A formal examination of roles and permissions in access control

Philippe Balbiani

To cite this version:

Philippe Balbiani. A formal examination of roles and permissions in access control. 3rd ACS/IEEE International Conference on Computer Systems and Applications (AICCSA 2005), Jan 2005, Cairo, Egypt. pp.1-4, 10.1109/AICCSA.2005.1387087 . hal-04002017

A formal examination of roles and permissions in access control

Philippe Balbiani
Institut de recherche en informatique de Toulouse, Université Paul Sabatier,
118 route de Narbonne, 31062 Toulouse Cedex 4, France

Abstract

This paper describes a model for access control based on roles and permissions. Then it considers computational problems related to the verification of properties in protection systems defined from our model.

1 Introduction

Most access control mechanisms integrate access-matrix models into computer systems. Their purpose is to monitor all accesses to objects with specific rules for protection states transformation. Their strength rests on the safety of such-and-such set of rules with respect to such-and-such security policy, see Bishop [2]. Through access control mechanisms, computer systems examine identities possessed by users in order to infer the actions they are allowed to carry out. Assuming that identities legally possessed by users are available by means of cryptographic techniques, this paper examines a framework formulated by means of an access-matrix model for describing the actions legally carried out by users.

A computer system can be seen as a collection of users such as human beings or robots and a collection of objects such as files or directories. Any user has a well-defined set of sessions during the duration of which the user can access to objects whereas any object has a well-defined set of actions during the execution of which the object can be accessed by users. Two types of access control mechanisms integrate access-matrix models: discretionary access control [8, 9, 10] and role-based access control [16]. With discretionary access, a matrix associates users with objects. Describing the current protection state in a computer system, it permits users to allow access to objects under their ownership. In many organizations however, users do not own objects and control is most of the time based on roles of users, i.e. positions, and permissions on objects, i.e. privileges. With role-based access consequently, the matrix associates roles with permissions: the possibility for a user to legally carry out such-and-such an action on some object during such-and-such a session depends both on the roles associated to the user with respect to that session and the permissions associated to the object with respect to that action. This simplifies the administration of access control in an organization, seeing that roles and permissions last usually longer than users and objects.

This paper examines a framework for describing the actions legally carried out by users by means of an access-matrix model based on roles and permissions. Although we follow the general principles for role-based access control, our framework slightly departs from the reference models presented, for instance, by Ferraiolo, Kuhn and Chandramouli [5]. The core of our model is a matrix whose rows are indexed by roles and whose columns are indexed by permissions. Following the line of reasoning suggested by recent studies [4, 6], we see roles as the means to name the links among users and sessions and permissions as the means to name the links among objects and actions. Though the same user can intervene in many sessions during the duration of which it plays one or more roles, we believe that the same session can involve different users. Though the same object can be under the effects of different actions during the execution of which it is concerned by one or more permissions, we believe that the same action can have an effect on different objects.

Section 2 introduces the concept of state as a tool for characterizing the link between roles and permissions. Considering roles as binary relations between users and sessions and permissions as binary relations between objects and actions, section 3 deals with the concept of global state. Section 4 reviews the implicit information between roles, users and sessions or permissions, objects and actions that is determined by any global state. In section 5, we will be examining the feasibility of deciding computational problems on states and global states. These problems have an infinite set of possible instances of which we ask a question and expect either a "yes" or "no" answer. They are usually called decision problems and we shall precisely see how hard it is to solve them. We assume in this respect some familiarity with computational complexity, especially with the relations between complexity classes and the tower of class inclusions: $L \subseteq NL \subseteq P \subseteq NP \subseteq PSPACE$. Readers wanting more details may refer to Papadimitriou [11].

2 States

The purpose of access control is to limit the actions on objects carried out by users during the sessions they participate to. With role-based access control, a strict control over users' actions is maintained by way of roles and permissions. Roles are played by users during the duration of sessions whereas permissions are concerned by objects during the execution of actions. The possibility for a user to legally carry out such-and-such an action on some object during such-and-such a session depends both on the roles associated to the user with respect to that session and on the permissions associated to the object with respect to that action. Section 4 will explore the many-to-many relationships among roles, users and sessions or permissions, objects and actions. To characterize the connection between roles and permissions, we present, in this section, the concept of state. A state $\sigma = (R, P, have)$ has three components:

- A nonempty set R of roles with typical member denoted r, r' etc, possibly with subscripts,
- A nonempty set P of permissions with typical member denoted p, p' etc, possibly with subscripts,
- A binary relation $have$ between roles and permissions.

