HOW TO PRESERVE PATIENT'S PRIVACY AND ANONYMITY IN WEB-BASED ELECTRONIC HEALTH RECORDS

Daniel Slamanig and Christian Stingl
School of Medical Information Technology, Carinthia University of Applied Sciences, Primoschgasse 10, Klagenfurt, Austria

Keywords: Anonymity, Cryptography, Electronic Health Record, Health Data, Information Security, Privacy.

Abstract: In recent years, demographic change and increasing treatment costs demand the adoption of more cost efficient, highly qualitative and integrated health care processes. The rapid growth and availability of the Internet facilitate the development of eHealth services and especially of electronic health records (EHRs) which are promising solutions to meet the aforementioned requirements. Considering actual web-based EHR systems, patient-centric and patient moderated approaches are widely deployed. Besides these initiatives there is an emerging market of so called personal health record platforms, e.g. Google Health. Both concepts provide a central and web-based access to highly sensitive data of EHRs. Additionally, the fact that these EHR systems may be hosted by not fully trustworthy providers necessitates to thoroughly consider privacy issues. In this paper we define security and privacy objectives that play an important role in context of web-based EHRs. Furthermore, we discuss deployed solutions as well as concepts proposed in the literature with respect to this objectives and point out several weaknesses. Finally, we introduce a system which overcomes the drawbacks of existing solutions by considering an holistic approach to preserve patient's privacy and discuss the applied methods in detail.

1 INTRODUCTION

In recent years many countries have installed eHealth initiatives and working groups in order to develop strategies to harmonize the exchange of health related information using the Internet. A central aspect of eHealth is called the electronic health record (EHR) which integrates all relevant medical information of a person and represents a lifelong documentation of the medical history. Considering implementations of EHRs, one of the most critical factors of success is the protection of the patient's privacy, which is clearly reflected in surveys concerning such systems (HI, 2004). Additional issues are, that the EHR is patient-centered and that the patient herself moderates her EHR (Pyper et al., 2004). This means, that solely the patient is able to grant access to her medical data to other parties and to nominate delegates respectively. Moreover, the study in (Pyper et al., 2004) shows, that patient access to their electronic records needs to be developed in partnership with the patients. In this paper we are considering web-based EHR systems which enable persons to manage their EHRs by means of a web-application.

Besides the classical aspects such as standardization, interoperability, time and location independent access, legal frameworks, etc. basic requirements for web-based EHRs are the possibility for a patient to freely define the structure (e.g. folders) of the EHR and to share medical data or even the entire EHR with other parties (e.g. physicians, relatives). Furthermore, we will introduce and discuss further aspects and concepts which are especially applicable for patient-moderated and web-based EHRs. This consideration for EHR architectures helps to improve the trustworthiness of an EHR system by means of privacy preserving techniques.

The organization of the rest of the paper is as follows: In the subsequent section 2 we motivate why privacy issues are important in this context and define potential attacker models. We propose and discuss basic management, security and privacy relevant objectives, which need to be considered when designing privacy enhanced EHRs in section 3. Based on these objectives in section 4 we investigate systems which are explicitly designed to provide EHRs as well as systems which are not originally developed to manage EHRs but may also be used to store health related

Slamanig D. and Stingl C. (2009).
HOW TO PRESERVE PATIENT'S PRIVACY AND ANONYMITY IN WEB-BASED ELECTRONIC HEALTH RECORDS.
In *Proceedings of the International Conference on Health Informatics*, pages 257-264
DOI: 10.5220/0001547502570264

data. In the subsequent section 5 we introduce a novel system for EHRs called PE^{2}HR (Privacy Enhanced EHR) that realizes the security and privacy objectives defined in section 3. In the remaining section 6 we will provide a conclusion and discuss some future aspects.

2 MOTIVATION

Web-based EHR solutions are growing in popularity and provide mechanisms that enable people to comfortably manage their medical data online and furthermore help to improve the quality of care, by means of availability of all relevant medical data. However, in context of the Internet we are confronted with a set of attacker models and threats that need to be considered when designing systems which deal with sensitive data. For example, the lack of anonymity in Internet communication and the trustworthiness of providers hosting such EHR systems may constitute serious problems. Additionally, there exists a phenomenon often denoted as privacy myopia. This means, that people often are not aware of dangers related to the "ordinary" use of the Internet, e.g. that they reveal IP-addresses or Ethernet MAC-addresses which may enable third parties to link several actions and may even enable them to identify the physical users behind their computers. Furthermore, users often give away their data very easily, without reflecting on potentially negative consequences.

