The Computational View of Information Privacy for Privacy Enhancing Technologies

Geoff Skinner, Song Han, and Elizabeth Chang
Centre for Extended Enterprise and Business Intelligence
Curtin University of Technology, Perth, WA, Australia

Abstract.
Information privacy is a very subjective and context sensitive area of research open to many interpretations. As such it has seen an increasing number of solutions proposed that address the issue of privacy protection. What is missing is a way of classifying the level of protection these privacy protecting solutions provide. This paper addresses this problem by firstly defining the computational view of Information Privacy. Within this view three levels of privacy protection are defined and applied to a number of Privacy Enhancing Technologies that are in use today or in current development. The paper is aimed at providing a unique proposal for terminology that can be utilized in the information privacy field to categorize privacy protecting solutions.

Keywords: **Inform**ation Privacy, Computational Privacy, Privacy Enhancing Technologies.

1 INTRODUCTION

The protection of personal information and the ability of information systems and data collectors to ensure the information privacy of the entities providing the data is a very important issue. Driving the interest in the field are two differing perceptions and objectives of the key entities involved. At one end of the spectrum are the data collectors and at the other end the data providers. Organizations and information collectors in general, have realised the value of data collection, analysis and storage [Damiani et al., 2003]. This has resulted in increased collection of data, in particular personal data, often for use in financially rewarding undertakings on behalf of the collectors. The collectors perception conveyed to the providers is that by increased collection of personal data they are able to provide improved, more efficient and personalized services [Milken Institute, 2006]. What is often overlooked is the need to protect the personal data and the privacy of the entities providing it. Increasing misuse of data and bad publicity on privacy violations and breached data protection procedures has resulted in many entities, the data providers, becoming increasingly concerned about collector's privacy practises [Oberholzer et al., 2005][Nykamp et al., 2001]. For clarity of terminology an entity is defined as being an individual, group, or organization [Skinner and Miller, 2006]. Each of the entities can be both an information collector and provider.

Numerous methods and solutions have been proposed to provide privacy protection. The proposals can be divided into four major privacy protection models [EPIC, 2003]. The four models are: Comprehensive Laws, Sectoral Laws, Self Regulation, and Technologies of Privacy. It is the last model, commonly referred to as Privacy Enhancing Technologies (PETs) that is the focus of this paper. Like privacy protection solutions, within the Technologies model a large number of solutions have been proposed, with an increasing number being implemented [Goldberg, 2002], [Langeinrich, 2000]. With so many solutions available it is proving very hard to determine the validity of one product against another. There has been no baseline measurement or terminology for their categorization. What is required is some form of classification and scaling method than can be applied to the PETs to rate them on their level of privacy protection. This is the motivation for this paper, to provide a terminology within Information Privacy, specifically from a computational context. A computational view of privacy encompasses the levels of privacy protection different PETs can provide when each is subjected to malicious attacks over varying time intervals and with varying computational resources.

It is proposed that the terminology defined within this paper can be adopted by PET designers and developers. The terms can be used to classify their proposals and likewise subject them to independent review for similar classification. Focus has been placed on the technologies of privacy model due to its privacy protecting nature. The other three models of privacy protection can be complimentary or contradictory depending on their application. The privacy protection can vary from country to country, industry to industry, and organization to organization often based on each principle's objectives. The technological model is less susceptible to the subjective nature of privacy interpretation, and focuses rather on providing system level protection. It must be noted though, that even the technological privacy protection schemes can be flawed due to incorrect or inadequate application by the entities utilizing them. As will be discussed through the remainder of the paper, some PET's can be poorly designed or designed for law enforcement access [EPIC, 2003]. Therefore entities wishing to apply the technologies for their own privacy protection need quality information on the effectiveness and level of protection provided by each PET. The terminology defined from our work takes positive steps in this direction.

Another aspect of privacy protection that is incorporated into the terminology proposed in this paper is the key principle of questioning the initial information collection process. The computational view of privacy encompasses the guidelines of ensuring the technologies can restrict the collection and use of personal data. This is in addition to the main objective of minimizing identifiable data [Weinstein and Neumann, 2003]. Entities should be able to engage in transactions without having to reveal their identity. A classification of a small subset of some of the well known PETs is provided later in this paper using the terminology defined. Before this however, Section 2 provides additional information on background material and related work. The proposed terminology for the computational view of privacy is provided in Section 3. Section 4 applies the terminology for PETs classification, and a conclusion is given Section 5. A bibliography of all references used throughout the paper is found following Section 5.

