Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp152-157)

Graph Representation of Access Controls for Managing Privacy, Trust and Security Requirements

GEOFF SKINNER & MIRKA MILLER
School of ITMS
University of Ballarat
P.O. Box 663, Ballarat, Vic 3353
AUSTRALIA
http://www.ballarat.edu.au

Abstract: - Determining who has access to personal data is an ongoing problem facing information system entities. The establishment of trust and its representation for known and unknown entities within the system further complicates access control rights allocation. One unique solution is through the application of graph representation to aid in the identification and management of privacy, trust and security requirements. Graphs provide a much better mental map than would textual information. In this paper we use graphs to represent informational relations concerning trust levels between entities for privacy and security requirements.

Key-Words: - Information Privacy, Information Security, Trust, Graph Representation, and Access Controls.

1 Introduction & Related Work

The barrage of requests to information system users for their personal data is an ongoing issue that needs to be managed. Any decision by an entity to divulge personal data within a virtual computing environment requires a very complex thought and rationalization process. As in the real world setting, the decision to reveal personal data to another entity is influenced by many factors. It has been shown that the most prominent elements of the decision process are security, trust, privacy, and context [1]. The existence of relationships between trust, privacy, security and context does not allow for adequate consideration of each of them in isolation.

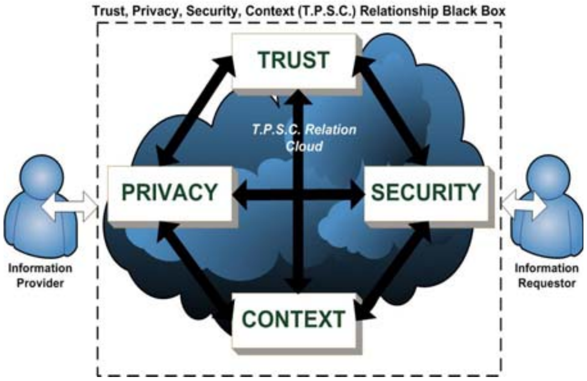

Fig. 1: The Trust, Privacy, Security and Context Relationship.

It is believed that in order to alter the value of one of the elements a trade off is needed that effects another. For example, in order to increase the trust in an entity, the privacy of that entity would be decreased [2]. That is, in order to trust someone more we need to learn more about them. The more we know about someone, the less privacy they have. Likewise, if we wish to increase security, then it comes at the cost of decreasing entity privacy. For example, many current authentication and authorization methods require identification of an entity. The identification process reduces the level of privacy of the entity using a system.

In most cases each of the above mentioned elements are also affected by the context of the situation and setting. Entities may be willing to sacrifice their personal privacy for increased trust in another entity based on various situational contexts. An example of such a context might be the financial reward offered for disclosure of personal information. Most often, the greater the reward or benefit to the entity, the more likely they are to reveal their personal data [3].

Figure 1 represents the inter-dependant relationships and factors that influence the reasoning around granting or denying a personal data request. On the left hand side of the figure, we have the Information Provider (IP) and on the right the Information Requestor (IR). The middle represents the Trust, Privacy, Security, and Context (T.P.S.C.) Relation Cloud. The IP makes a decision to reveal personal data to the IR after a ‘comfortable’ balance has been mentally reached by the IP to do so. This is obtained by working through and evaluating the possible outcomes generated within the T.P.S.C. Relationship Cloud.

Each of these elements in their own right represents a very large field of study. This paper focuses on the technological and informational components of each element. Consideration of every single aspect is beyond the scope of this paper. Rather, our objective is to produce solutions for managing privacy, trust and security requirements. This is achieved by providing an entity with the right tools and data for making critical information privacy decisions. The data provided should be presented in a legible and easy to process way as it incorporates the inter-relationships between privacy, trust, security and context.

The preservation and protection of information privacy is a pervasive issue, and one that is addressed in this paper. Information privacy is defined as '… the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.'[4]. Much work has already been done in the area of information privacy protection with variety of solutions available or proposed. The proposed solutions range from technological approaches, commonly referred to as Privacy Enhancing Technologies (PET's) [5], through to operating guidelines governed by privacy policies and regulations [6, 7]. Additionally, there are many hybrid solutions combing both aspects, as well as including the principle of Privacy by Design [8].