2.1 Attacker Models

In order to identify realistic threats, we need to consider potential attackers firstly, which are listed subsequently.

- Client intruder: This kind of attackers breaks into the client computer, e.g. they compromise a host by means of malware, e.g. trojan horses, and thus obtain access to sensitive data which should solely be available to its owner. This threat is highly realistic and indeed one of the major problems in context of the Internet and should be reduced by means of trusted computing (TCG, 2008) in the future.
- Eavesdropper: An eavesdropper compromises or owns a subset of nodes of the communication infrastructure and thus is able to inspect messages which are routed over them. This attacker is usually able to link communicating parties by means of addresses used by the communication media (e.g. IP-addresses) and to fully access content data of messages in absence of transmission encryption (e.g. SSL/TLS).
- Curious insider or server intruder: This attacker is in possession of administrative privileges and thus has full access to log information as well as content data of the EHR system. Clearly, in analogy to the client intruder an external adversary may also compromise a host which provides server applications.

In this work we are especially interested in the latter two types of attackers, since in absence of trusted computing and remote attestation in particular, it is very hard to decide whether client hosts are secure or not.
In context of eavesdropping, even if transmission encryption is used, the attacker may be able to obtain information about users which are communicating with an EHR system. Thus, an attacker is able to derive communication patterns. In order to hide these patterns from external parties, e.g. how often a user logs into the system, we need to investigate communication anonymity (cf. section 5). Additionally, there exist potential attackers which are located at the provider of the EHR system. As a recent study (CSI, 2007) shows, more than 50% of attacks against information system are conducted by insiders, and hence this threat is highly realistic. Consequently, the trustworthiness of service providers is in question and we need to design and investigate concepts, which protect content as well as metadata (e.g. relationships between users and data objects) from insiders in order to improve their privacy.

3 SECURITY AND PRIVACY OBJECTIVES FOR EHR'S

In this section we propose and discuss security and privacy objectives which need to be considered when designing privacy enhanced EHRs. Before discussing the main objectives in detail, we want to point out that there are some basic functionalities which need to be provided by any serious EHR system. These functionalities comprise amongst others the availability of the system, the confidentiality of data transmitted between users and the system (e.g. SSL/TLS) and the integrity of stored data.
A major criterion for the choice of these objectives was the influence of a user on the degree of privacy. More precisely, considering a single objective, the privacy protection depends mainly on the provider or on the user, subject to the applied method. For example, confidentiality can be realized on the one hand

by means of client-side encryption (by the user, e.g. XML-Encryption) and on the other hand by means of server-side encryption (by the provider, e.g. database encryption).
Subsequently we will provide a brief discussion regarding our objectives.

3.1 Anonymity

Anonymity is often referred to as the property of being not identifiable with respect to a set of actions inside a group of people, the so called anonymity set (Pfitzmann and Köhntopp, 2000). Intuitively the degree of anonymity is the higher, the larger the anonymity set is and the more uniformly the actions are distributed within this set. Considering an EHR system we can define anonymity at three different levels.

- Anonymous communication: Anonymous communication is guaranteed, if an observer is not able to determine a communication relationship between two communicating parties by means of information revealed by the communication channel.
- Sender- and receiver-anonymity: A communication relationship between a sender and receiver provides sender-anonymity, if the receiver is not able to identify the sender by means of received messages. The receiver-anonymity can be defined analogously.
- Data anonymity: A system provides data anonymity, if data stored in the system of the receiver and related to a specific sender can not be linked to the sender by the receiver and any other person. This means, that even an insider of a system is not able to establish a relationship between a patient and her related data. Consequently, serious measures to provide data anonymity must be realized by the sender.

3.2 Authentication

If access to a system is restricted to an authorized set of users, the systems needs to establish the identity of a potentially authorized user. This is in general realized by means of authentication mechanisms. In authentication or identification protocols the holder of an identity usually claims a set of attributes including an identifier and interactively proves the possession of the claimed identity to a verifier based on these attributes. This identifier is usually unique within a specific context (e.g. application) and thus enables the system to link an authentication and subsequent transactions to a specific user.
The above mentioned authentication mechanisms obviously establishes a one-to-one mapping between an authenticating user and her identity. In contrast, anonymous authentication (cf. section 5.2) provides mechanisms such that the before mentioned one-to-one mapping does not longer exist. In particular, an authenticating user proves solely her membership in a group of authorized users, whereas the verifier is not able to decide which member of this group actually conducted the authentication.