2 BACKGROUND AND RELATED WORK

Just as privacy protection can be sub-divided into four major models, so can further categorization made within the Technologies of Privacy model. Formally, Privacy Enhancing Technologies (PETs) are the application of information and communication technologies for privacy protection [Borking, 2001]. They include tools, standards and protocols that protect privacy by preventing unnecessary and unauthorized processing of personal data, as well as eliminating or at least reducing the amount of personal data collected. A leading expert in the field of privacy, Clarke classifies PET's into three broad kinds [Clarke, 2001]:

- Countermeasures against privacy-invasive technologies: aim to defeat or neutralise privacy-invasive technologies.
- Savage PET's: set out to deny identity and provide genuine, untraceable anonymity.
- Gentle PET's: balance the interest of privacy and accountability, and are oriented towards protected pseudonymity.

Each kind provides a different level of privacy protection, but until now no formal terminology has been defined for the level of privacy protection each kind provides. It is understood that no matter what kind of PET we are discussing they all aim to perform a variety of key functions. Some of the functions include: preventing unauthorized access to personal data; automating retrieval of data collector's privacy practises and data provider privacy preferences; filtering unwanted messages; preventing automated data capture (such as cookies); preventing communication from being linked to a specific entity; and facilitating transactions that reveal minimal personal information [Cranor, 2000].

As PET's focus on the protection of personal data and an entities digital identity (its virtual representation of their real world identity) we must also clearly define the type of privacy protection we are providing. That is, from a definition of a particular dimension of privacy one can loosely categorize the solutions aimed at each of them. Privacy in general is very subjective and means different things to different people. Common among all interpretations is the perspective that privacy is a human right but is context and environmentally dependent. A number of common privacy dimensions have been defined that have gained wide acceptance [Clarke, 1999]. They are as follows:

- Privacy of the person
- Privacy of personal behaviour
- Privacy of personal communications
- Privacy of personal data

Personal data, also referred to as information privacy is the focus of PETs and their privacy protection. In [Clarke, 1999] Clarke also provides a well referenced definition of information privacy after initially stating it as being a combination of personal communication privacy and personal data privacy. His formal definition of information privacy is "… the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves." [Clarke, 1999]. The Common Criteria (CC) [CC, 2004] provides a more formal requirements based definition for providing "… user protection against discovery and misuse of identity by other users.". As you can see from the CC definition, it is information systems requirements focused, with emphasis on identity protection. Identity protection is a major component of information privacy but by no means represents the complete embodiment of its full meaning. Likewise PETs privacy protection encompasses more than just identity protection as mentioned above.

There are an increasing number of PETs being proposed and developed to help provide increased levels of privacy protection. One extensive solution has been proposed and partially implemented by Borking and Hes [2000]. It is based around the concept of Identity Protectors. The authors approach is to question the amount of personal data that really needs to be collected in information systems. Once collected they divide a 'privacy-protected' system into two separate domains and use the identity protector to convert a user's actual identity into a pseudo-identity. The idea is to minimize the 'identity-domain', and maximize the 'pseudo-domain' for increased privacy protection. Their view of privacy-protection systems of the future would have the identity protector take the form of a user controlled smart card. The card seems to be initially 'separate' from the Information System and is primarily used to generate pseudo-identities. For anonymous transactions it is mentioned that the identity protector can be integrated into the information system. Along similar lines of privacy protection to the Identity Protector are the solutions proposed in [Skinner & Chang, 2004b] which developed a Privacy Shield and also work on Hippocratic Privacy Policies for Information Systems [Skinner & Chang, 2004a]. They were in turn inspired by the work being done on Hippocratic Databases [Agrawal et al., 2002]. It involves the designing and developing of databases to include responsibility for the privacy of data as a fundamental tenet. The privacy principles the database is responsible for are built upon the 'foundation' principles found in most current privacy legislations and guidelines. They normally have been derived from the Fair Information Practices (FIPs) [FTC, 2003] and the OECD Guidelines for Governing the Protection of Privacy and Transborder Data Flows of Personal Data [OECD, 1980].

