A Framework of Privacy Shield in Organizational Information Systems

Geoff Skinner, Song Han and Elizabeth Chang
School of Information Systems, Curtin University of Technology
Australia
Email: geoff.skinner@newcastle.edu.au, {Song.Han,
Elizabeth.Chang}@cbs.curtin.edu.au

Abstract

Preserving Privacy and the protection of personally identifiable information (PII) have been of increasing interest over the last few years. Many privacy advocates, and a significant portion of the general public, feared that the new initiatives used in an attempt to fight terrorism, would have a serious impact on an individual's right and ability to protect their privacy. This paper proposes a new framework for Preserving Privacy for individuals along with the protection of personally identifiable information. We have termed it Privacy Shield. Through the application of anonymity and privacy principles in design, the privacy protecting separation of data, the use of public key infrastructure, and the application of our Information System Hippocratic Policies, we provide a framework of privacy shield to protect an information system user's personal data.

.

1 Introduction

Consider the following scenario: There is an international logistics company DEDAO PR, who's President wants to receive some suggestions from the managers in DEDAO PR. The President hopes every manager will provide reasonable and practical suggestions that will help the President to manage and conduct the DEDAO PR in a successful and fruitful way. However, the managers of West PR are located all over the world. Some managers do not always provide their true suggestions; since they worry that the President may de-rank some managers, because of their suggestions. That is, information from the suggestions may be helpful to DEDAO PR, but a little offending to the President. Therefore, the President wishes that the suggestions would be protected. In order that they not to be viewed by outside users. Also, the managers wish the company to maintain privacy such that the President will not identify them if they choose to make an anonymous statement.

For this case, how could we realize the President's intention for DEDAO PR? How could we maintain the managers' privacy? To solve these issues, we propose a framework of privacy shield. This framework will be flexible and useful in organizational information systems.

2 Background and Related Work

Privacy and anonymity have both been the topics of much debate in the wake of recent and ongoing terrorist attacks and threats. These events have further highlighted the there is a distinct difference between security and privacy. Along with the diverging objectives of each. Security is not privacy, in that a secure information system does not necessarily mean a privacy preserving system. Likewise, a privacy preserving system does not infer it is a secure system. One of the main issues that need's to be addressed, is how to find a suitable balance between security and privacy. The balance needs to be maintained at all levels: individual, system, and organizational. With all of the new security regulations we address the need for privacy equilibrium.

Privacy is viewed as a fundamental human right, and one of the most important of the modern age. However, it is perhaps the most difficult to define [1]. Specific rights to access and control one's personal information appears in most updated constitutions and regulations, along with the ongoing introduction of new privacy laws. There is a need to develop future information systems that support these privacy rights. This paper focuses primarily on one of the main components of privacy, that is, information privacy. The proposed solution is aimed at a technological model for privacy protection.

Our own goal in this paper is to develop what we have termed privacy shield, which is primarily achieved through the use of anonymity and other privacy principles. Additionally, it requires the integration of another one of our proposals, the concept of the separation of data. The separation of data is discussed in the next section and aims at addressing privacy preserving methods of not

Proceedings of the International Conference on Mobile Business (ICMB'05)
0-7695-2367-6/05 $20.00 © 2005 IEEE

only protecting personal information stored in databases, but also other information system storage mediums.

3. A Framework of Privacy Shield

This section will provide a new framework for privacy shield. This framework is composed of four aspects of privacy protection techniques: ***separation of data***, ***using of information system hippocratic polices***, ***selection rights of anonymity***, and ***embedding of public key infrastructure***. We will first provide the overview of specifications for these techniques. Finally, we propose the framework for the privacy shield.

3.1 Separation of Data

The concept of separation of data is defined from a data-property point of view. The following is the formal definition of Separation of Data:

Separation of Data: We assume D is an information system. D includes two categories of data: (1) A is defined as data of personally identifiable information; (2) B is defined as data of operational system information. We call a technique as Separation of Data if:

***** Any data*** $a \in A$ ***will be protected by the highest level of security and privacy protection.***

***** Any data*** $b \in B$ ***will be limitedly accessed with limited permission of the information system administrator.***

Separation of data also means that where ever feasible the information should be collected and stored in an anonymous format. This is to provide better personal information privacy. While this is a very simple outline of the separation of data, please refer to our other work [2,3] to help better understand this concept. At the same time, the framework of this definition applies to both the use of separate databases for different types of classified data, and also the use of separate storage locations for all data not stored in the databases.

