Privacy Enforcement with an Extended Role-Based Access Control Model

Qingfeng He

Department of Computer Science
North Carolina State University
Raleigh, NC 27695-8207, USA

qhe2@unity.ncsu.edu

February 28, 2003

Abstract

Privacy enforcement has been one of the most important challenges in IT area. Current privacy practices within companies and organizations, e.g. enabling a P3P compliant policy, incorporating a privacy seal program, etc., cannot truly protect consumer privacy. Privacy protection can only be achieved by enforcing privacy policies within an organization's online and offline data processing systems. Traditional security models are more or less inappropriate for enforcing basic privacy requirements, such as purpose binding. This paper proposes an extended role-based access control (RBAC) model, called Privacy-Aware Role-Based Access Control (PARBAC) model, for enforcing privacy policies within an organization. The PARBAC model combines RBAC, Domain-Type Enforcement, and privacy protection by modeling business purposes and data policies. Consented consumer privacy preferences are recorded as data policies, which govern how to use actual consumer data. One of the key elements in a privacy policy is purpose. The actual purpose of a business operation to consumer data must be consistent with the purpose consented by the consumer. This is the so-called purpose binding privacy requirement. This paper focuses on enforcing this requirement. Privacy enforcement mechanism with the PARBAC model is then discussed and a privacy scenario is illustrated to describe its application.

Keywords: Privacy Enforcement, Privacy Policy, Purpose, Role-Based Access Control, Domain-Type Enforcement

1 Introduction

Privacy is often considered as a societal, moral or legal concept. To be simple, privacy is "the right to be alone" [WB 1890]. A more specific and common definition of privacy is, "Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" [Wes67].

As Internet and e-commerce has prospered recently, privacy has been one of the most important issues in IT (Information Technology) and has received increasing attention from consumers[1], stakeholders, and legislators. Legislative acts, e.g. Health Insurance Portability and Accountability Act (HIPAA) for healthcare [HIP96] and Gramm Leach Bliley Act (GLBA) for financial institutions [GLB01], require these industries to protect consumer privacy. Although companies and organizations have taken various approaches to protect customer privacy, such as publishing a privacy policy on their websites, enabling a P3P[2] compliant privacy policy, incorporating a privacy seal program (e.g. Truste, BBBOnline, CPAWebTrust)[3], etc., these approaches cannot truly safeguard consumers because they do not address how consumer personal data is actually handled after it is collected [AE01, AEA01, GHS00]. Companies and organizations' actual practices might intentionally or unintentionally violate the privacy policies they published on their websites.

The OECD[4] guidelines for data protection [OEC80] define eight privacy principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability principle. These principles intend to protect personal data privacy while pursuing free information flow between different organizations and different countries. A more general privacy protection guideline is FTC[5] Fair Information Practice (FIP) Principles [FIP98]: notice/awareness, choice/consent, security/integrity, access/participation, and enforcement/redress. These principles are the major privacy requirements that organizations must comply with. For example, when websites collect information from customers, they need to inform customers for what purpose the data is collected, who the data recipient is, how long the data will be kept, and how the data will be used, etc. (notice/awareness principle in FIP). They should also provide opt-in/opt-out choices for customers or obtain customer consent on how to use the collected data (choice/consent principle). The actual data operations of companies and organizations shall be consistent with user consented privacy policies (enforcement/redress principle).

Privacy protection can only be achieved by enforcing privacy policies within an organization's online and offline data processing systems. Privacy and security policies

[1] In this paper, consumers, customers, data subjects, and data owners are used interchangeably to represent the group of people whose personal data is collected by companies and organizations.

[2] The Platform for Privacy Preferences Project (P3P), http://www.w3.org/p3p/.

[3] http://www.truste.com/, http://www.bbbonline.com/, http://www.cpawebtrust.org/.

[4] Organization for Economic Cooperation and Development (OECD): http://www.oecd.org/.

[5] Federal Trade Commission: http://www.ftc.gov/.

overlap in that both policies intend to protect data confidentiality and integrity. It is important to combine security and privacy protection together. However, traditional security models, such as Mandatory Access Control (MAC) [Den76, San93] and Discretionary Access Control (DAC) [Lam74, SS94], are not designed for enforcing privacy policies. They are solely designed to provide security from a system's perspective. Security policies only cover one FIP principle: security/integrity. The other four principles are not addressed, not even mentioned in any traditional security policy. Although three principles: notice/awareness, choice/consent, and access/participation may be modeled in security policies and implemented in system design, there is no evidence in the literature that addresses privacy policies enforcement using traditional security models.

Fischer-Hübner has published a summary of privacy evaluation of well-known security models [Fis01]. She contends that traditional security models (i.e. Bell LaPadula Model, Lattice Model, Biba model, Clark Wilson Model, Chinese Wall Model, Role-Based Access Control (RBAC) Model, Workflow Authorization Model (WAM) Model, Object-Oriented Security Models, etc.) are more or less not appropriate for enforcing basic privacy requirements, e.g. purpose binding (i.e. data collected for one purpose should not used for another purpose without user consent), and principle of necessity (i.e. the collection and processing of data shall only be allowed if it is necessary for completing appropriate tasks). Powers et al. [PAS02] suggested enforcing privacy throughout an enterprise by extending access control.

Role-based Access Control (RBAC) [SCF96, FSG01] has been shown to meet a large variety of commercial security requirements, e.g. separation of duties, principle of least privileges, data abstraction, etc., and has received considerable attention as a promising alternative to MAC and DAC models. The characteristic of *role* in RBAC has some relation to *purpose*, which is a key element in privacy policies (i.e. for what purpose the data is collected). In RBAC, role is defined as "a job function within the organization that describes the authority and responsibility conferred on a user assigned to the role" [SCF96]. When a role is derived from business tasks, a certain responsibility is assigned and some purposes of the role are embodied implicitly. Thus, role and purpose have a close relation to each other [FBP01]. It is possible to derive this relationship and use it as the basis for enforcing purpose binding, one of the key privacy requirements. This is the objective of this paper. In addition, RBAC is a suitable candidate to implement context-based access control, which is important for privacy protection. According to HIPAA security regulation [HIP96], at Section 142.308(c)(1)(i)(B), requires the use of either (1) user-based access control, (2) role-based access control, or (3) context-based access control. Context-based access control not only takes into account the person attempting to access the data and the type of data being accessed, but also the context of the transaction in which the access attempt is made. In a privacy-aware environment, this context may be the data usage policy consented by a particular customer, e.g. collect children's data under 13 only if parental consent is obtained. By combining RBAC and other mechanisms such as Domain-Type Enforcement (DTE), RBAC models can be extended to provide context-based access control [Cha01].

This paper proposes an extended RBAC model, called Privacy-Aware RBAC (PARBAC) model, for enforcing privacy policies within an organization. The PARBAC model is based on Domain-Type Enforcement (DTE) and models business purposes and data usage policies. A new element *purpose* is introduced in the PARBAC model, which is not modeled in traditional RBAC models. When a data user requests to access certain customer data, not only roles and permissions of the data user are considered, but also the business purpose of the operation and the privacy policy that pertains to that particular customer are checked. Validation scenario demonstrated that the PARBAC model could be used to enforce purpose binding and policy-driven data usage control.