A number of IBM Research groups and collaborators have been working on a few interesting approaches to privacy. Part of their work has been extensions and usage of P3P [W3C, 2002]. This includes implementing P3P using Database Technologies [Agrawal et al., 2003]. This is an architectural alternative for implementing P3P, moving away from a client-centric model. Rather, it is based on a server-centric implementation that reuses database querying technology. The other P3P related work is termed the Platform for Enterprise Privacy Practices (E-P3P) [Karjoth et al., 2002]. It defines technology for privacy-enabled management and exchange of customer data. The basic concept is to place access restrictions on personal data. The restrictions are expressed in a privacy-specific access control language. The Enterprise Privacy Authorization Language (EPAL) is another privacy initiative developed by IBM [Karjoth and Schunter, 2002], [Backes et al., 2003], [Backes et al., 2004], [IBM, 2003]. EPAL enables an organization to formalize the exact privacy policy that shall be enforced within the organization. It formalizes the privacy promises into policies and associates a consented policy to each piece of collected and possibly shared data. A number of privacy enhancing tools and contributions have been provided by David Chaum. In particular his work on: Blind Signatures [1985a], [1992], [1985b]; Digital Cash [1989]; Un-traceable electronic mail, return address, and digital pseudonyms [1981]; and privacy protecting protocols for transmitting personal information between organizations [1986].

3 THE COMPUTATIONAL VIEW OF INFORMATION PRIVACY

The computational view of privacy is derived from a time and resource dependent dimension. It is a representation of the level of privacy protection offered by an information system over a period of time. During this time frame computational resources are being used in an attempt to compromise the level of privacy protection and therefore gain unauthorized access to personal data. We have identified and defined three categories of privacy protection. The classifications are from the highest level of protection to the lowest. The three include Ideal Privacy, Computational Privacy, and Fragile Privacy, listed from highest to lowest protection respectively. From an object perspective the nature of the computation view of information privacy is the level of privacy protection.

Only three levels of privacy protection have been defined due to the logical mapping to three distinct computational states, respectively corresponding to each level. That is, for a computational comparison and classification there are those measures that remain very large or approach infinity, then at the opposite end of the measurement spectrum those that are very small or approach zero. In addition to the two extremes there are those cases that fall in between. In the case of computational privacy, the measurement is based on attempting to circumvent or compromise the level of protection. Therefore, privacy protection measures taken in the middle will always approach zero but at slower rates than those closer to or at the spectrum end of zero. This implies that defining additional privacy protection levels besides the three discussed would not be beneficial. As all additional middle spectrum measures still approach zero eventually. Hence, the middle measure of privacy protection, computational privacy, is sufficient and encompasses all levels of protection between the two extremes.

NATURE (N) = Level of Privacy Protection (pp).

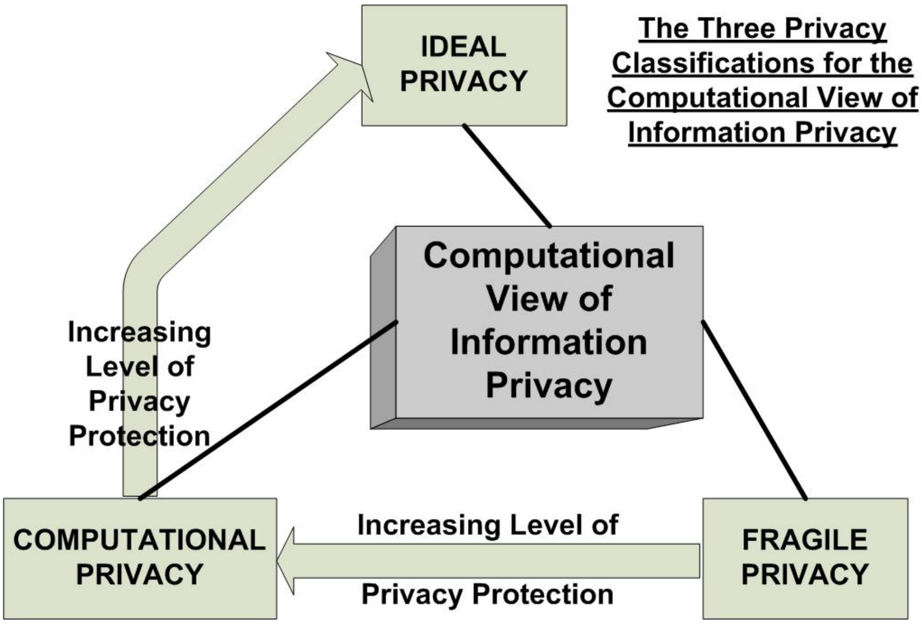
The Three Privacy Classifications for the Computational View of Information Privacy
IDEAL PRIVACY
Computational View of Information Privacy
Increasing Level of Privacy Protection
COMPUTATIONAL PRIVACY
Increasing Level of Privacy Protection
FRAGILE PRIVACY