It can be seen as a matrix whose rows are indexed by roles, i.e. positions, and whose columns are indexed by permissions, i.e. privileges. We assume that R and P are finite sets. For role r and permission p, the relation $have(r, p)$ means role r possesses permission p or permission p is possessed by role r. For technical reasons, we assume that R and P have no common elements. With the binary relation $have$, roles correspond to sets of permissions whereas permissions correspond to sets of roles, seeing that any role r is implicitly associated to the set $have(r) = \{p$: p in P and $have(r, p)\}$ of permissions and any permission p is implicitly associated to the set $have^{-1}(p) = \{r$: r in R and $have(r, p)\}$ of roles.

3 Global states

With role-based access, the possibility for a user to legally carry out such-and-such an action on some object during such-and-such a session depends both on the roles associated to the user with respect to that session and on the permissions associated to the object with respect to that action. In states, roles and permissions are treated as non-interpreted symbols. Through the concept of global state, they have nevertheless the same status as sets of ordered pairs, seeing that roles are played by users during the duration of sessions and permissions are concerned by objects during the execution of actions. Though the same user can intervene in many sessions during the duration of which it plays one or more roles, we believe that the same session can involve different users. Though the same object can be under the effects of different actions during the execution of which it is concerned by one or more permissions, we believe that the same action can have an effect on different objects. To synthetize these ideas, we present, in this section, the concept of global state. A global state $\gamma = (\sigma, U, S, O, A, play, concern)$ has seven components:

- A state $\sigma = (R, P, have)$,
- A nonempty set U of users with typical member denoted u, u' etc, possibly with subscripts,
- A nonempty set S of sessions with typical member denoted s, s' etc, possibly with subscripts,
- A nonempty set O of objects with typical member denoted o, o' etc, possibly with subscripts,
- A nonempty set A of actions with typical member denoted a, a' etc, possibly with subscripts,
- A ternary relation $play$ between roles, users and sessions,
- A ternary relation $concern$ between permissions, objects and actions.

We assume that U, S O and A are finite sets. For role r, user u and session s, the relation $play(r, u, s)$ means role r is played by user u during the duration of session s. For permission p, object o and action a, the relation $concern(p, o, a)$ means permission p is concerned by object o during the execution of action a. A user is an active entity such as a human being or a robot whereas an object is a passive entity such as a file or a directory. Sessions are the frameworks in which users play roles and actions are the processes in which objects concern permissions. For technical reasons, we assume that R, P, U, S, O and A have no common elements. As such, roles are the means to name the many-to-many relationships among users and sessions whereas permissions are the means to name the many-to-many relationships among objects and actions. There are many practical implementations where the same role is played by several users during the duration of multifarious sessions whereas the same permission is concerned by one or more objects during the execution of numerous actions. Just as the same user can intervene in different sessions, the same session can involve different users. Similarly, just as the same object can be under the effects of different actions, the same action can have an effect on different objects. We now shall consider more closely the ways in which roles, users and sessions or permissions, objects and actions can be related in a global state.

4 $play$ relations and $concern$ relations

We are now interested in the implicit information that relates roles, users and sessions or permissions, objects and actions within a global state $\gamma = (R, P, have, U, S, O, A, play, concern)$. This implicit information is determined by the ternary relations $play$ and $concern$:

Roles and users: $play^{\gamma}_{RU}(r, u)$, role r is played by user u, iff there exists s in S such that $play(r, u, s)$,

Permissions and objects: $concern^{\gamma}_{PO}(p, o)$, permission p is concerned by object o, iff there exists a in A such that $concern(p, o, a)$,

Roles and sessions: $play^{\gamma}_{RS}(r,s)$, role r is played during the duration of session s, iff there exists u in U such that $play(r,u,s)$,

Permissions and actions: $concern^{\gamma}_{PA}(p,a)$, permission p is concerned during the execution of action a, iff there exists o in O such that $concern(p,o,a)$,

Users and sessions: $play^{\gamma}_{US}(u,s)$, user u intervenes in session s, iff there exists r in R such that $play(r,u,s)$,

Objects and actions: $concern^{\gamma}_{OA}(o,a)$, object o is under the effects of action a, iff there exists p in P such that $concern(p,o,a)$.