This paper is organized as follows. Sections 2 provides a summary of related work. Section 3 describes entities and entity relationships based on the architecture of the PARBAC model. In Section 4, privacy enforcement using the PARBAC model is discussed. Then in Section 5, a privacy scenario is described and the application of the PARBAC model on this scenario is illustrated. Finally, a summary of the paper is given in Section 6. The limitations of the PARBAC model and future work are also discussed in this section.

2 Related Work

The underlying bases of this paper are three research areas: Role-Based Access Control (RBAC), Domain-Type Enforcement (DTE), and privacy models and privacy enforcement. This section summarizes related work but focus on these three areas.

2.1 Role-Based Access Control (RBAC)

Role-Based Access Control has received increasing attention in the security literature as a promising alternative to traditional discretionary and mandatory access controls. Recent ACM RBAC/SACMAT workshop series since 1996 is an example that signifies this research trend. RBAC has recently been proposed as NIST[6] standard [FSG01].

According to RBAC, a user can only access an object, if he/she is assigned a role, and if the role is assigned certain permission, which is allowed to access the object. An important milestone of RBAC is Sandhu RBAC96 model [SCF96]. In RBAC 96, Sandhu defined a family of RBAC models to manage authorizations in complex systems to perform tasks with many users and many resources. The concept of *role* is similar to functional role in an organization and hence RBAC provides an intuitive way to modeling organizational security policies. RBAC was later proven to be policy neutral, which means it is a way for expressing policy instead of embodying a particular security policy. Osborn and Sandhu [OSM00] proved that RBAC could be configured to enforce traditional mandatory and discretionary access control policies. RBAC supports several well-known security principles: information hiding, least privilege, separation of duties, and data abstraction. Supporting a large set of commercial

[6] National Institute of Standards and Technology (NIST)'s RBAC Research: http://csrc.nist.gov/rbac/.

security requirements is an important reason that RBAC models are widely used in many applications, such as operating systems (e.g. Solaris 8), database management systems (e.g. Oracle 8), and various information systems, etc. Another strength of RBAC is that managing authorizations is much easier than traditional security models because roles are relatively persistent in an organization, compared with user turnover and task reassignment. Complexity, cost, and potential errors are reduced by assigning permissions to roles within an organization [AS00a]. RBAC has also been found able to enforce security policies on the Web [PSA01]. Its potential support for multi-domain environment has been identified in [JAG01, JGA01].

Beznosov suggested RBAC might be used to implement security requirements in the healthcare domain [Bez98]. Chandramouli proposed a framework for multiple authorization types in a healthcare application system using RBAC [Cha01]. Cole argued RBAC might also be an appropriate candidate for implementing privacy requirements in healthcare environment [Col01]. However, RBAC cannot be directly used to enforce privacy policies because it was not designed to model purpose, obligations, and consents of data subjects [Fis01, FO98]. A possible way for implementing RBAC to enforce context-based access control, which can be used to provide privacy enforcement mechanisms, is to combine RBAC with Domain-Type Enforcement (DTE).

2.2 Domain-Type Enforcement (DTE)

Type enforcement is a low-level mandatory access control mechanism that restricts the accesses of a subject to objects by using domain labels on subjects and type labels on objects. Hoffman [Hof97] described a distinction between RBAC and type enforcement: RBAC associates users with roles and describes how a role limits the operations available to a user, whereas type enforcement ties subjects to domains and describes how a domain limits the operations available to a subject. Hoffman combined RBAC and DTE to implement a secure operating system LOCK6 [Hof97]. Hoffman's work does not consider contextual information and applies to operating systems rather than application systems.

Chandramouli [Cha01] proposed a framework, called Dynamic Authorization Framework for Multiple Authorization Types (DAFMAT), in a healthcare application system by combining RBAC and DTE. The DAFMAT framework supports multiple types of authorizations, such as context-based authorizations and emergency authorizations. A logical-driven authorization engine is used to formulate authorization requests and determine the validity of requests. Supporting multiple authorization types is the most important feature of DAFMAT. It provides a basic architecture to enforce privacy policies using context-based authorizations. The limitation of DAFMAT framework for enforcing privacy policies is that it does not model purposes and data policies. Consequently, it cannot enforce purpose binding and policy-driven data usage control. The PARBAC model proposed in this paper is based on the DAFMAT framework and extends its scope to enforce purpose binding and policy driven data usage control.

2.3 Privacy Models and Privacy Enforcement

Privacy protection approaches can be categorized according to how they enforce privacy policies: metadata-based approaches and others. In metadata-based approaches, a tag or some kind of metadata that governs how to use the data is associated with each group of data. The metadata must be checked to decide whether an operation is allowed or not when a subject requests to access its associated data. Metadata-based approaches have an important assumption: the enforcement of security and privacy policies depends on a trusted system environment [Ste97]. The approach proposed in this paper falls into this category.

2.3.1 Metadata-based Approaches

Karjoth et al. [KSW02a] described a technology for privacy-enabled management and exchange of customer data, called the Platform for Enterprise Privacy Practices (E-P3P). E-P3P introduced a viable separation of duty between the three roles of a privacy system: The *privacy officer* designs and deploys privacy policies, the *security officer* designs access control policies, and the *customers* give consent and select opt-in/opt-out choices. A privacy policy language [KS02] is proposed for formalizing a privacy policy and expressing restrictions on the access to personal data. Authorization is granted based on both access control level, which focuses on restricting the access of employees to enterprise applications, and privacy control level, which focuses on restricting the access of applications to collected data. E-P3P is the core technology of IBM Enterprise Privacy Architecture (EPA) [KSW02b]. Powers et al. [PAS02] further defined this approach for enterprise-wide privacy management as five steps. These five steps can be summarized as: define an enterprise privacy policy, deploy a policy to the IT systems, record user consents, enforce the privacy policy, and generate reports of access history.

This approach has several advantages. First, privacy enforcement is built upon access control so that it may be applied to an enterprise's legacy applications. Second, separating privacy control and access control provides more flexibility because privacy control can be realized as real-time enforcement or near-time conformance checking depending on the efficiency requirement of the system. Third, separation of duty for three major roles in a privacy system facilitates privacy management in a large enterprise.

However, this metadata-based approach still has its limitations. The privacy enforcement system in this approach is independent of any access control models. However, the access control model that a system adopts affects how privacy policies can be enforced in the system. This is because privacy policies can only be enforced if they are formalized as access control rules just like security policies. Different systems may use different access control models. To achieve best efficiency, privacy control must be considered together with access control. However, there is no concrete method in this approach that describes how privacy control and access control can be incorporated. Furthermore, this approach only provides a framework for a privacy enforcement system. There is no detail in [KSW02a, KSW02b, PAS02] on how the purpose of an operation is inferred. The privacy enforcement approach using PARBAC

proposed in this paper adopts the basic privacy enforcement and management ideas of E-P3P but base on a concrete access control model.

E-P3P is the first comprehensive privacy enforcement system in the industry and academia we have found to date. There are several other privacy models in the literature that could possibly be used to protect privacy in different domains.

Langheinrich [Lan02] introduced a privacy awareness system (called *pawS*) for ubiquitous computing environments. A key component in this system is a privacy-aware database (called *pawDB*) that combines the collected data elements and their privacy policies into a single unit for storage in order to consequently handle the data according to its usage policy. Langheinrich's approach is innovative but there are some problems. In *pawS* system, data users must submit a corresponding data usage policy together with the data operation request to specify who they are, for what purpose they are querying this information, and how long they plan to keep this information. First, the data usage policy submitted by data users may be not trustable. Second, it requires redeveloping every application in the system, which is sometimes unacceptable and unpractical.