Fig. 1. The three levels of privacy protection within the Computational View of Information Privacy

3.1 Ideal Privacy

Privacy Protection: pp = ∞ for Ideal Privacy

With Ideal Privacy, users at all times determine when, how and what personal information is revealed. Additionally personal data owners decide to what extent others can utilize their information once access is granted. Ideal Privacy gives users complete control over their personal data and more generally all of their information privacy concerns.

Definition 1: *Ideal Privacy provides the highest level of privacy protection (theoretical and practical), providing users with complete control over all of their privacy concerns. No amount of computation can compromise ideal privacy protection.*

$$\{\text{As } r(t) \to \infty;\ pp = \infty\}. \qquad \textbf{(1)}$$

This translates to: Given unlimited computational resources, (r), (r -> ∞) over and infinite time, (t), (t-> ∞) privacy protection, (pp), will always remain at the highest level and stay uncompromised (pp = ∞).

This kind of privacy is maintained through unconditional privacy and security mechanisms. In this case there is no possible way that the privacy protection can be circumvented or compromised. Absolute or complete privacy is guaranteed from an information owner's perspective. The context and extent of ideal privacy is defined for the virtual environments in advance. It is the defined scope of privacy protection that is deemed to be ideal for the information systems in question. The entities that are also the owners of the personal information are assured that their personal data is unconditionally protected. To further facilitate this level of protection, the entities using the system have complete control over their own personal information. They are able to access and modify it as required. Access permissions to their personal information, along with the security and privacy settings protecting that information, may be altered at any time by the personal data owner. In the ideal setting not even the system owners and administrators are able to access or use an individual's personal information without their consent.

The provision of Ideal Privacy requires the additional environmental condition of ideal security. That is, the personal data that is to remain private is protected with ideal security measures. Therefore, the personal data is under the complete control of the owner and only the owner. This requires the entity to be able to manage authorization and access control methods to their data. Entities are able to manage not only when, how and what personal information is revealed, but also who that information is available to. Due to the inherent membership characteristics of virtual environments, such as collaborations and virtual communities, access control lists may be utilized. Unlike more open information sharing environments like the Internet, users are initially registered and authenticated when joining the membership of a virtual environment. The preferred method would be the use of Role based Access Control approaches to decrease the administration burden for system administrators and users.

Perfect privacy is very rarely obtainable in the real world if at all. Therefore, perfect privacy is generally only obtained in theoretical frameworks and solutions of similar ideal conditions. However, with the correct application and enforcement of ideal privacy principles and unconditional security mechanisms future systems will get very close. A factor that will always be a burden for Ideal Privacy is due to the subjective nature of the concept of privacy itself. Each entity may have different interpretations of information privacy and therefore to each individual entity ideal privacy may be reality or a goal that can never truly be reached. Another factor that influences an entity's perception of privacy is trust. This relates to the privacy protection of the personal data once shared and who it is shared with. However, this area encroaches into the field of trust which is a rapidly growing area of research and therefore beyond the scope of this paper due to space limitations. For brevity the important concept to note is that privacy and trust are inter-related, along with security and context. All four of these elements exert an influence on each of the other elements [5]. In order to maintain Ideal Privacy the entity revealing their personal data must be confident that the data receiver will respect their privacy preferences. That is, to only use the data provided for the purpose it was requested for and nothing more.

3.2 Computational Privacy

Privacy Protection: pp -> 0 for Computational Privacy

With Computational Privacy, users are provided with significant control over when, how and what personal information is revealed. Additionally personal data owners are the primary entities deciding to what extent others can utilize their information once access is granted. Computational Privacy gives users a high level of control over their personal data and more generally all of their information privacy concerns. However, system owners and data collectors also have a level of control over personal data collection and use, once terms have been agreed upon with personal data owners. Computational Privacy means that it is infeasible to compromise privacy protection within reasonable operational parameters. However, given a very long amount of time and a very large amount of resources, it may be possible to compromise the level privacy protection.