3.3 Authorization

Authorization is the concept of providing access to resources only to users who are permitted to do so. Usually the process of authorization takes place after a successful authentication. Mainly, authorization concepts in systems are realized by means of discretionary access control (DAC) strategies, e.g. access control lists (ACLs) or mandatory access control (MAC) strategies, e.g. role based access control (RBAC) (Win, 2005). In the former case, the access policies for objects are specified by the their owners whereas in the latter case access policies are specified by the system. The before mentioned strategies represent only a selection methods which exist in the literature and in practice today (Bishop, 2002), however they share one important commonality. These strategies are implemented by means of application layer mechanism which can be easily bypassed by insiders of the respective system.

3.4 Confidentiality

In context of EHRs, which provide web-based access to health related data, methods to guarantee confidentiality are essential. In general, confidentiality is realized by means of encryption and relies on the protection of the respective cryptographic keys. For the key management we distinguish two widely used techniques. On the one hand cryptographic keys are solely accessible to the user and all cryptographic operations are performed by the user's client (client-side encryption). On the other hand the system at the provider is responsible for the key management and all cryptographic operations (server-side encryption). From the security point of view, client-side encryption provides a higher level of confidentiality, since content data is not available in plaintext at any time at the provider. Thus, the number of feasible attacks can be reduced significantly. It must be mentioned, that in this paper we are not considering proprietary encryption-software that may be applied by the user

in addition to mechanism provided by the EHR system.

3.5 Deniability

One major advantage of a web-based EHR is the time and location independent availability of health related data. However, under certain circumstances this can be disadvantageous and even result in dramatic consequences for the user. In order to demonstrate this problem, we will provide an example which is in our opinion highly realistic. Assume that a person was suffering from a cardiovascular diseases, diseases of the musculoskeletal system, drug addiction or a mental diseases like (burn out) depression. This disease is in detail documented in the EHR of the person, however does not affect the current state of health of that person significantly. It is obvious, that this potentially compromising information is solely available for persons who are directly involved in the medical treatment process of the person and are authorized to access these data. In our opinion this is a basic requirement of an EHR. Consequently, there is absolutely no way for unauthorized persons to gain access to these data by means of the EHR system. However, since the EHR is accessible via the Internet, the user herself may be "motivated" or even enforced to present this compromising data during a job interview or an insurance contract conclusion. This is what we call the disclosure attack. It must be emphasized, that a person which has presented her EHR under such circumstances is not able to prove this involuntary disclosure to another party later on. Thus, there exists the need for mechanisms to plausibly deny the existence of highly compromising information (e.g. a cured burn out depression) from people who dot not need to know that information at all.

3.6 Unlinkability

Unlinkability of items of interest means that relations between items, which a priori exist, can not be identified through pure observation of the system (Pfitzmann and Köhntopp, 2000; Steinbrecher and Köpsell, 2003). A system containing n users provides perfect unlinkability, if the relation of an object and a user u_i exists with probability $p = 1/n$ for all objects. Hence, an insider of the system can not gain any information on links between users and objects by means of solely observing the system. In context of EHR systems we additionally need to consider static as well as dynamic aspects of unlinkability. The static aspect covers data objects which are stored in the EHR system and unlinkability is provided, if an insider at the system is not able to establish links between data objects and users significantly better than guessing. The dynamic aspect covers user's interaction with the system. In particular, we raise the question whether an eavesdropper or an insider at the system is able to link instances of authentication protocols and transactions with the system together and to a specific user. Clearly, a system which does not provide dynamic unlinkability also negatively influences static unlinkability aspects. For example, if a transactions represents an access to a specific data object and this transaction can be linked to a specific user then the data object linked to the user, although the system may provide static unlinkability.

3.7 Data Structure

The data structure defines primarily the logical structure of the EHR, e.g. a hierarchy of users, folders, subfolders and documents. In contrast to the objectives discussed above, the data structure does not contribute to the overall security of the system. However, the data structure is the main component regarding the usability and efficiency of the EHR system. Moreover, the degree of structuredness massively influences the concepts used for authorization. Especially, when considering sharing of health data between several parties the absence of any structure complicates standardized mechanisms for this task.
We want to point out that the data structure always contains information on the entire system (metadata), which may potentially reduce the degree of privacy, e.g. unlinkability, authorization, provided by the system. For example, if a system holds pseudonymized or even anonymized medical documents then authentication information and information provided by the data structure can be used to identify the holder of the respective documents.