Jiang and Landay [JL02] proposed a theoretical model for privacy control in context-aware systems based on *information space*, a semantic construct to formulate privacy control policy. The owners of an information space define the permissions to access the objects in the space. A boundary delimits an information space and serves as a trigger in privacy control. Boundary crossing or alteration may imply privacy violation. Every object in an information space is associated with a privacy tag. Unified privacy tags are used in the model to support decentralized systems. These tags represent both virtual tags of data objects and physical tags of physical objects to enable similar privacy control for physical resources. The information space model is an innovative theoretical model for privacy control in context-aware environment. However, the information space model is not designed to address privacy invasions to collected consumer data within an organization.

Myers and Liskov [ML00] proposed an approach for control of information flow in systems with mutual distrust and decentralized authority to protect privacy using decentralized label model. Although this approach may be used to protect privacy, the domain in which it is applied is completely different. This approach is used in operating systems for information flow control, rather than in application systems to protect customer data privacy.

2.3.2 Other Approaches

Fischer-Hübner [Fis01, FO98] proposed a formal task-based privacy model, which can be used to technically enforce two privacy requirements, purpose binding and necessity of data collection and processing. A user can access personal data if the access is necessary to perform the current task and the user is authorized to perform the task. In addition, the task's purpose must be consistent with the purposes specified in the privacy policy when data is collected or with the purpose consented by the data owner. Fischer-Hübner also illustrated how privacy policy could be specified and implemented according to the Global Framework

for Access Control (GFAC) approach. This model is the first complete formal privacy model in the literature, as far as we know. However, this model does not consider context-based access control or obligations. It is restricted in a single enterprise.

Park and Sandhu [PS02] proposed a new access control model, called Usage Control (UCON), which can be used to deal with privacy issues in commercial and non-commercial environments. The UCON model encompasses traditional access control, trust management, and digital rights management and goes beyond them in its definition and scope. UCON has similarity with Chandramouli [Cha01]'s DAFMAT framework in that they both include subjects and objects in the model. UCON is similar to Karjoth and Powers et al. [KSW02, PAS02]'s enterprise privacy enforcement approach in that conditions and obligations are considered. However, The UCON model is a preliminary model; it is far from complete. Details on processing conditions, obligations, and authorizations are not addressed in [PS02]. To date no prototype system that implements UCON exists. In addition, UCON is simply an independent model, which may be significantly expensive and hard to implement in a real system because it would require starting from scratch.

2.4 Privacy Policy Modeling

Privacy policies are usually expressed as natural language. To technically enforce a privacy policy, it must be formally represented. Karjoth et al. [KS02] presented a privacy policy language for formalizing a privacy policy and expressing restrictions on the access to personal data. A basic authorization rule contains (*purpose*, *data user*, *operation*) on a data *type*. By extending Flexible Authorization Framework (FAF) with grantors and obligations, an authorization rule may also specify additional *conditions* that must hold, or *obligations* that must be carried out if access is granted. This privacy policy language is used in E-P3P [KSW02a].

Dreyer and Olivier proposed a model called InfoPriv that can be used to model privacy policies [DO99, DO98a, DO98b]. The InfoPriv model maps privacy policies to graphs called information can-flow graphs. An Information Engine analyzes the graph for all possible information flow between entities including conflicting information flow by using graph-traversal algorithms. The Information Engine can further resolve conflicting information flow by using a rule-based approach to choose the best arcs to remove. The InfoPriv model is helpful in analyzing potential privacy violation from the information flow perspective. However, technically it does not indicate how to enforce privacy policies in a real system. It does not consider some major privacy policy elements, such as purposes, conditions, and obligations.

Lategan and Olivier [LO02] proposed a Chinese Wall approach to privacy policies by extending P3P. This approach allows a user to define conflict of interest class information to prevent an organization from learning too much information about him/her. However, this approach does not model a generic privacy policy. It only considers a particular privacy requirement: conflict of interest personal information.

There are many works in the literature on security policy modeling. Some of these works may also be used on privacy policy. However, a security policy usually does not consider purpose and obligations. Thus, modeling privacy policy needs special consideration. This paper adopts a similar privacy policy language that is mostly based on Karjoth et al. [KS02]'s work because their approach can model most basic privacy policies.

2.5 Other Related Work

Protecting collected consumer data is the working domain of this paper, but privacy protection is not limited to this domain. Other privacy issues include protecting user identities by providing *anonymity*, *pseudonymity*, *unlinkability*, and *unobservability* of users at communication level, system level, or application level [PW87, Cha81, Cha85, Cha88, RR98], protecting usee identities by providing *anonymity* and *pseudonymity* of data subjects, e.g. inference control in statistical database systems [Dom02], data mining and privacy [AS00b], email privacy, e.g. PGP[7] [RFC2440], etc. These topics are beyond the scope of this paper.

Because purpose as a new entity is modeled in PARBAC, we have also looked up in the literature for purpose-oriented access control. Yasuda et al. [YTT97, YTT98a, YTT98b] proposed a purpose-oriented access control model to manage information flow control in distributed applications. Purpose-oriented access rules indicate what operation in each object can invoke operations of other objects. This approach is not suitable for customer privacy protection within an organization.

3 The PARBAC Model

The PARBAC model is an extended role-based access control model, which combines Chandramouli's DAFMAT framework [Cha01] and privacy enforcement and management ideas from [KSW02, PAS02]. This section describes components and entity relationships between components in detail.

3.1 Components in the PARBAC Model

The main authorization entities in the PARBAC model are (1) User, (2) Role, (3) Subject, (4) Domain, (5) Purpose, (6) Object-Type, and (7) Object-Policy. Figure 1 illustrates the PARBAC model architecture. Among these entities, purpose and object-policy are newly introduced in the PARBAC model. We briefly describe the other five entities first and then go through details in purpose and object-policy. New components in Figure 1 are dark-shaded. The arrows from role to role and from purpose to purpose represent role hierarchy and purpose hierarchy respectively. M:N, N:1, 1:N, and 1:1 on each arrow represent entity

[7] Pretty Good Privacy: http://www.pgp.com/.