Definition 2: *Computational Privacy provides a medium or operational level of privacy protection, providing users with significant but not complete control over all of their privacy concerns. With an infinite or unreasonably large amount of computation, computational privacy protection can be compromised.*

$$\{\text{As } r(t) \rightarrow \infty;\ pp \rightarrow 0\}. \qquad (2)$$

This translates to: Given unlimited computational resources, (r), (r -> ∞) over and infinite time, (t), (t-> ∞) privacy protection, (pp), will eventually be compromised (pp -> 0).

In this case it would take a very long time and an unreasonable amount of resources to compromise this level of privacy protection. Given an extremely large or unreasonable amount of time and resources privacy protection may be compromised. Certain trade-offs or compromises are sought from each user to facilitate the operational and functional requirements of computational privacy in virtual environments. The main design and operational parameters of the information systems based on and working with Computational Privacy should follow the Fair Information Practices (FIP's) [13] as a bare minimum. In addition, a well defined and easily understood set of privacy principles for personal data and system management should govern its operation.

As discussed above for Ideal Privacy, Computational Privacy is supported by Computational Security mechanisms. These increased privacy and security aware environmental operating conditions are most common with more recently developed systems. This is in a response to system owners designing systems that accommodate the increasing number of privacy laws and regulations. Users usually are required to consider and agree to a privacy policy that governs the virtual environment. Under computational privacy an entity has reduced control over their personal information in order to facilitate system operation. The privacy policy an entity agrees to may reduce management and ownership over their personal data. This may be done in order to service the needs of the other entities and tasks of the virtual collaboration. What is important to computational privacy and privacy policy agreements used with it is a clear understanding by the entity of the policy and level of privacy protection. Entities should be made aware that their personal data is protected with computationally secure methods and techniques. These methods should be readily identifiable and where possible explained to the entity. This is to ensure they are accepting of the level of security and privacy protection provided.

3.3 Fragile Privacy

Privacy Protection: pp ->> 0 for Fragile Privacy

Given a reasonable amount of time and resources fragile privacy can be compromised. This level of privacy protection is only deemed effective against weak threats and attacks. Unfortunately, a large number of virtual environments are of this nature, when they should be offering higher levels of privacy protection. As the adaptation and uses for networked computer systems have increased so has the need for better privacy protection. Many internet sites are still of the format that an entity either accepts the organizations stated privacy as is, or the entity is denied access to their services and resources. Additionally, it is normally the case that if the entities consent is given, control over most personal data is relinquished to the information collectors. What further exacerbates the problem is that for the majority of entities, they do not really pay attention to the finer details of the privacy policy they are agreeing to. This results in a privacy agreement that is very fragile in its nature and understanding. Either the entity had no choice but to agree to the conditions, or they did not understand what they were agreeing to.

Definition 3: *Fragile Privacy provides the lowest level of privacy protection, providing users with limited control over all of their privacy concerns. With a reasonable amount of computation, fragile privacy protection can be compromised.*

$$\{\text{As } t\text{->}N_t \text{ AND } r\text{->}N_r;\ pp\ \text{->>}\ 0\}. \qquad \textbf{(3)}$$

This translates to: Given a reasonable amount (N_t a large value) of time (t) (t -> N_t) and a reasonable amount (N_r a large value) of computational resources (r) (r -> N_r) privacy protection (pp) will be compromised (pp ->> 0). That is, the level of privacy protection approaches 0 at a faster rate than Computational Privacy.

From the entity and personal data owner perspective this is likewise perceived as fragile security. The security is fragile in the context that a user is unsure exactly how secure their personal data is once it has been collected. This includes any possible third party uses, such as to whom the initial collector may be revealing the data to, and what it may be used for. This may lead to revelations at a later time that are perceived by the users as a breach of the privacy policy. A common example is the user that suddenly starts receiving a large amount of spam and marketing emails from unknown third party sources. Upon further investigation, it is found that their email details were provided to the third party from the original data collectors. The third parties may be other organizations that are part of a virtual collaboration with the initial data collectors. This data sharing process was outlined either in an indirect or ambiguous way in the privacy policy. However, the user may not have understood its full implications nor had readily available access to someone who could explain it. The end result is a lack of confidence which can result in a breaking down of the relationship.

