: Evaluation of functionality and utility. *J. Am. Med. Inf. Assoc.* 9(2):171–180, 2002.
25. Tobacman, J. K., Kissinger, P., Wells, M., Prokuski, J., Hoyer, M., McPherson, P., Wheeler, J., Kron-Chalupa, J., Parsons, C., Weller, P., and Zimmerman, B., Implementation of personal health records by case managers in a VAMC general medicine clinic. *Patient Educ. Couns.* 54:27–33.
26. Fowles, J. B., Kind, A. C., Craft, C., Kind, E. A., Mandel, J. L., and Adlis, S., Patient' interest in reading their medical record: Relation with clinical and sociodemographic characteristics and patients' approach to health care. *Arch. Intern. Med.* 164:793–780, 2004.
27. Songini, M. C., and Dash, J., Hospital confirms hacker stole 5,000 patient files: Attack points to need for standards for patient records. *Comput. World* 34(51):7, 2000.
28. Chin, T., Security breach: Hacker gets medical records. *Am. Med. News* 44:18–19, 2001.
29. Chadwick, D. 2003, Patient privacy in electronic prescription transfer, IEEE Secur. Priv. 1(2):77–80.
30. American Society for Testing and Materials, E1714-00: Standard Guide for Properties of a Universal Healthcare Identifier, Available at: http://www.astm.org/cgibin/SoftCart.exe/index.shtml?E + mystore>, (n.d.).
31. Allaert, F. A., Le Teuff, G., Quantin, C., and Barber, B., The legal knowledge of the electronic signature: A key for a secure direct access of patients to their computerised medical record, *Int. J. Med. Inf.* 73:239–242, 2004.
32. Horst, H., How to Tamper with Electronic Health Records. Available at: <http://www.gnumed.net/gnotary/tampering.html> (accessed May 2004), 2001.
33. Schattner, P., and Plteshner, C., The GPCG Computer Security Project: Final Report, Monash University, The Department of General Practice in Affiliation with the Department of Rural Health, The University of Melbourne, Monash Division of General Practice, 2004.
34. Bilykh, I., Bychkov, Y., Jahnke, J. H., McCallum, G., Obry, C., Onabajo, A., and Kuziemsky, C., Can GRID Services Provide Answers to the Challenges of National Health Information Sharing? Proceedings of the 2003 Conference of the Centre for Advanced Studies Conference, IBM, Canada, pp. 39–53, 2003.
35. Sax, U., Kohane, I., and Mandl, K. D., Wireless technology infrastructures for authentication of patients: PKI that rings. *J. Am. Med. Inf. Assoc.* 12(3):263–268, 2005.
36. Fried, B. M., and Pittman, S., Protecting medical privacy in a digital age: Beyond policies and procedures. A critical role for technology. California, Surf Control Inc. Available at:<http://itpapers.news.com>, 2001.
37. Gao, Y., Mu, Y., and Susilo, W., A New Client Puzzle Scheme Against DoS/DDoS Attacks. International Journal of Computer Science and Network Security (IJCSNS), Vol. 5 No. 10, pp.189–200, 2005.
38. Gao, Y., Mu, Y., and Susilo, W., Preventing DoS Attacks with A New Client Puzzle Scheme. The AUUG'2005 Annual Conference, pp. 3–16, 2005.
39. Huang, J., Susilo, W., and Seberry, J., Observations on the Message Integrity Code in IEEE 802.11 Wireless LANs. The 3rd Workshop on the Internet, Telecommunications and Signal Processing (WITSP 2004), pp. 328–332, 2004.
40. Huang, J., Seberry, J., Susilo, W., and Bunder, M., Security Analysis of Michael: The IEEE 802.11i Message Integrity Code. Second International Symposium on Ubiquitous Intelligence and Smart Worlds (UISW2005), *Lecture Notes in Computer Science 3823*, pp. 423–432, Springer-Verlag, Berlin, 2005.