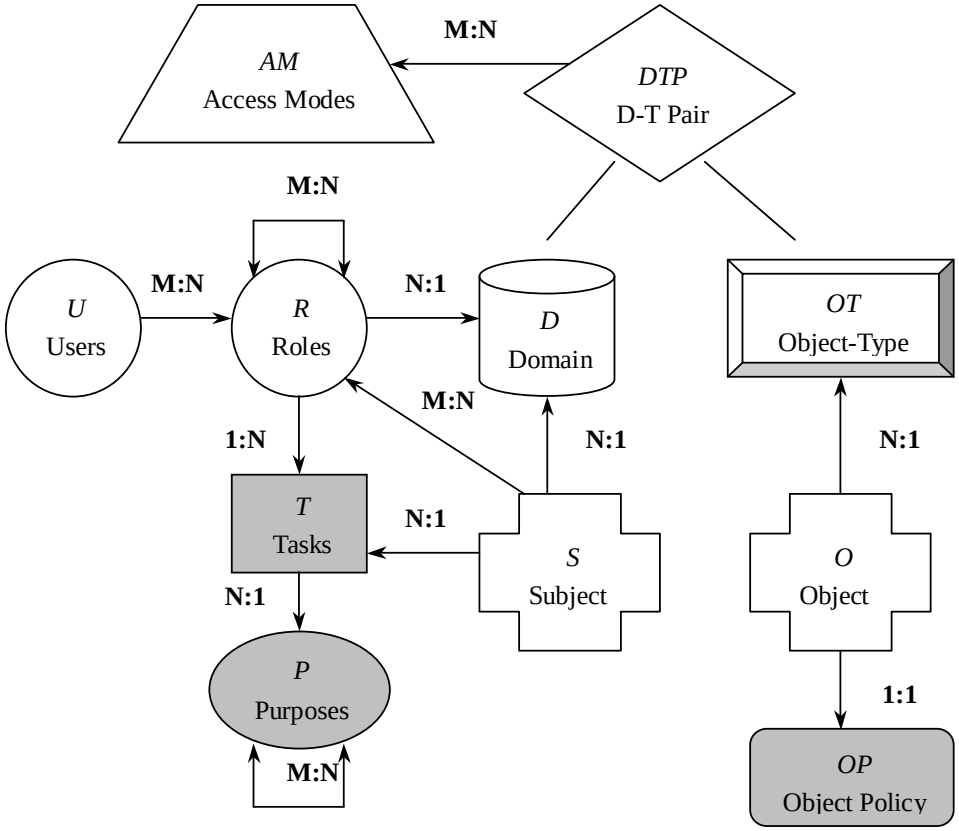

Figure 1 The PARBAC Model Architecture

mapping relationships as explained in Section 3.2.

3.1.1 Entities also Included in DAFMAT Framework

Roles in DAFMAT framework represent job positions. This definition leads User_Role relation to a many-to-one relation: every user is assigned a unique role and each role may be assigned several users. PARBAC still adopts the traditional semantic definition of role in RBAC96 [SCF96]: a role is "a job function within the organization that describes the authority and responsibility conferred on a user assigned to the role". This definition allows User_Role relation to be a many-to-many relation.

Subjects are programs, user agents or executables that a user invokes to carry out business process functions with delegation of certain roles. **Domains** represent high-level enterprise functional area within which roles should perform. For example, marketing representative role performs tasks within the domain of marketing. An **Object-Type** represents a group of objects that carry related information and can be processed in a similar way. For example, a Customer-Contact-Info-Type may consist of a collection of objects and records pertaining to customer contact information, such as address, email, phone, etc.

3.1.2 Purpose and Task

A new component introduced in the PARBAC model is **purpose**. To be specific, the purpose here means business purpose: the purpose for which an operation is executed. This is to differentiate business purpose from customer data usage purpose specified in privacy policies and consented by customer, which we called data purpose. One difference between business purpose and data purpose is that data purpose is usually high level, such as completing transaction, contacting, marketing, etc., whereas business purpose is sometimes more concrete and specific, such as email-marketing, postal-marketing, etc.

Purpose relation is a partial ordered relation just like role hierarchy relation in [SCF96]. A partial order is a reflexive, transitive, and antisymmetric relation. Partial ordered relation enables the PARBAC model to support complex purpose hierarchies, such as tree, inverted tree and lattice structure. Purpose hierarchy is used to map high-level data purpose to low-level business purpose. If an operation is allowed for a given purpose, it is also allowed for all sub-purposes. Figure 2 illustrates a sample hierarchy of marketing purpose. In this example, email marketing, postal marketing and phone/fax marketing are sub-purposes of both direct marketing and third-party marketing.

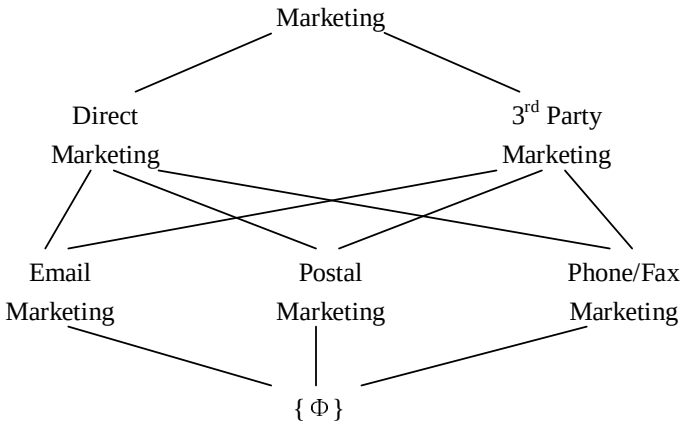

Figure 2 Purpose Hierarchy for Marketing

Purpose relation must allow unambiguous purpose lookup. The following scheme is an example of ambiguous purpose lookup. If a customer consented his personal information can only be used for email marketing purpose, the access decision of an operation with the purpose of direct marketing cannot be determined. This is because email marketing belongs to both direct marketing and third-party marketing purpose. The system cannot determine what the exact parent purpose is that email marketing belongs to.

The above problem can be solved by placing restrictions on the purpose hierarchy. In the PARBAC model subjects are required to map to the lowest level of purpose hierarchy. This is to say, the purpose for an operation must be as specific as possible. In this way, data purpose is either in the same level as business purpose or in a higher level. Therefore, there is no ambiguous purpose lookup from business purpose to data purpose.

Purpose cannot be directly associated with <role, permission> pairs. This is because if two

roles are granted the same permission for different purposes and a user is assigned both roles, then system cannot decide the actual purpose of an operation. For example, a role in the delivery department and a role in the marketing department may have the permission to access customer contact information but for different purposes. If a user is assigned both roles and accesses customer contact information, system cannot determine the exact purpose of this operation. This is why **task** is introduced in the PARBAC model. Task serves as an intermediary entity between roles and permissions. This function was also described in [Eps02, ES01]. A role invokes one or more subjects in order to perform some task. Task has a similar hierarchy as purpose but this is not illustrated in Figure 1. To make the task that a subject maps as specific as possible, the subject is required to map to a lowest level task. As for the above example, although a user may be assigned both roles, he/she is performing different tasks to access customer contact information. Thus, the exact purpose can be derived from the task he/she is performing. Task has a similar hierarchy as purpose, which we named task network.

3.1.3 Object-Policy

Another new entity in the PARBAC model is object-policy. Object-policy is actually data usage policy. In a privacy-aware application system, each customer's personal information should be governed to use by a separate policy. This policy is based on the organization's privacy policy, customized with each customer's special preferences, such as opt-in/opt-out choices, user consent, etc. More details about object-policy are described in Section 4.

3.2 Entity Relationships in the PARBAC Model

The relationship of entities are mapping from a source entity to a target entity with either a many-to-many, many-to-one, one-to-many, or one-to-one relation, which are represented as M:N, N:1, 1:N, 1:1 respectively in Figure 1.

3.2.1 User_Role(user, role): many-to-many

A user may be assigned several roles and a role may be assigned to several users. This is different from the User-Role relation in DAFMAT framework as it is mentioned in Section 3.1.1. This paper uses similar notations in DAFMAT framework to represent the entity relationships. In this case, User-Role relation is represented as User_Role(user, role).

3.2.2 Role_Domain(role, domain): many-to-one

A domain represents a functional area within an enterprise. Several roles may be associated with a domain but a role always belongs to a unique domain.