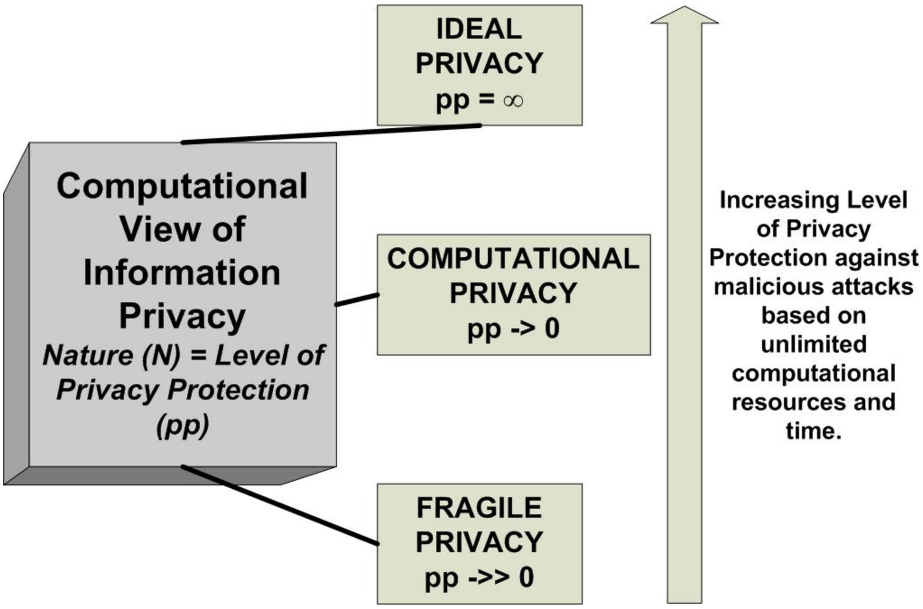
IDEAL PRIVACY pp = ∞
Computational View of Information Privacy
Nature (N) = Level of Privacy Protection (pp)
COMPUTATIONAL PRIVACY pp -> 0
FRAGILE PRIVACY pp ->> 0
Increasing Level of Privacy Protection against malicious attacks based on unlimited computational resources and time.

Fig. 2. Graphical representation of the Computational View of Information Privacy

4 COMPUTATIONAL PRIVACY CLASSIFICATIONS APPLIED TO PRIVACY ENHANCING TECHNOLOGIES

This section classifies some of the more well known privacy enhancing technologies. This includes the recent IBM proposals, the privacy/identity protector, the privacy shield, P3P based solutions, anonymizers, mixers, and a number of other forms of technical based privacy protection techniques.

4.1 Ideal Privacy PETS

- Anonymity Based Technologies: through the use of genuine, untraceable anonymity these technologies deny an entity's identity, and therefore protect their privacy. Some examples include: Anonymous Remailers such as Type II remailers, that provide anonymous email communications, Mixmaster and Mixminion systems that also allow anonymous communication [Sassaman and Moller, 2005]. Anonymizer [Anonymizer, 2005] is a web proxy that can hide your IP address and some other personal information.
- Authorization rather than Authentication: technologies that require authorization rather than authentication are candidates for Ideal Privacy. With Authorization an entity only proves they are authorized to use a service rather than prove who they are by revealing their identity.
- Digicash or Anonymous Transactions and Credentials: Chaum's [1989] Digicash was one proposed method to allow Ideal Privacy in financial transactions. Unfortunately the technology never gained wide acceptance and therefore is not used globally. Where possible cash transactions are preferable or other methods of payment that do not reveal an entities Identity or personal information. Often this is impractical for electronic commerce and communication. Some working examples still in their development stages include idemix by IBM [IBM, 2002] and Credentica by Stefan Brands [Credentica, 2004].
- Encryption Tools: encrypting stored information and transmitted information increases privacy protection. On its own, encryption is not a complete solution. However, through the use of strong, computationally secure encryption algorithms and techniques a level of Ideal Privacy is obtainable.

4.2 Computational Privacy PETs

- Hippocratic Databases: this form of PET provides Computational Privacy as long as the system controls and security are maintained and monitored. The privacy of the database and its contents are only as secure as the access controls protecting it. Likewise, the privacy of the personal information contained in the databases is of a computational privacy protection level.
- Identity Protector & Privacy Shield: these two similar technologies are based on computationally secure design and implementation methods and techniques. However, they are unable to provide

total and uncompromisable privacy protection of the personal data they protect, nor the identity of the system entities providing the personal data. Rather, they provide computational secure protection of the personal data to maintain the privacy.