At the core of the separation of data concept is the use of separate databases to store the different categories of information. Like most information systems, the majority (but not all) of the data is stored in databases, and therefore we propose the use of Hippocratic Databases [4] for this purpose. As they include the responsibility for the privacy of data they manage, it provides our system with another privacy protection layer for the privacy shield. Hippocratic databases also share our goal of preventing disclosure of private information, so their use for storing PII data is ideal for the proposed framework. The key is to ensure that the initial design and collection of data from various inputs classifies the collected information into their correct groupings. It then stores it in the corresponding database. We have used separate database structures rather than a single database with multiple tables due to the benefits of working with complete and separate data sources from a coding and connection perspective. This is in addition to the added security and database system management advantages.

The same principles apply to any data that is not stored in the database. That is, files and other documents such as emails; reports; system logs; etc, when collected and/or created in the information systems are classified on the contents of the information contained within them. They are then stored in locations that have the respective privacy and security mechanism applied to them depending on their level of sensitive information. The greater the level of sensitive information the higher level of privacy and security protection applied to the data.

3.2 Selection Rights of Anonymity

Generally in information systems, anonymity is categorized into three different levels: (1) Anonymous; (2) Pseudo-Anonymous; (3) Identifiable. This privacy design principal entitles any user in the information system to choose their own level of anonymity. It allows for anonymous data collection and use; the availability and the encouraged use of multiple pseudonyms for each user. Further, data storage and system design is focussed on not revelling any information that could be used for inferring addition information or relations between the different operational system ID's for a user.

3.3 Information System Hippocratic Polices

This subsection will provide our information system hippocratic polices. Like the hippocratic database principles that govern the design and implementation of the databases used for our information systems, the rest of the system

should be designed through the guidance of the information system hippocratic policies.

1. ***Anonymity:*** Whenever and wherever possible the personal information collected and stored in the information system should be done in a way that supports anonymity for the individual user.
2. ***Limited Collection and Use:*** The personal information collected must be the minimum necessary for the primary purpose specified to the individual. Once collected the system will only use that information for the primary purpose specified to the individual.
3. ***Limited Disclosure and Retention:*** The information system may not disclose the personal information other than for the primary purpose of collection or keep it for a period longer than the primary purpose requires without the individuals explicit consent.
4. ***Security and Sensitive Information:*** The information system must take all reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure. Sensitive information must always be protected by 'stronger' security safeguards.
5. ***Openness, Access, and Integrity:*** The information system must have documented and make easily available its policies and procedures for the management of personal information. It must also make all personal information about an individual available to that individual and allow them available to make corrections and up-to-date. If the individual is unable to make the corrections then the system must take all reasonable steps to ensure the integrity of the personal information.
6. ***Third Party and Transborder Uses:*** The information system may not transfer information to a third party or foreign country without the consent of the individual.
7. ***Identifiers:*** The information system must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by external agency or government body.

3.4 Embedding of Public Key Infrastructure

Public key infrastructure has already been well developed and applied to e-government, e-commerce, e-health, e-society [5, 6]. For the information systems, embedding of public key infrastructure means that the use of PKI technologies facilitates the additional implementation and support of strong security methods. Through the use of SSL for all network communications, the generation of user public-private key pairs for anonymity support and data security, and the use of certificate authorities for identity confirmation the comprehensive protection provided by the privacy shield is complete.

4 Framework of Privacy Shield

In this subsection, we will combine the above four components (***separation of data***, ***using of information system hippocratic polices***, ***selection rights of anonymity***, and ***embedding of public key infrastructure***) to be a new model: ***privacy shield***.

Our proposed Privacy shield is there to oversee and manage privacy issues in an information system. It functions to coordinate the privacy policies of a system and the collection and use of data and personal information. Additionally, it assures compliance with the privacy and security procedures built into an information system. Privacy shield is not a single entity but rather a collection of policies, procedures and technological approaches to system design to provide a comprehensive privacy preserving environment. Through the application of anonymity, the separation of data, Public Key Infrastructure (PKI) [7] technologies, and Information System Hippocratic Policies [8] in the system development life cycle of information systems a shield of privacy can be provided.

Privacy shield when used provides the protection of both system and personally identifiable information (PII). The protection extends beyond normal database storage structures to include all types of data storage mediums used by an application, information system, and/or collaborative environment. Privacy shield provides a complete and comprehensive system solution for addressing information system privacy and security requirements and user concerns. It is made up of the four key foundation components listed above. The diagram below (Figure 1) provides a graphical representation of Privacy shield and the relation of its four foundation components.