Some of the solutions are particularly relevant to our past and current work. This has included the work on Hippocratic Database's [9]. The idea of including entity privacy preferences with data elements is one that should be considered for all new systems. Work on Shield Privacy [10] includes the Hippocratic design considerations in addition to a number of other unique privacy enhancements. The Identity Protector, proposed in [11], is useful in its approach to separate system privacy domains and the use of pseudo-identities.

An important issue that has not been adequately addressed is how, when and to what level these protections should be applied. In the end the data owner still needs to be able to make an informed decision on what level of protection is afforded to their personal data. Personal data requests come from different entities and in different contexts. So no single generic approach is suitable for all situations. Therefore, the personal data owners need a clear representation of each personal data request and take action based on this information.

The information provided should be a representation that relays information about the privacy, security, trust and context factors. A proven method of representation and simplification is through the use of diagrams [12]. For the situation where complex relations need to be modelled, the use of graph diagrams gives the best solution. However, there has been limited application of graphs for use in representing privacy, security, trust and context relationships as they relate to information privacy and data security. The work to date has focussed primarily on access controls and other security specific components [13, 14]. We propose the use of weighted graphs to represent privacy, trust, security and context relationships within information systems. The resulting graphs are to be used by entities to make informed decisions on whether to provide their personal data to system entities requests.

The remainder of the paper is structured in the following manner. Section 2 provides additional information on our previous background work in the area and develops the problem further. A solution and framework for a proposed application for implementation is discussed in Section 3. Section 4 contains the conclusion and discussion of future work.

2 Representing the Trust, Privacy, Security, and Context Relationship.

Research into the inter-relationships between trust, privacy, security, and context in a virtual setting has been gaining momentum of late. As information systems evolve and become 'smarter', so do the systems emulation of real world situations. An entity's thoughts and decision making processes on determining their trust in another entity is a complex procedure, influenced by many factors. The issues addressed in this paper are the increasingly common problem of an entity's decision to divulge their personal information to other entities, either known or unknown. In this setting entities represent individuals, groups, or organizations. An individual represents a unique identity such as a system user. A group is an informal membership of entities, and an organization is a formal membership of entities [15].

The problem of managing privacy and trust for personal information has been addressed previously by the first author of this paper. The proposed framework and solution from the previous work provides the foundation that is greatly improved upon in this paper [16]. The aim of this paper is the development of a more complete solution, simpler for user interpretation and use. It is a proposal that utilizes graphs for the representation of the inter-relationship between trust, privacy, security and context.

From a conceptual level, the initial motivation was provided by the real world concept of 'six degrees of separation' [17], where, it is believed that '… everyone on Earth is separated from anyone else by no more than six degrees of separation, or six friends of friends of friends.' [18]. Related to this concept is the well known cryptographic term 'a web of trust', which is used to build PGP key chains [19]. These ideas provided the basis for system emulation. For completeness, a brief summary of the key components of the proposed initial solution has been included in this paper.

An example which is very relevant for the current work is that of a collaborative environment or virtual community. The entities, that are members of the collaboration, are often separated by less than six degrees. In this case the degrees of separation (DoS) encountered in the collaboration are proportional to the size of the collaboration or membership (number of entities) {M}, location or distance between collaboration member entities {L}, and the duration of collaboration existence {T}. That is:

$$DoS \text{ -> } 6\ AS\ (\{M\}\ \&/||\ [L\}\ \&/||\ [T\} \text{ -> } \infty) \qquad (1)$$

For a large collaboration, with many organizations, groups, and individual entities, it is practical for an entity to classify other entities into realms. The realms are based on the four elements of trust, privacy, security and context. Generally, the further the degree of separation, the higher the realm an entity is placed in. This equates to the higher the realm an entity is in, the less trusted they are by a personal data owner. The realm positioning in turn determines the security mechanisms, such as access control restrictions, placed on the personal data.