- Pseudo-anonymous Schemes: these approaches to privacy try to obtain a balance between the interest of privacy and accountability. This means that given a particular set of conditions the privacy of system entities can be compromised. This may include entities conducting illegal activities through a pseudo-anonymous identity, entities in life or death situations such as administration of medial treatment based on previous medical history, or revealing one's true identity to refute identity misrepresentation allegations, to collect payment or receive services.

4.3 Fragile Privacy PETs

- P3P and other Policy Based systems (EPAL): the objective of these privacy enhancing technologies is one of awareness rather than enforcement and protection. While an entity who is an information collector may state their privacy policy, through the use of P3P or EPAL, it does not mean that it will be enforced or adhered to.
- Fixed and reusable password systems: systems based on these authentication and authorization schemes provide only Fragile Privacy protection. Fixed and reusable password shave been proven to provide the weakest level of security.
- Authentication Schemes: authentication is the process of validating an entities identity. This simple process means the identity of an entity is revealed and therefore their privacy is compromised. Therefore system really on identity based authentication schemes provide on Fragile Privacy protection levels.
- Automated Privacy Audits: these technologies only provide assistance and knowledge on data flow and practises. They do not provide enforcement and actual privacy protection. Unless action is carried out on the privacy shortcomings found through the auditing process, the system continues to provide Fragile Privacy.
- Spam Filtering, Proxies, Firewalls and Cookie Cutters: These Internet based browsing privacy technologies are not guaranteed to provide complete protection. Rather they reduce the possibility of privacy invasive incidents. It is possible that some of an entity's personal information can still be leaked to other unauthorized entities.

5 CONCLUSION

The computational view of privacy is concerned with the level of privacy protection provided by models, tools, and protocols when they are subject to malicious attack from entities with unlimited time and computational resources. Within the computational view three clearly defined levels of protection have been defined that can be applied to Privacy Enhancing Technologies to classify their level of privacy protection. The highest level of protection is provided by Ideal Privacy, which represents uncompromising levels of privacy. The middle level of protection is termed Computational Privacy which reflects the very large amount of computational resources and time required to circumvent its protection level. The weakest level of privacy protection is termed Fragile Privacy. Fragile privacy represents the nature of weak protection that given a reasonable amount of time and resources can be compromised. A fair number of current Privacy Enhancing Technologies in operation today are unfortunately still categorized as Fragile Privacy for their levels of privacy protection.

REFERENCES

1. Agrawal, R., Kiernan, J., Srikant, R., and Xu, Y. (2002): Hippocratic Databases. Proceedings of the 28th VLDB Conference, Hong Kong, China.

2. Agrawal, R., Kiernan, J., Srikant, R., and Xu, Y. (2003): 'Implementing P3P Using Database Technology'. 19th International Conference on Data Engineering, Bangalore, India.

3. Anonymizer.com (2005): Online privacy services. http://www.anonymizer.com/.

4. Backes, M., Pfitzmann, B., and Schunter, M. (2003): 'A Toolkit for Managing Enterprise Privacy Policies'. ESORICS 2003, LNCS 2808, pages 162-180, October.

5.Backes, M., Bagga, W., Karjoth, G., and Schunter, M. (2004): 'Efficient Comparison of Enterprise Privacy Policies'. SAC'04, Nicosia, Cyprus, March.

6.Borking, J.J. (2001): Laws, PETs, and Other technologies for Privacy Protection. http://www.dutchdpa.nl/asp/CBPPrint.asp. Journal of Information, Law, and Technology.

7.Chaum, D. (1981): ‘Untraceable Electronic Mail, Return Ad-dresses, and Digital Pseudonyms’. Communications of the ACM, 24,2, Feb.

8. Chaum, D. (1985a): ‘Showing Credentials Without Identification. Signature Transfers Between Unconditionally Unlikable Pseudonyms’. Advances in Cryptology - EUROCRYPT '85, Proceedings; LNCS 219; Springer Verlag, pages 241-244.

9. Chaum, D. (1985b): ‘Security without Identification: Card Computers to make Big Brother Obsolete’. Communications of the ACM, 28, 10, Oct.

10.Chaum, D. and Evertse, J.H. (1986): ‘A Secure and Privacy-Protecting Protocol For Transmitting Personal Information Between Organizations’. Crypto '86, LNCS 263, Springer-Verlag, Berlin, p118-167.