3.2.3 Role_Task(role, task): one-to-many

Each task is assigned to a unique role to execute, but a role may perform different tasks.

3.2.4 Subject_Role(subject, role): many-to-many

Subjects are invoked by one or more roles to perform certain task on behalf of a user. A role may have to invoke several subjects in order to carry out designated task.

3.2.5 Subject_Domain(subject, domain): many-to-one

The execution semantics of a subject is to be defined based on the domain it belongs to. Therefore, a subject is associated with a unique domain. There may be more than one subject in a domain.

3.2.6 Subject_Task(subject, task): many-to-one

Task serves as an intermediary entity between roles and permissions. A subject can be associated with many tasks. However, in the PARBAC model, a subject is always mapped to the lowest level task, a leaf node in the task network. Performing a task may need to invoke several subjects.

3.2.7 Task_Purpose(task, purpose): many-to-one

A task can be associated with many purposes. In the PARBAC model, a task is required to be associated with a lowest level purpose, a leaf node in purpose hierarchy. Multiple tasks can be mapped to the same purpose.

3.2.8 Object_ObjectType(object, object-type): many-to-one

An Object-Type stands for a collection of objects carrying related information. Hence, each object is mapped to a unique object-type and an object-type may contain several objects.

3.2.9 Object_ObjectPolicy(object, object-policy): one-to-one

Each object must have a unique policy to govern its use and each policy belongs to a unique object.

3.2.10 DTE_Entry(domain, object-type, access-modes): many-to-many

The domain-type pairs are stored in a table called Domain-Type Access Matrix (DTE table). In each entry of the DTE table is a collection of allowable access modes. Thus, the mapping from domain-type to access modes is a many-to-many relation.

3.2.11 Role_Role(role1, role2): many-to-many

Role relationship in the role hierarchy is a partial ordered relation, in which role2 is a super-role of role1.

3.2.12 Task-Task(task1, task2): many-to-many

Task relation is similar to role relation. Task2 is a super-task of task1.

3.2.13 Purpose-Purpose(purpose1, purpose2): many-to-many

Purpose relation is similar to role relation. Purpose2 is a super-purpose of purpose1.

3.3 Constraints on Entity Relationships

The relationships of entities may be qualified by constraints. Constraints are one of the most important features of RBAC, which can be used to express security requirements such as separation of duties. In the following example constraints, ∀ represents "for any", ∃ represents "there exists", ∧ represents "logical and", and ➔ represents "implies".

Constraint 1: All the roles from which a subject can be invoked should be assigned to the same unique domain, which is associated with the subject. Constraint 1 can be expressed as

∀ (subject, domain, role), Subject_Domain(subject, domain) ∧ Subject_Role(subject, role) ➔ Role_Domain(role, domain)

Constraint 2: If performing two tasks needs to invoke the same subject, these two tasks must be mapped to the same purpose. This constraint can be expressed as

∀ (subject, task1, task2), Subject_Task(subject, task1) ∧ Subject_Task(subject, task2) ➔ ∃ a unique purpose, Task_Purpose(task1, purpose) ∧ Task_Purpose(task2, purpose)

Constraint 3: A role can be associated with a subject if and only if the role is authorized to perform some task and it is necessary to invoke the subject to complete the task. This constraint can be expressed as

∀ (task, role, subject), Role_Task(role, task) ∧ Subject_Task(subject, task) ➔ Subject_Role(subject, role)
∀ (role, subject), Subject_Role(subject, role) ➔ ∃ a unique task, Role_Task(role, task) ∧ Subject_Task(subject, task)

4 Privacy Enforcement with the PARBAC Model

In this section, how privacy can be enforced using the PARBAC model is described. We first briefly introduce the prerequisites of this approach, privacy policy elements and rules, and then focus on the authorization process in the PARBAC model.

4.1 Prerequisites

An important module of a privacy enforcement system is customer privacy preferences management. When customer data are collected online or offline, customers can specify their privacy preferences (e.g. opt-in/opt-out choices, user consent, etc.) on how the organization can use the data. Customers may change their privacy preferences at any time after the data has been collected. In addition, customer data may be grouped together and the group of data can be handled under a single policy. Another task of privacy preferences management is to link these preferences with the actual data with which they are associated. This paper assumes each group of customer data is associated with a privacy preference tag. Whenever a subject requests to access a group of customer data or some specific customer data, we can retrieve

its corresponding privacy preferences from privacy management system.

4.2 Privacy Policy Elements and Rules

According to [PAS02], a general privacy policy rule can be expressed as

ALLOW [Data User]
to perform [Operation] on [Data Type]
for [Purpose] provided [Condition]
Carry out [Obligation]

The element *purpose* is described in Section 2. Here we only discuss several other elements special to privacy policy: *data type*, *condition* and *obligation*. The concept of *data type* is very important for privacy enforcement because data are usually treated in groups in privacy policies. For example, a sample privacy policy is "purchase history can be used for research analysis in an anonymous way and contact information cannot be used for marketing purpose". Contact information and purchase history are examples of data types. Name, address, zip code, and telephone number, etc. belong to contact information data type.

Some privacy policies require certain *conditions* to be satisfied in order to access data. For example, legislation requires organizations obtain data subject consent first before they use personal information for a particular purpose. User consent is a sample condition. Another example of conditions is the *retention* period in P3P, i.e. how long the data will be kept. The condition is "under valid data lifetime". Some privacy policies require additional operations to be carried out when a certain access is allowed. These additional operations are *obligations* that the privacy enforcement system must carry out if the access is allowed. For example, a sample policy is "my contact information can be used to complete transaction, but they must be deleted in 30 days". "Delete customer data in 30 days" is a sample obligation in this case.

4.3 Purpose Inference in the PARBAC Model

The purpose of a data access can be inferred from the entity relationships defined in the PARBAC model. When a user invokes some subject to carry out business process functions with delegation of certain roles, the subject is first mapped to a unique task in the task network. As it is mentioned in Section 3.2.6, a subject is always mapped to a leaf node in the task network. Then the corresponding task is mapped to a unique purpose, which is also a leaf node in the purpose hierarchy as it is mentioned in Section 3.2.7. In this process, the business purpose of the data access request is identified.

4.4 Privacy Authorizations

The authorization process in the PARBAC model is illustrated in Figure 3. When a data user requests to access certain privacy protected data resource, access control is to be checked first and the corresponding data policy is retrieved from privacy management system at the same time. Access control is checked based on roles activated in the current session, the subjects

invoked by these roles to access data, role-subject mapping, subject-domain mapping, and the domain-type access matrix. If the request passes the role/permission check, then data purpose, which is retrieved from data policy, is to be checked against the business purpose inferred from the PARBAC model as described in Section 4.3. Because the business purpose is always a leaf node in the purpose hierarchy, the decision can be made by using graph search algorithms. If there exists a path from the data purpose node to business purpose node, then the business purpose is compliant with the data purpose. Otherwise, it is not compliant. If these two purposes match, then conditions are to be checked, if there are additional conditions need to be qualified. If the request passes this procedure, then access is granted.