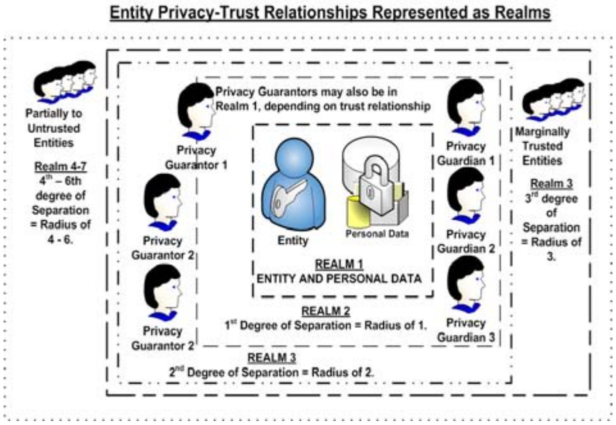
Entity Privacy-Trust Relationships Represented as Realms
Partially to Untrusted Entities
Realm 4-7
4th – 6th degree of Separation = Radius of 4 - 6.
Privacy Guarantors may also be in Realm 1, depending on trust relationship
Privacy Guarantor 1
Privacy Guarantor 2
Privacy Guarantor 2
Entity
Personal Data
REALM 1
ENTITY AND PERSONAL DATA
REALM 2
1st Degree of Separation = Radius of 1.
REALM 3
2nd Degree of Separation = Radius of 2.
Privacy Guardian 1
Privacy Guardian 2
Privacy Guardian 3
Marginally Trusted Entities
Realm 3
3rd degree of Separation = Radius of 3.

Fig. 2: Representation of an Entity's Trust, Privacy, Security and Context Relationships to Other Entities.

To support the real time operation of the network of trust relationships and the processing of personal data access requests special roles are available. The first is the role of Privacy Guardian (PGa). A privacy guardian is an entity that is unconditionally or implicitly trusted by the personal data owner. They exist in Realm 2, which normally equates to 1 degree of separation. Due to the possible misunderstanding of terms once graph principles are introduced, a degree of separation between two entities will henceforth be referred to as the distance. For individual entities, the translation is very simple in that there is a one-to-one mapping between degree of separation and the length of shortest path. For the overall network, a degree of separation D equates to the so-called diameter (longest distance between any two entities in the network) D. A Privacy Guardian always is at distance 1 from the personal data owner. Fig 2 shows this representation along with a number of other properties.

The second of the two major roles is that of a Privacy Guarantor (PGu). A Privacy Guarantor acts as a supporter of an entity. That is, in terms of real world relations a Privacy Guardian is a 'power of attorney', while a Privacy Guardian is a 'referee', for an entity. Privacy Guarantors may appear in any of the realms, but usually occur in either Realm 2 or 3. This is because for an entity to be a Privacy Guarantor, there must be a significant level of trust between the entities.

For example, when an entity (the information requestor) requests another entities personal data (the information provider), it is useful for the information owner to consult other entities that know the information requestor. Hence, Privacy Guarantors should be entities that already have high levels of virtual systems trust. Examples may include system administrators, organizational managers or human resource managers, or other entities that readily reveal their true identity and have a good operational history.

In the same example it is preferred that the selected trusted path leading from the Information Provider to the Information Requestor also goes through an Information Provider's Privacy Guardian. As the Privacy Guardians represent the most trusted related entities of the information provider, they also have full access to the personal data being requested. The presence of such relationships increases the overall trust level of the path from provider to requestor. Therefore, the overall objective is to firstly find the shortest path. This is the path with the least number of entities (friends of friends of friends), between provider and requestor. Secondly, find the shortest path that has the highest trust level. The path with the highest trust level would be one made up of the maximum number of Privacy Guardians and Privacy Guarantors.