4 INVESTIGATION OF EHR SYSTEMS

Prior to presenting our proposed solution in detail, we investigate systems which are either explicitly designed to provide web-based EHR functionality, i.e. Personal health record platforms, PIPE, and systems which may be used by people to "build" their own web-based EHR, i.e. virtual hard disks. This investigation is based on the security objectives introduced in section 3 and summarized in Table 1. In the remainder of this section we provide a discussion of the above mentioned systems with respect to the security objectives.

Table 1: This table provides an analysis of the virtual hard disk concept (VHD), Google Health (GH), the PIPE system and our system introduced in section 5 regarding the objectives defined in section 3. Thereby C denotes client-side, S server-side, SC a combination thereof, ¬ denotes that this feature is not provided and ? denotes that it is not clear whether this feature can be provided. In context of authentication T denotes traditional and A anonymous authentication.

Objective	VHD	GH	PIPE	PE^{2}HR
Comm. anonymity	O	O	O	C
Sender anonymity	¬	¬	¬	C
Data anonymity	¬	¬	?	C
Authentication	T	T	T	A
Authorization	S	S	C	C
Confidentiality	?	?	?	C
Deniability	¬	¬	¬	C
Unlinkability	¬	¬	?	C
Data structure	C	SC	¬	SC

4.1 Virtual Hard Disk

This approach provides remote storage space which is accessible via the Internet. It offers the user the possibility to realize arbitrary folder structures for data management, usually by means of the WebDav protocol. Typical representatives are iDisk (Apple), Xdrive (AOL) and Gspace (Google). Considering these products one can conclude that authentication is realized by means of traditional authentication methods, e.g. username/password, and authorization is realized by means of DAC or MAC strategies. The data structure is solely determined by the user. In general methods to guarantee confidentiality are not integrated into these products, however server-side encryption could be established. Methods for the remaining objectives are not yet implemented in the above mentioned products, as far as we could find out.

4.2 Personal Health Record Platforms

Personal health record platforms provided by major vendors such as Google (Google Health) or Microsoft (Health Vault) are growing in popularity. For example, Google provides a patient centric and patient moderated system, that offers the possibility to organize health related data of a person and moreover enables the integration of third party services offered by physicians, hospitals and pharmacies. As above, the same arguments hold for these systems, but the server takes influence on the data structure by demanding certain aspects of this structure.

4.3 PIPE

The architecture PIPE (pseudonymization of information for privacy in eHealth) (Riedl et al., 2007; Riedl et al., 2008) focuses on the management of person related medical documents in a pseudonymized fashion. In this context pseudonymization means the replacement of personal information by a document related specifier which is not linkable to the holder of the document. The authorization for pseudonymized documents is realized by means of a hierarchical structure of cryptographic keys and encrypted document related specifiers. Both can be shared with other users. One major aspect of the architecture is the establishment of key-backup mechanisms based on threshold secret sharing schemes. The latter aspect positively influences the availability of cryptographic keys, however, has no positive impact on security and privacy properties considered in this paper.
Authentication against the system is realized by applying digital signatures, whereas the used protocol easily allows impersonation attacks. However, the authentication solely provides access to the encrypted master cryptographic key of the user, which will subsequently be decrypted at the client. In context of an EHR the above mentioned pseudonymization is in our opinion impractical when using different medical document types, because they always contain unstructured narrative text passages (even CDA Level 3). Consequently, the pseudonymization has to be performed manually, and hence the effort would be unacceptable in our opinion. Additionally, data anonymity can not be guaranteed when not using anonymous authentication. For example, if a patient integrates a pseudonymized medical finding into the system, then this document will be linkable to the authenticating party (the patient) by an insider. The same argument holds for the objective unlinkability. Confidentiality is not taken into the consideration in (Riedl et al., 2007; Riedl et al., 2008) due to the pseudonymization. The remaining objectives are not provided by this architecture. The data structure can not be analyzed seriously due to the facts that a simple conceptual model is used and further crucial details are not published. Additionally, it must be emphasized that the "pseudonymization" of more complex conceptual models requires more sophisticated methods (Slamanig et al., 2007).