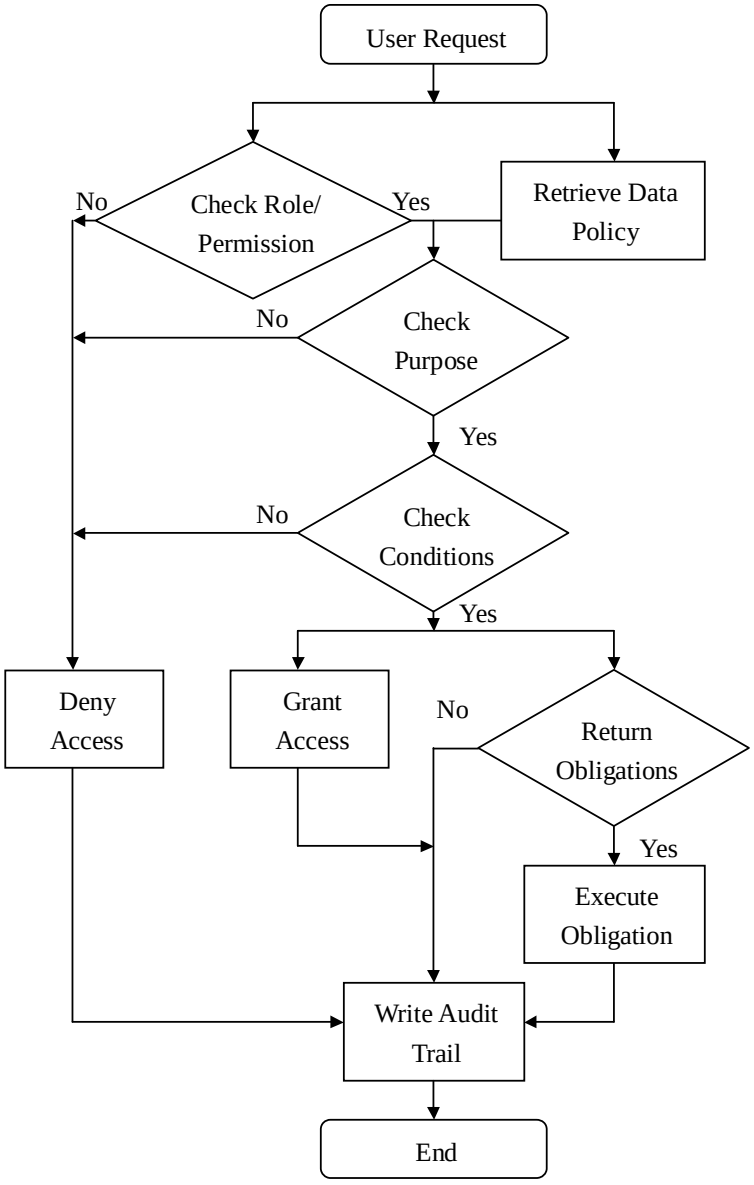

Figure 3 Authorization Process of Privacy Enforcement

Otherwise, access is denied. Note if obligations are found in data policy, they need to be executed by obligation execution module. All data access requests should be logged in the audit trail for future auditing; no matter access requests are granted or denied.

5 Application of the PARBAC Model in A Privacy Scenario

A simplified privacy scenario is constructed to describe the application of the PARBAC model. Consider an online drug store named eDrug, which belongs to healthcare industry and should conform to HIPAA [HIP96]. eDrug sells over-the-counter medicine to customers older than 18 years old.

5.1 Data Collection by eDrug

The data collected by eDrug is listed in Table 1.

Fieldnames	Data Type	Description
Username	LoginInfo	
Password	PasswordInfo	
FirstName, MiddleInitial, LastName	IdentityInfo	
Birthday	BirthdayInfo	Birthday is used to determine the age of customer.
StreetAddress, City, State, ZipCode	PostContactInfo	
Phone, Fax	PhoneFaxContactInfo	
Email	OnlineContactInfo	
CardType, CardOwner, CardNumber, ExpirationDate	CreditCardInfo	Credit card info is only used for payment authentication and it will not be shared with third-parties.
OrderHistory	OrderInfo	
AnonymousResearchOptOut	CustomerPrivacyPref	Anonymous Research of customer order history by eDrug, customer may opt-out from this service
DirectMarketingOptIn	CustomerPrivacyPref	Require customer opt-in, if TRUE, customer data can be used for direct marketing purpose from eDrug,
OrderHistorySharingConsent	CustomerPrivacyPref	Require customer's written consent. If set to TRUE, IdentityInfo, ContactInfo, and OrderHistory may be shared with third-parties.

Table 1 Fields of Data Collected by eDrug

5.2 Privacy Policy of eDrug

eDrug's privacy policy is committed to protect customer privacy. A customer consents to the

data being collected and stored. Customer information is essentially used to complete transactions. Order history may be used for research purpose in an anonymous way without obtaining individual customer consent, but eDrug allows customers to opt-out from this service. Contact information and order history may be used for direct marketing purpose by eDrug, but this service requires customer opt-in. Credit card information is only used for payment authentication and will not be shared with third-parties. Contact information and order history may be shared with third-parties but customer written consent is required.

5.3 Entities and Entity Relationships

In this scenario, four users (i.e. Olive, David, Paul, and Ron) assume four roles in different departments of eDrug. The main entities and entity relationship mappings in the PARBAC model are listed below.

Users = {Olive, David, Paul, Ron}
Roles = {OPC, DMR, PRM, RDE}
OPC: Order Process Clerk, DMR: Direct Marketing Representative
PRM: Partner Relationship Manager, RDE: Research & Development Expert
Domains = {OPD, DMD, TPMD, RDD}
OPD: Order Process Domain, DMD: Direct Marketing Domain
TPMD: Third-Party Marketing Domain, RDD: Research & Development Domain
Subjects = {OPP, DMP, TPSP, RDP}
OPP: Order Process Procedure, DMP: Direct Marketing Procedure
TPSP: Third-Party Sharing Procedure, RDP: Research & Development Procedure
Tasks = {DP, CC, SCCI, AR}
DP: Deliver Product, CC: Contact Customer,
SCCI: Share Customer Contact Information, AR: Anonymous Research
Purposes = {CTP, ARP, DMP, TPSP}
CTP: Complete Transaction Purpose, ARP: Anonymous Research Purpose,
DMP: Direct Marketing Purpose, TPSP: Third-Party Sharing Purpose

User-Role Assignment = {User_Role(Olive, OPC), User_Role(David, DMR), User_Role(Paul, PRM),
User_Role(Ron, RDE)}
Role-Domain Mapping = {Role_Domain(OPC, OPD), Role_Domain(DMR, DMD),
Role_Domain(PRM, TPMD), Role_Domain(RDE, RDD)}
Role-Task Mapping = {Role_Task(OPC, DP), Role_Task(DMR, CC), Role_Task(PRM, SSCI),
Role_Task(RDE, AR)}
Subject-Domain Mapping = {Subject_Domain(OPP, OPD), Subject_Domain(DMP, DMD),
Subject_Domain(TPSP, TPMD), Subject_Domain(RDP, RDD)}
Subject-Role Mapping = {Subject_Role(OPP, OPC), Subject_Role(DMP, DMR),
Subject_Role(TPSP, PRM), Subject_Role(RDP, RDE)}
Subject-Task Mapping = {Subject_Task(OPP, DP), Subject_Task(DMP, CC),
Subject_Task(TPSP, SCCI), Subject_Task(RDP, AR)}
Task-Purpose Mapping = {Task_Purpose(DP, CTP), Task_Purpose(CC, DMP),
Task_Purpose(SCCI, TPSP), Task_Purpose(AR, ARP)}

Domain-Type Access Matrix (C: create, U: update, D: delete, V: view):

Domain	Object-Type/Access Modes		
	OrderHistory	CreditCardInfo	ContactInfo
OPD	C, U, D, V	V	V
DMD	V		V
TPMD	V		V
RDD	V		V

Table 2 Domain-Type Access Matrix

5.4 Privacy Enforcement with the PARBAC Model

Based on the authorization process described in Section 4.4, we now examine several example requests from data users and analyze whether these requests will be granted or denied access.