In order to obtain privacy shield there are a number of additional processes and procedures

that need to be followed in addition to the use and planned application of the four core components listed above. Each of these processes and procedures and detailed in some of our other publications and are performed throughout different stages of the system development lifecycle. That is, through the traditional phases of project planning, analysis, design, implementation and testing, and support and maintenance of a new information system.

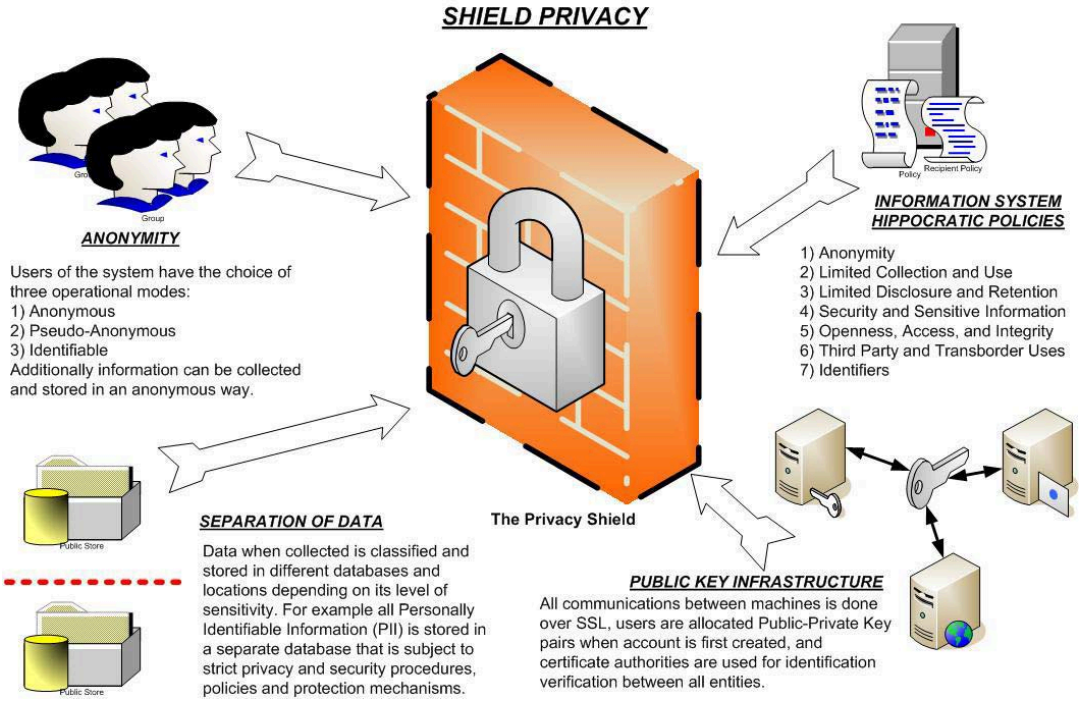

Figure 1: Privacy shield and its key components.

5. Conclusion

In this paper we proposed a framework for information systems – *privacy shield*. This framework consists of the application and usage of Anonymity, the concept of the Separation of Data, the application of Information System Hippocratic Policies, and the well planned use and implementation of Public Key Infrastructure technologies. The objectives of privacy shield is to promote and enforce privacy considerations in all stages of the (Information) System Development Life Cycle (SDLC).

References

[1] Electronic Privacy Information Centre and Privacy International; Privacy and Human Rights 2003 – An International Survey of Privacy Laws and Developments. *http://www.privacyinternational.org.*

[2] G.D. Skinner; Name of paper. *Ethical Spectacle and CATO Institute Briefing Papers, December 8, 1999. http://www.spectacle.org.*

[3] G.D. Skinner; Name of paper. *Ethical Spectacle and CATO Institute Briefing Papers, December 8, 1999. http://www.spectacle.org.*

[4] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu; Hippocratic Databases. *Proceedings of the 28th VLDB Conference, Hong Kong, China, 2002.*

[5] B. Schneier. Applied Cryptography. John Wiley & Sons, 1996.

[6] E. Eklund; Controlling and Securing Personal Privacy and Anonymity in the Information Society. *http://www.niksula.cs.hut.fi/~eklund/Opinnot/netsec.html.*

[7] 108th Congress, 2d Session, H.R. 4414; Privacy shield Act (Introduced into the House). *http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4414:, May, 2004.*

[8] G. Skinner, E. Chang, M. Miller, and J. Aisbett; Privacy shield Hippocratic Security Method for Virtual Communities. *IECON2004, The 30th Annual Conference of the IEEE Industrial Electronics Society, Nov 2-6. 2004 Korea.*