5 PRIVACY ENHANCED EHR

In this section we discuss methods that help to preserve the patient's privacy in context of EHRs with

respect to the security and privacy objectives defined in section 3.

5.1 Anonymous Communication

Mechanisms that provide anonymity and unlinkability of messages sent over a communication channel are denoted as anonymous communication techniques and have been intensively studied in recent years, see (Danezis and Diaz, 2008) for a sound overview. There are several implementations available for low-latency services like Web browsing, e.g. Tor (Dingledine et al., 2004), JAP (Federrath, 2005) as well as high-latency services like E-Mail, e.g. Mixminion (Danezis et al., 2003).
These anonymous communication channels help to improve the privacy of users in context of eavesdroppers and curious communication partners. Especially, regarding the latter one anonymity can be preserved if electronic interaction does not rely on additional identifying information at higher network layers, i.e. the application layer. For example, a user who queries a public web page using an anonymous communication channel may remove all identifying information from higher network layers and thus can stay anonymous. However, if service providers offer their services only to authorized sets of users (e.g. subscription-based services, closed communities), they require identification which in general takes place at higher layers by means of authentication mechanisms. In the latter context anonymity can however be preserved by means of anonymous authentication.

5.2 Anonymous Authentication

Anonymous authentication aims to provide a somewhat paradoxical solution to enhance user's privacy in context of authentication. It provides mechanisms such that a user is able to prove membership in a group $U' \subseteq U$ of authorized users U, whereas the verifier does not obtain any information on the identity of the user. Clearly, anonymous communication systems are a prerequisite for providing anonymity in the context of anonymous authentication.
A naive approach to realize anonymous authentication would be to give a copy of a secret k to every user $u \in U$, which could be used in conjunction with a traditional authentication scheme. Obviously, the revocation of a single user u_i would result in a reinitialization and thus in reissuing a new secret k' to every user $u \in U \setminus u_i$. Hence, this approach is far from being practical. Improved techniques for anonymous authentication were explicitly treated in (Boneh and Franklin, 1999; Lindell, 2007; Schechter et al., 1999) and can additionally be derived from group signatures (Ateniese et al., 2000; Chaum and van Heyst, 1991, etc.), ring signatures (Rivest et al., 2001; Dodis et al., 2004, etc.) or similar concepts as (deniable) ring authentication (Naor, 2002), whereas the latter class of signatures and authentication schemes is preferable to group signatures in the context of large groups, since they can be generated "ad hoc" without depending on an explicit setup phase.

5.3 Authorization and Confidentiality

In contrast to strategies implemented by means of application layer mechanism (see section 3.3) there exists the possibility to realize DAC based on cryptographic tokens (Stingl et al., 2006). In particular, all resources are encrypted by their owners (client-side encryption) which hold the corresponding secret keys and are stored encrypted in the system. In particular, if a user grants access to another user she provides a cryptographic token to this user. This cryptographic token represents the secret key to the respective data object, encrypted with the public key of the grantee. In other words, access control based on cryptographic tokens is realized by means of the ability of authorized persons to properly decrypt resources, e.g. content data. This access control strategy provides a serious advantage in comparison with the before mentioned strategies, namely insiders are solely able to bypass the access control by breaking the underlying cryptographic primitives (symmetric resp. asymmetric cryptosystem). Additionally, it can be used to realize fine-grained access, i.e. to single data objects, in contrast to approaches which allow to share all data or no data with other persons, e.g. physicians, (Demuynck and Decker, 2005).

5.4 Pseudonymization

Pseudonymization of person related data (u,x) is the process of replacing every person identifier u for example by the value $nym = E_k(u)$, where E_k is an appropriate symmetric encryption function with a corresponding secret key k. Since k is kept secret it is practically impossible to invert $E_k(\cdot)$ without the knowledge of k and thus compute u given the value nym. However, a person which is in possession of k can easily compute $D_k(nym) = u$ using the corresponding decryption function $D_k(\cdot)$. Hence (nym,x) can not be linked to u anymore.
We realize pseudonymization by letting every user u_i choose a second identifier P_{u_i} uniformly at random, i.e. a pseudonym (Chaum, 1981). This pseudonym is used by her to identify her shares. In order to pre-

vent the linkage between a user and a pseudonym, the pseudonym is solely stored in an encrypted fashion, $E_{k_{u_i}}(P_{u_i})$, in the user repository. The unlinkability holds, since P_{u_i} is independently chosen from u_i and furthermore $E_{k_{u_i}}(P_{u_i})$ can only be inverted by u_i, who holds the corresponding key k_{u_i} (which can be derived from a appropriately chosen password or passphrase defined by u_i). This simple example can be generalized to pseudonymize an arbitrary conceptual model (Slamanig et al., 2007). The resulting pseudonymized conceptual model provides data anonymity and static unlinkability (concerning any observer of the system) and it enables highly efficient implementations. Additionally, by means of anonymous authentication the system provides dynamic unlinkability. Furthermore, it must be emphasized that the conceptual model can be defined by the EHR system and users are able to freely create their own structures with respect to the conceptual model.