11.Chaum, D. (1989): ‘Privacy Protected Payments: Unconditional Payer and/or Payee Untraceabiliy’. Smart Card 2000: 69-93.

12.Chaum, D. (1992): ‘Achieving Electronic Privacy’. Scientific American, August 1992, p. 96-101.

13.Clarke, R. (1999): “Introduction to Dataveillance and Information Privacy, and Definitions and Terms.”. http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

14.Clarke, R. (2001): Introducing PITs and PETs: Technologies Affecting Privacy. http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPets.html.

15.Common Criteria (2004): Common Criteria for Information Technology Evaluation. January, 2004, http:// www.commoncriteria.org.

16.Cranor, L.F. (2000): The Role of Privacy Enhancing Technologies. AT&T Labs Research, Secure Systems Research. http://www.research.att.com/~lorrie/

17.Credentica (2004) – Enterprise Solutions for Identity and Access Management: Credentica. http://www.credentica.com/.

18.Damiani, E., De Apitani di Vimercati, S., Jajodia, S., Paraboschi, S., and Smarati, P. (2003): Balancing Confidentiality and Efficiency in Untrusted Relational DBMSs. Proceedings of the 10th ACM Conference on Computers and Communication Security. Washington, DC, USA, October 27-31, pp93-102.

19.EPIC (2003): Privacy and Human Rights 2003. http://pi.gn.apc.org/survey/phr2003/forward.htm, (2003).

20.Federal Trade Commission (FTC) (2003): Fair Information Practise Principles. Federal Trade Commission Online Privacy, http://www.ftc.gov/reports/privacy3/fairinfo.htm

21.Goldberg, I. (2002): Privacy-enhancing technologies for the Internet, II: Five Years Later. Workshop on Privacy Enhancing Technologies. San Francisco, CA, USA, 14 - 15 April.

22.Hes, R. and Borking, J. (2000): Privacy-Enhancing Technologies: The path to anonymity. Registratiekamer, The Hague, August.

23.IBM (2003): Enterprise Privacy Authorization Language (EPAL) Specification. http://www.zurich.ibm.com/security/enterprise-privacy/epal/.

24.IBM Research – Security Division (2002): Idemix: pseudonymity for e-transactions. http://www.zurich.ibm.com/security/idemix/.

25.Karjoth, G. and Schunter, M. (2002): ‘A Privacy Model Enterprises’. 15th IEEE Computer Security Foundations Workshop, June.

26.Karjoth, G., Schunter, M., and Waidner, M. (2002): ‘Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data’. 2nd Workshop on Privacy Enhancing Technologies, LNCS. Springer Verlag.

27.Langeinrich, M. (2000): Personal Privacy in Pervasive Computing. Research Group for Distributed Systems. Swiss Federal Institute of Technology, Zurich.

28.Milken Institute (2006): The Milken Institute Privacy Notice, 2006. http://www.milkeninstitute.org/privacy.taf.

29.Nykamp, M. and McEachern, C. (2001): Customer Relationship Report: Privacy, CRM and ROI. DM Review, February.

30.Oberholzer, H.J.G. and Olivier, M.S. (2005): Privacy Contracts as an Extension of Privacy Policies. International Workshop on Privacy Data Management 2005, April 9, Tokyo, Japan.

31.Organization for Economic Co-operation and Development (1980): OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org.

32.Sassaman, L. and Moller, U. (2005): Mixmaster. http://sourceforge.net/projects/mixmaster/.

33.Skinner, G. and Miller, M. (2006): Managing Privacy, Trust, Security, and Context Relationships using Weighted Graph Representations. WSEAS Transactions on Information Science and Applications, February.

34.Skinner, G. and Chang, E. (2004a): Hippocratic Policies in Computer Based Collaborations. PHCRC 2004, Newcastle Australia.

35.Skinner, G. and Chang, E. (2004b): Shield Privacy Hippocratic Security Method for Virtual Community. IECON2004, The 30th Annual Conference of the IEEE Industrial Electronics Society, Nov 2-6, Korea.

36.W3C (2002): The platform for privacy preferences 1.0 (P3P1.0) specification, Jan., 2002. W3C Proposed Recommendation, http://www.w3.org/TR/P3P.

37. Weinstein, L. and Neumann, P.G. (2003): Privacy Issues and Privacy Enhancing Technologies. A Report of Research on Privacy for Electronic Government, 15 February.