The problem is how do we find and represent the relationships and optimal paths between entities. The proposed solution that will be detailed in the next section is the use of graphs for privacy-trust-security-context representations. The solution makes use of weighted graphs to represent the different trust, privacy, security and contextual relationships between entities. The entity is able to define parameters such as the diameter of the relationship graph, the maximum threshold weighting of the paths, and the preferred number of Privacy Guardian and Privacy Guarantor vertices the graph includes. The limitations placed on the parameters are used to find the optimal paths between provider and requestor. The paths are used by the provider to determine whether their personal data should be divulged to the requestor.

3 Graph Representations for Privacy Management Requirements

The 'PGP Web of Trust' [19] has proved to be a useful way of building trust in a virtual environment. Our proposal follows a similar trust infrastructure by implementing a trust level classification system. It assigns to system entity roles certain default levels of trust. The entities within a role may be known or unknown. The adaptation is developed further to overlay upon the various vertices within a personal data relationship graph. So like the web of trust there are four default levels of trust. However, in our context they relate to an entity's personal data and the trust they have in other entities assigned to specific roles accessing their data. The levels are:

- Implicit (Ultimate): Owner of the data.
- Full (Complete): Privacy Guardian.
- Marginal: Privacy Guarantor.
- Untrusted: 2-6 radius of separation.

So for example, once an entity selects another entity as their Privacy Guardian, the Privacy Guardian role by default has full access to the personal data.

Privacy Classification	**Description of Classification**
Very Confidential	Most private personal data not to be shared with any other entities.
Confidential	Personal data that can only be shared with completed trusted entities (PGa)
Very Sensitive	Personal data that can only be shared with marginally trusted entities (PGa)
Sensitive	Personal data that can be shared with entities within the radius threshold.
General	Personal data that can be shared with all entities within the system.

Table 1: Personal data privacy classification.

In order to increase the level of privacy further another useful approach that has been implemented in various ways, in a number of systems, is the use of data classification. In our case the personal data is classified, by the data owner, as it is collected and stored, according to its personal or 'sensitive' nature. Our framework is based on the Bell-LaPadula Model [20], with a number of small modifications. Personal data is classified as either: Very Confidential, Confidential, Very Sensitive, Sensitive, or General. A description of each classification is in Table 1. The classification is used by an entity to determine the security protection techniques applied to the data elements and likewise who has access to their personal data.

For clearly defined roles such as Privacy Guardians and Privacy Guarantors, they are by default granted access to all data classified up to a certain level. For each and every data element the owner of the data determines the sensitivity rating. This is one of the classifications listed in Table 1. Following 'privacy by design' system principles, the sensitivity levels are stored with the individual data elements. This is in addition to storing the Hippocratic privacy preferences components [9].

By using a two layered trust categorization structure we are providing the fine grained privacy and security management required for current and future information systems. So not only are roles within the system assigned trust classifications but also the individual personal data elements. For example, a Privacy Guardian role has 'Full' level trust. Depending on entity configuration this may mean that Privacy Guardians can access all personal data with a Privacy Classification of Confidential or less. Similarly, an unknown entity in the system may be assigned to a role with an Untrusted classification. The Untrusted classified roles may be assigned a General Privacy Classification. So only personal data that can be shared with all entities is accessible to the Untrusted classified roles, and hence unknown entities.

The methods we have proposed to this point for managing privacy, trust, security and context are unique in their application and enhancement of established methods. Additionally the incorporation of Privacy Guardians and Guarantors builds upon web of trust principles. The next component that is required is the integration of a weighting and representation system within the framework. The need for representing relationships with different trust levels, that in turn affect privacy and security parameters, is solved through the use of weighted graphs. The weighted graphs, as will be shown, can be dynamically generated. The real time generation addresses the fourth element of changing contexts and their relationship to privacy, trust and security.

Weighting an edge between two vertices provides a simple but effective means of representing trust relationships between two entities. The entities are represented by the respective vertices on either end of the edge. By default, a weighting classification is also assigned to represent virtual trust that correlates to the classifications used for system roles. The main difference is that the weightings are adjustable by each entity based upon their perceived trust, privacy, security and context relationships. The default weightings are as follows:

- 1 : Privacy Guardians of the entity owning the personal data and those roles and entities with full or complete trust.
- 2 : Privacy Guarantors and those roles and entities with marginal trust.
- 3 -> x : Other roles and entities that are untrusted to varying degrees. This scale is an arbitrary measure determined by the entity using the framework. Generallym even for large scale collaborations, a range of 3 to 5 is sufficient.