5.5 Multiple Identities

However, there still exists the precarious disclosure attack which can lead to the disclosure of the complete EHR of a person. Therefore we need a measure to provide plausible deniability in a cryptographically provable sense. As countermeasure we propose the use of so called multiple identities (Slamanig and Stingl, 2008b). In this context multiple identities can be described by means of dividing the EHR of a person into so called sub-identities (see Figure 1).

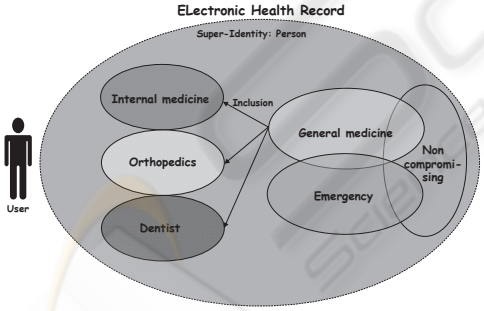

Figure 1: Multiple identities.

A user can assign a subset of her EHR to each of these sub-identities. Thereby, these subsets do not need to be disjoint. Subject to the person, the medical data are presented to, the user is able to choose one of her sub-identities (e.g. a special prepared, non compromising one) and consequently opens the assigned subset of medical data. Hence, a user can hide sensitive data in a special sub-identity in order to prevent disclosure of medical data. However, one drawback of this approach is that passwords which are used to derive the cryptographic keys for the respective identities need to be chosen independently of each other. More precisely, there must not be any relationship between passwords which clearly could be computed by an adversary too. However, we assume that in practice the number of identities and passwords respectively will be moderate. Furthermore, this concept additionally provides the possibility to create so called super-identities which can hold several sub-identities. Thus, super-identities can be used to comfortably manage the respective sub-identities.

6 CONCLUSIONS

In this paper we discussed security and privacy aspects which are especially of relevance in context of web-based EHR systems. Following these objectives, we investigated deployed solutions for EHR systems as well as concepts discussed in the literature. Regarding these systems we can conclude that either patient's need to fully rely on the trustworthiness of the provider of an EHR system (e.g. Google Health) or there exist methods to bypass the implemented security concepts. This is due to the fact that security concepts are focusing solely on specific aspects and not the entire EHR system. However, in our opinion it is absolutely necessary to consider all the relevant security objectives in order to provide an adequate protection of the patient's privacy. Nevertheless, by applying specific methods (e.g. anonymous authentication) one is confronted with additional challenges. For example, in context of anonymous authentication it is apparently impossible to realize user specific resource limits. Actually, we are working toward a solutions based on blind signature techniques. Furthermore, we are investigating strategies for the choice of anonymity sets for anonymous authentication. The latter aspect is crucial, since not appropriately chosen strategies may lead to unwanted user identification (Slamanig and Stingl, 2008a).

REFERENCES

Ateniese, G., Camenisch, J., Joye, M., and Tsudik, G. (2000). A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In *Advances in Cryptology – CRYPTO '00*, pages 255–270. Springer.

Bishop, M. (2002). *Computer Security: Art and Science*. Addison-Wesley.

Boneh, D. and Franklin, M. (1999). Anonymous authentication with subset queries. In *Proc. of the 6th ACM conference on Computer and communications security*, pages 113–119.

Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–90.

Chaum, D. and van Heyst, E. (1991). Group signatures. In *Advances in Cryptology – EUROCRYPT '91*, LNCS, pages 257–265.

CSI (2007). Computer Crime and Security Survey 2007, Computer Security Institute. http://www.gocsi.com/forms/csi survey.jhtml.

Danezis, G. and Diaz, C. (2008). A Survey of Anonymous Communication Channels. Technical Report MSR-TR-2008-35, Microsoft Research.