Request 1: User David invokes Direct Marketing Procedure (DMP) and requests to access customer credit card info

Access denied. David with role Direct Marketing Representative (DMR) falls into Direct Marketing Domain (DMD). DMR is authorized to invoke subject Direct Marketing Procedure (DMP) from Subject-Role mapping. However, DMD is not authorized to access customer credit card info in the DTE-table. After checking role/permission, access is denied. Traditional access control can also implement this function.

Request 2: User David invokes Direct Marketing Procedure (DMP) and requests to access customer contact info

Whether access granted or denied depends on specific customer privacy preferences. David with role Direct Marketing Representative (DMR) falls into Direct Marketing Domain (DMD). DMR is authorized to invoke subject Direct Marketing Procedure (DMP) from Subject-Role mapping. From DTE-table, DMD is authorized to access customer contact info. The request passes the role/permission check. The next step is to check purpose. From Subject-Task and Task-Purpose mapping, a unique purpose Direct Marketing Purpose (DMP) is identified. Business purpose and data purpose is matched. However, additional addition customer.DirectMarketingOptIn = TRUE needs to be qualified. In the data policy, customer contact info can be used for direct marketing purpose only if the customer opts in this service. If it returns true, then access is granted. Otherwise, access is denied.

The above example requests demonstrate that the PARBAC model can be used to enforce purpose binding and policy-driven data usage control. However, it is to indicate that this is a simplified scenario. This paper does not consider cases in a large organization that have many roles and many tasks. In these cases, role hierarchies, purpose hierarchies, and task networks complicate the PARBAC authorization process. Therefore, this model needs further validation in a wider scope.

6 Summary and Future Work

Privacy protection can only be achieved by enforcing privacy policies within an organization's online and offline data processing systems. Privacy should be considered together with security protection and combined with data management technologies. The PARBAC model proposed in this paper provides support to privacy enforcement by combining access control and privacy management. PARBAC goes beyond traditional access control models in that it not only provides system security from an organization's perspective, but also protects consumer privacy from a consumer's standpoint. PARBAC enables enterprises and organizations to act as a trusted custodian to protect customer data privacy.

However, this approach is still a metadata-based approach and cannot guarantee privacy compliance because it is built upon a trusted system. Object policies are used to govern the use of objects. If malicious applications or users changed object policy, privacy enforcement cannot be guaranteed. That's why we call this model a privacy-aware model. In addition, this approach cannot solve all privacy problems. It can only protect collected customer data privacy. Several other privacy issues, such as privacy invasion by data mining, anonymity, etc., are beyond the scope of this approach.

Furthermore, this paper is far from complete. Many details are omitted, such as formal definition of the PARBAC model, privacy policy language specification, privacy preferences management, detailed authorization mechanism, and further validation, etc. This paper only illustrates the basic idea of integrating privacy protection with RBAC.

Developing such a model is only part of my work. Besides enriching and completing the PARBAC model, my research plan also includes defining a general role engineering [Coy96] methodology to map applications and policies into the PARBAC model. I plan to use goal-driven requirements engineering [Lam01] techniques to derive roles, permissions, purposes, and assign permissions to roles within a privacy-aware environment. This part of work will be discussed in my Ph.D. thesis proposal.

7 Acknowledgement

The author would like to thank Dr. Annie I. Antón and Dr. Peng Ning for their direction and suggestion.

References

[AE01] Annie I. Antón and Julia B. Earp. Strategies for Developing Policies and Requirements for Secure Electronic Commerce Systems, In *E-Commerce Security and Privacy*, edited by Anup K. Ghosh, Kluwer Academic Publishers, pp. 29-46, 2001.

[AEA01] Annie I. Antón, Julia B. Earp and Thomas A. Alspaugh. The role of Privacy and Privacy Values in Requirements Engineering, *IEEE 5th International Symposium on Requirements Engineering (RE'01)*, Toronto, Canada, pp. 138-145, August 2001.

[AS00a] Gail-Joon Ahn and Ravi Sandhu. Role-Based Authorization Constraints Specification, *ACM Transaction on Information and Systems Security*, Volume 3 No. 4, pp. 207-226, November 2000.

[AS00b] Rakesh Agrawal and Ramakrishnan Srikant. Privacy-preserving data mining, *Proc. of the 2000 ACM International Conference on Management of Data and Symposium on Principles of Database Systems*, pp. 439-450, Dallas, Texas, 2000.

[Bez98] Konstantin Beznosov. Requirements for Access Control: US Healthcare Domain, *Proc. of the 3rd ACM Workshop on Role-Based Access Control*, pp. 43, Fairfax, VA, 1998.

[Cha01] Ramaswamy Chandramouli. A Framework for Multiple Authorization Types in a Healthcare Application System, *Proc. of the 17th Annual Computer Security Applications Conference (ACSAC 2001)*, pp. 137-148, IEEE, 2001.

[Cha81] D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, *Communications of the ACM*, Vol. 24 (2), pp. 84-88, 1981.

[Cha85] D. Chaum. Security without Identification: Transaction Systems to Make Big Brother Obsolete, *Communications of the ACM*, Vol. 28 (10), pp. 1030-1044, 1985.

[Cha88] D. Chaum. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, *Journal of Cryptology*, No. 1, pp. 65-75, 1988.

[Col01] Kenneth Cole. HIPAA Compliance: Role Based Access Control Model, *GSEC-SANS Security Essentials Certified Program Graduates Research Project*, http://www.giac.org/practical/Kenneth_Cole_GSEC.doc, 2001.

[Coy96] Edward J. Coyne. Role Engineering, *Proc. of the 1st ACM Workshop on Role-Based Access Control*, Gaithersburg, MD, 1996.

[Den76] Dorothy E. Denning. A Lattice Model of Secure Information Flow, *Communications of the ACM*, Volume 19 Issue 5, pp. 236–243, May 1976.

[DO98a] Lucas C. J. Dreyer and Martin S. Olivier. A Workbench for Privacy Policies, *Proc. of 22nd Annual International Computer Software and Applications Conference (COMPSAC'98)*, pp. 350-355, IEEE, 1998.

[DO98b] Lucas C. J. Dreyer and Martin S. Olivier. Dynamic Aspects of the InfoPriv Model for Information Privacy, *Proc. of the 9th International Workshop on Database and Expert Systems Applications*, pp. 340-345, IEEE, 1998.

[DO99] Lucas C. J. Dreyer and Martin S. Olivier. An Information-Flow Model for Privacy (InfoPriv). In S Jajodia (editor), *Database Security XII: Status and Prospects*, pp. 77-90, Kluwer, 1999.

[Dom02] Domingo-Ferrer, J. (Editor). Inference Control in Statistical Databases, *Lecture Notes in Computer Science (LNCS)*, Volume 2316, Springer-Verlag, 2002.