Once the weightings have been placed on all edges, they can be summed along the various paths leading from an Information Provider (IP) to an Information Requestor (IR). The summation values are used in determining the minimum weighted value for all of the paths. The path with the smallest weighting value is therefore the most 'trusted' path available from IP to IR. Finding the minimum weighted path is only one of a number of threshold parameters that are set by the IP entity. The IP entity is able to set the parameters based on their personal preferences.

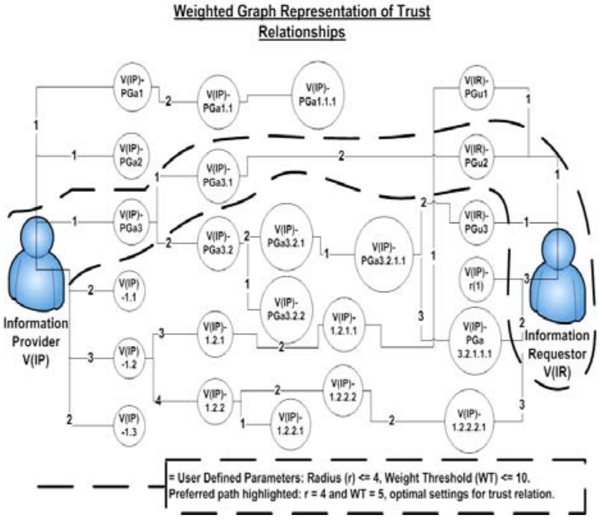

Fig. 3: A weighted graph representation of trust, privacy, security and context relationships from IP to IR.

The most important threshold parameter that can be set by an entity is the diameter of the graph, that is, the maximum number of vertices (entities) the path traverses from any IP to any IR. The optimal or most trusted path is the one with the smallest length. In the case that a number of paths all have the smallest length then the path with the minimum weight is deemed to be the optimal one. If there are again a number of paths that are not only the smallest length but also all have the minimum weight then the path with the maximum number of Privacy Guardian vertices is the optimal one. For general operational precedence within the framework, and to allow automation in the resulting application, the above parameters translate to the following system rules:

1) Find the shortest path, that is, the path with the least number of vertices and edges.
2) Find a path with the minimum weighting, that is, the sum of all edge weights for the path should be the minimum.
3) Find the path with the maximum number of Privacy Guardians, that is, select the path with the maximum number of Privacy Guardian vertices.

Each of the above mentioned parameters can have threshold values set by the personal data owner, which is the information provider in the framework. That is, an entity is able to specify the diameter of a graph, the maximum weight of a path, and also the minimum number of Privacy Guardians vertices required in a `good' path. By setting the threshold values, the privacy and security requirements are tailored to the personal preferences of each entity using the system, additionally, reducing the amount of redundant information displayed in the resulting graphical representations. Only those paths that meet the desired criteria are displayed to the IP. For example, in Figure 3, only the completed path enclosed in the dashed line would be displayed to the IP. This is because the highlighted path has length that is less than or equal to 4 and a weighted summation of the edges of the path less than or equal to 10.

A collaborative environment provides an ideal testing and working environment for the proposed framework and application. Membership to a collaborative environment normally involves some degree of authentication and authorization for new and ongoing entities. Further, the principle of six degrees of separation holds true in this virtual world. Establishing virtual trust networks is therefore very easy. As new entities are added to the collaboration, they initially select their Privacy Guardians and Guarantors which can be modified at anytime once they are a system member. The entity and their preferences are integrated into the system and new trust paths and relationships are graphed and generated as required for personal data requests.

4 Conclusion and Future Work

Managing Privacy, Trust and Security in a given situation is a complex process. When confronted by the decision to share personal information in varying contexts, such as those presented in Information Systems and Virtual Environments, the management requirements of privacy, trust and security become an unnecessary burden. This paper has proposed a solution to alleviate this burden by providing a framework and application for privacy, trust, security and context relationship modelling.