Danezis, G., Dingledine, R., and Mathewson, N. (2003). Mixminion: Design of a Type III Anonymous Remailer Protocol. In *SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 2–15, Washington, DC, USA. IEEE Computer Society.

Demuynck, L. and Decker, B. D. (2005). Privacy-Preserving Electronic Health Records. In *Communications and Multimedia Security, 9th IFIP TC-6 TC-11 International Conference (CMS 2005)*, volume 3677 of *LNCS*, pages 150–159. Springer-Verlag.

Dingledine, R., Mathewson, N., and Syverson, P. (2004). Tor: The Second-Generation Onion Router. In *Proceedings of the 13th USENIX Security Symposium*, pages 21–21.

Dodis, Y., Kiayias, A., Nicolosi, A., and Shoup, V. (2004). Anonymous Identification in Ad Hoc Groups. In *Advances in Cryptology - EUROCRYPT'04*, volume 3027 of *LNCS*, pages 609–626.

Federrath, H. (2005). Privacy Enhanced Technologies: Methods, Markets, Misuse. In *Proceedings of the 2nd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus '05)*, volume 3592 of *LNCS*, pages 1–9. Springer-Verlag.

HI (2004). Harris Interactive, Survey on Medical Privacy. http://www.harrisinteractive.com/news/newsletters/healthnews/HI_HealthCareNews2004Vol4_Iss13.pdf.

Lindell, Y. (2007). Anonymous Authenticaion. *Whitepaper Aladdin Knowledge Systems, 2007, http://www.aladdin.com/blog/pdf/Anonymous Authentication.pdf*.

Naor, M. (2002). Deniable Ring Authentication. In *CRYPTO '02: Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, LNCS, pages 481–498. Springer-Verlag.

Pfitzmann, A. and Köhntopp, M. (2000). Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In *Workshop on Design Issues in Anonymity and Unobservability*, pages 1–9.

Pyper, C., Amery, J., Watson, M., and Crook, C. (2004). Access to Electronic health records in primary care – a survey of patients views. *Med Sci Monit*, 10(11):17–22.

Riedl, B., Grascher, V., and Neubauer, T. (2008). A Secure e-Health Architecture based on the Appliance of Pseudonymization. *Journal of Software*, 3(2):23–32.

Riedl, B., Neubauer, T., Goluch, G., Boehm, O., Reinauer, G., and Krumboeck, A. (2007). A Secure Architecture for the Pseudonymization of Medical Data. In *Proceedings of the The Second International Conference on Availability, Reliability and Security (ARES 2007)*, pages 318–324. IEEE Computer Society.

Rivest, R. L., Shamir, A., and Tauman, Y. (2001). How to Leak a Secret. In *Advances in Cryptology – ASIACRYPT '01*, LNCS, pages 552–565. Springer.

Schechter, S., Parnell, T., and Hartemink, A. (1999). Anonymous Authentication of Membership in Dynamic Groups. In *Proc. International Conference on Financial Cryptography 99*, volume 1648 of *LNCS*, pages 184–195. Springer-Verlag.

Slamanig, D. and Stingl, C. (2008a). Anonymous Authentication - Principles and Application (German). In Horster, P., editor, *Proceedings of DACH-Security 2008*, pages 123–134. IT-Verlag.

Slamanig, D. and Stingl, C. (2008b). Privacy Aspects of eHealth. In *Proceedings of the The Third International Conference on Availability, Reliability and Security (ARES 2008)*, pages 1226–1233. IEEE Computer Society.

Slamanig, D., Stingl, C., Lackner, G., and Payer, U. (2007). Preserving Privacy in a Web-based Multiuser-System (German). In Horster, P., editor, *Proceedings of DACH-Security 2007*, pages 98–110. IT-Verlag.

Steinbrecher, S. and Köpsell, S. (2003). Modelling Unlinkability. In *Proceedings of Privacy Enhancing Technologies workshop (PET 2003)*, volume 2760 of *LNCS*, pages 32–47. Springer-Verlag.

Stingl, C., Slamanig, D., Rauner-Reithmayer, D., and Fischer, H. (2006). Realization of a Secure and Centralized Data Repository (German). In Horster, P., editor, *Proceedings of DACH Security 2006*, pages 32–45. IT-Verlag.

TCG (2008). Trusted Computing Group. http://www.trustedcomputinggroup.org.

Win, K. T. (2005). A review of security of electronic health records. *HIM J*, 34(1):13–8.