[FBP01] James Fan, Ken Barker, Bruce Porter, and Peter Clark. Representing Roles and Purpose, *Proc. of the 2001 International Conference on Knowledge Capture (K-CAP'01)*, pp. 38-43, ACM, October 2001.

[FIP98] *Fair Information Practice Principles, Privacy Online: A Report to Congress (Part III)*, Federal Trade Commission, http://www.ftc.gov/reports/privacy3/fairinfo.htm, June 1998.

[Fis01] Simone Fischer-Hübner. IT-Security and Privacy, *Lecture Notes in Computer Science 1958 (LNCS 1958)*, Springer-Verlag, 2001.

[FSG01] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, et al. Proposed NIST Standard for Role-Based Access Control, *ACM Transactions on Information and System Security*, Volume 4 No 3, pp. 224-274, August 2001.

[FO98] Simone Fischer-Hübner and Amon Ott. From a Formal Privacy Model to its Implementation, *Proc. of the 21st National Information Systems Security Conference*, Oct. 5-8, 1998.

[GHS00] J. Goldman, Z. Hudson and R. Smith. *Privacy: Report on the Privacy Policies and Practices of Health Web Sites*, California HealthCare Foundation, January 2000.

[GLB01] *Gramm-Leach-Bliley Act: Financial Privacy and Pretexting*, Federal Trade Commission, http://www.ftc.gov/privacy/glbact/index.html.

[HIP96] *The 1996 Health Insurance Portability and Accountability Act (HIPAA)*, HEP-C ALERT, http://www.hep-c-alert.org/links/hippa.html.

[Hof97] John Hoffman. Implementing RBAC on a Type Enforced System, *Proc. of the 13th Annual Computer Security Applications Conference*, pp. 158-163, IEEE, 1997.

[JAG01] James B.D. Joshi, Walid G. Aref, Arif Ghafoor, and Eugene H. Spafford. Security Models for Web-Based Applications, *Communications of the ACM*, Volume 44 No 2, pp. 38-44, Feb. 2001.

[JGA01] James Joshi, Arif Ghafoor, Walid G. Aref, and Eugene H. Spafford. Digital Government Security Infrastructure Design Challenges, *IEEE Computer*, Vol. 34 Issue 2, pp. 66-72, Feb. 2001.

[JL02] Xiaodong Jiang and James A. Landay. Modeling Privacy Control in Context-Aware Systems, *IEEE Pervasive Computing*, Volume 1 Issue 3, pp. 59-63, July-September, 2002.

[KS02] Günter Karjoth and Matthias Schunter. A Privacy Policy Model for Enterprises, *Proc. of the 15th IEEE Computer Security Foundations Workshop*, pp. 271-281, IEEE, 2002.

[KSW02a] G. Karjoth, M. Schunter, and M. Waidner. The Platform For Enterprise Privcy Practices – Privacy-enabled Management of Customer Data. *Proc. of the 2002 Workshop on Privacy Enhancing Technologies*, San Francisco, CA, 2002.

[KSW02b] G. Karjoth, M. Schunter, and M. Waidner. Privacy-enabled Services for Enterprises. *Proc. of the 13th International Workshop on Database and Expert Systems Applications (DEXA'02)*, IEEE, 2002.

[Lam01] Axel van Lamsweerde. Goal-Oriented Requirements Engineering: A Guided Tour, *Proc. of the 5th International Symposium on Requirements Engineering (RE'01)*, pp. 249-262, IEEE, 2001.

[Lam74] B. Lampson. Protection, *Proc. of the 5th Symposium on Information Sciences and Systems*, Princeton, NJ, pp. 437-443, March 1974.

[Lan02] Marc Langheinrich. A Privacy Awareness System for Ubiquitous Computing Environments, *Proc. of the 4th International Conference on Ubiquitous Computing (UbiComp 2002)*, Sep. 2002.

[LO02] Frans A. Lategan and Martin S. Olivier. A Chinese Wall Approach to Privacy Policies for the Web, *Proc. of the 26th Annual International Computer Software and Applications Conference (COMPSAC'02)*, IEEE, 2002.

[ML00] Andrew C. Myers and Barbara Liskov. Protecting Privacy Using the Decentralized Label Model, *ACM Transactions on Software Engineering and Methodology*, Volume 9 No 4, pp. 410-442, October 2000.

[OEC80] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Organization of Economic Cooperation and Development, http://www1.oecd.org/publications/e-book/9302011E.PDF, 1980.

[OSM00] Sylvia Osborn, Ravi Sandhu and Qamar Munawer. Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies, *ACM Transactions on Information and System Security*, Volume 3 Issue 2, pp. 85-106, May 2000.

[PAS02] Calvin S. Powers, Paul Ashley, Matthias Schunter. Privacy Promises, Access Control, and Privacy Management, *Proc. of the 3rd International Symposium on Electronic Commerce*, pp. 13-21, IEEE, 2002.

[PS02] Jaehong Park and Ravi Sandhu. Towards Usage Control Models: Beyond Traditional Access Control, *Proc. of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT'02)*, Monterey, CA, pp. 57-64, ACM, 2002.

[PSA01] Joon S. Park, Ravi Sandhu, and Gail-Joon Ahn. Role-Based Access Control on the Web, *ACM Transactions on Information and System Security*, Volume 4 No 1, pp. 37-71, February 2001.

[PW87] A. Pfitzmann and M. Waidner. Networks without User Observability, *Computers and Security*, Vol. 6 (2), pp. 158-166, 1987.

[RFC2440] OpenPGP Message Format, *The Internet Engineering Task Force (IETF)*, http://www.ietf.org/rfc/rfc2440.txt.

[RR98] M. Reiter and A. Rubin. Crowds: Anonymity for Web Transactions, *ACM Transactions on Information and System Security*, Volume 1 No 1, pp. 66-92, November 1998.

[San93] Ravi S. Sandhu. Lattice-Based Access Control Models, *IEEE Computer*, Volume 26 Issue 11, pp. 9–19, Nov. 1993.

[SCF96] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman. Role-Based Access Control Models, *IEEE Computer*, Volume 29 Issue 2, pp. 38–47, Feb. 1996.

[SS94] R. Sandhu and P. Samarati. Access Control: Principles and Practice, *IEEE Communications Magazine*, Volume 32 Issue 9, pp. 40-48, Sep. 1994.

[Ste97] Mark Stefik. Trusted Systems, *Scientific American*, pp. 78-81, March 1997. Also available at http://www.sciam.com/0397issue/0397stefik.html.

[WB 1890] S. D. Warren and L. D. Brandeis. The Right to Privacy, *Harvard Law Review*, No. 5, pp. 193-220, 1890-91.

[Wes67] A. Westin. Privacy and Freedom, New York, 1967.

[YTT97] Masashi Yasuda, Takayuki Tachikawa, and Makoto Takizawa. Information Flow in a Purpose-Oriented Access Control Model, *Proc. of the 1997 International Conference on Parallel and Distributed Systems*, pp. 244-249, IEEE, 1997.

[YTT98a] M. Yasuda, T. Tachikawa, M. Takizawa. A purpose-oriented access control model, *Proc. of 12th International Conference on Information Networking (ICOIN-12)*, pp. 168-173, IEEE, 1998.

[YTT98b] Masashi Yasuda, Takayuki Tachikawa, and Makoto Takizawa. A Purpose-Oriented Access Control Model for Object-Based Systems, *Proc. of the 1st International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC'98)*, pp. 146-147, IEEE, 1998.