Through the use of weighted graphs, to represent the relationships between themselves and other entities in the system, an entity is better equipped to make a personal data sharing decision. The paths between an entity and the entity requesting their information goes through vertices of other entities trusted to varying degrees. The graphs are dynamically generated for an Information Provider on receiving a request for their personal information and are therefore context specific. Based on the information provided and entity threshold settings, appropriate access control mechanism can be applied to protect the data.

Discussion of the development of a prototype system to implement the framework has not been covered for space reasons. The name of the system is called TRUTH (Trust Relationships Using Tree Hierarchies). Within the system an entity is able to call a TRUCE (Trust Representation Using Closest Entities) to obtain a dynamic graph representation.

References:

[1] Robinson P., Vogt H., Wagealla W., Privacy, Security, and Trust in the Context of Pervasive Computing. *SPPC: Workshop on Security and Privacy in Pervasive Computing*, 2004, Vienna.

[2] Seigneur J. & Jensen C.D., Trading Privacy for Trust. *PET2002*, 2002, San Francisco, USA.

[3] Seamons K.E. *et al*., Protecting Privacy During Online Trust Negotiation. *2nd International Conference on Trust Management*, 2004, St Anne's College, Oxford, UK.

[4] Clarke R., Introduction to Dataveillance and Information Privacy, and Definition of Terms. *Australian National University, Australia. http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html*.

[5] Goldberg I., Privacy-enhancing technologies for the Internet, II: Five years later. *PET2002*, 2002, San Francisco, USA.

[6] Carminati B. and Ferrari E., Trusted Privacy Manager: A System for enforcing privacy on outsourced data. *PDM2005*, 2005, Tokyo, Japan.

[7] Ildemaro A., Privacy Mechanisms supporting the building of trust in e-commerce. *PDM2005*, 2005, Tokyo, Japan.

[8] He Q., Privacy Enforcement with an Extended Role-Based Access Control Model. *NCSU Technical Report TR-2003-09*, 2003, North Carolina, USA.

[9] Agrawal R. *et al*., Hippocratic Databases. *28th International Conerence on Very Large Databases (VLDB)*, 2002, Hong Kong.

[10] Skinner G. and Chang E, Shield Privacy Hippocratic Security Method for Virtual Community. *IECON2004 The 30th Annual Conference of the IEEE Industrial Electronics Society,* 2004, South Korea.

[11] Borking J.J. *et al*., Handbook of Privacy and Privacy-Enhancing Technologies. *College Bescherming Persoonsgegevens,* Den Haag, The Netherlands. (NRC 47403), 2003.

[12] Diezmann C.M. and English L.D., Promoting the use of diagrams as tools for thinking. *2001 National Council of Teachers of Mathematics Yearbook: The Role of Representation in School Mathematics*, 2001, QUT, Australia.

[13] Sandhu R., A Perspective on Graphs and Access Control Models. *2nd International Conference on Graph Transformations,* 2004.

[14] Kock M. *et al*., A Graph Based Formalism for RBAC. *ACM Transactions on Information and System Security (TISSEC),* Volume 5, Issue 3, 2002.

[15] Skinner G. & Song H., A New Conceptual Framework within Information Privacy: Meta Privacy. *CIS2005,* 2005, Xian, China.

[16] Skinner G., Dynamic User Reconfigurable Privacy and Trust Settings for Collaborative Industrial Environments. *INDIN05,* 2005, Perth, Australia.

[17] Knight W., Email experiment confirms six degrees of separation. *New Scientist*, 2003.

[18] Shullman Q\P., From Muhammad Ali to Grandma Rose. *Discover*, December 1998.

[19] PGPi, How PGP Works. *http://www.pgpi.org/doc/pgpintro/.*

[20] Bell D.E. and LaPadula L.J., Secure Computer Systems: Mathematical Foundations and Model. *The Mitre Corporation,* 1976.