It is easy to prove the following lemmas:

Lemma 1 *Let r be in R, u be in U and s be in S. Then:*

- *If $play^{\gamma}_{RU}(r,u)$ then there exists s' in S such that $play^{\gamma}_{RS}(r,s')$ and $play^{\gamma}_{US}(u,s')$,*
- *If $play^{\gamma}_{RS}(r,s)$ then there exists u' in U such that $play^{\gamma}_{RU}(r,u')$ and $play^{\gamma}_{US}(u',s)$,*
- *If $play^{\gamma}_{US}(u,s)$ then there exists r' in R such that $play^{\gamma}_{RU}(r',u)$ and $play^{\gamma}_{RS}(r',s)$.*

Lemma 2 *Let p be in P, o be in O and a be in A. Then:*

- *If $concern^{\gamma}_{PO}(p,o)$ then there exists a' in A such that $concern^{\gamma}_{PA}(p,a')$ and $concern^{\gamma}_{OA}(o,a')$,*
- *If $concern^{\gamma}_{PA}(p,a)$ then there exists o' in O such that $concern^{\gamma}_{PO}(p,o')$ and $concern^{\gamma}_{OA}(o',a)$,*
- *If $concern^{\gamma}_{OA}(o,a)$ then there exists p' in P such that $concern^{\gamma}_{PO}(p',o)$ and $concern^{\gamma}_{PA}(p',a)$.*

Lemmas 1 and 2 motivate the following definitions. A role-state will be any structure $(R,U,S,$ $play_{RU},play_{RS},play_{US})$ where R, U and S are nonempty sets and $play_{RU}$ is a binary relation on R and U, $play_{RS}$ is a binary relation on R and S and $play_{US}$ is a binary relation on U and S subject to the conditions of lemma 1. A permission-state will be any structure $(P,O,$ $A,concern_{PO},concern_{PA},concern_{OA})$ where P, O and A are nonempty sets and $concern_{PO}$ is a binary relation on P and O, $concern_{PA}$ is a binary relation on P and A and $concern_{OA}$ is a binary relation on O and A subject to the conditions of lemma 2. Every role-state $\rho = (R,U,S,play_{RU},play_{RS},play_{US})$ contains some implicit information between roles, users and sessions. This implicit information is determined by the binary relations $play_{RU}$, $play_{RS}$ and $play_{US}$:

Roles, users and sessions: $play^{\rho}(r,u,s)$ iff $play_{RU}(r,u)$, $play_{RS}(r,s)$ and $play_{US}(u,s)$.

It follows immediately from the definition that:

Lemma 3 *Let r, r' be in R, u, u' be in U and s, s' be in S. If $play^{\rho}(r,u,s')$, $play^{\rho}(r,u',s)$ and $play^{\rho}(r',u,s)$ then $play^{\rho}(r,u,s)$.*

As well, every permission-state $\pi = (P,O,A,concern_{PO},$ $concern_{PA},concern_{OA})$ contains some implicit information between permissions, objects and actions. This implicit information is determined by the binary relations $concern_{PO}$, $concern_{PA}$ and $concern_{OA}$:

Permissions, objects and actions: $concern^{\pi}(p,o,a)$ iff $concern_{PO}(p,o)$, $concern_{PA}(p,a)$ and $concern_{OA}(o,a)$.

We can easily show the following:

Lemma 4 *Let p, p' be in P, o, o' be in O and a, a' be in A. If $concern^{\pi}(p,o,a')$, $concern^{\pi}(p,o',a)$ and $concern^{\pi}(p',o,a)$ then $concern^{\pi}(p,o,a)$.*

Lemmas 3 and 4 motivate the following definition. A global state $(R,P,have,U,S,O,A,play,concern)$ is said to be normal iff $play$ and $concern$ are subject to the conditions of lemmas 3 and 4. The following lemmas explain the connection between global states, role-states and permission-states.

Lemma 5 *Let $\gamma = (R,P,have,U,S,O,A,play,concern)$ be a normal global state, $r(\gamma) = (R,U,S,play^{\gamma}_{RU},$ $play^{\gamma}_{RS},play^{\gamma}_{US})$ be the role-state over γ and $p(\gamma) = (P,O,A,concern^{\gamma}_{PO},concern^{\gamma}_{PA},concern^{\gamma}_{OA})$ be the permission-state over γ. Then $play = play^{r(\gamma)}$ and $concern = concern^{p(\gamma)}$.*

Lemma 6 *Let $\rho = (R,U,S,play_{RU},play_{RS},play_{US})$ be a role-state, $\pi = (P,O,A,concern_{PO},concern_{PA},$ $concern_{OA})$ be a permission-state and $\mathfrak{g}(\rho,\pi) = (R,P,have,U,S,O,A,play^{\rho},concern^{\pi})$ be a global state over ρ and π. Then $play_{RU} = play^{g(\rho,\pi)}_{RU}$, $play_{RS} = play^{g(\rho,\pi)}_{RS}$, $play_{US} = play^{\mathfrak{g}(\rho,\pi)}_{US}$, $concern_{PO} =$ $concern^{g(\rho,\pi)}_{PO}$, $concern_{PA} = concern^{g(\rho,\pi)}_{PA}$ and $concern_{OA} = concern^{g(\rho,\pi)}_{OA}$.*

There is no unique mathematical definition of what global states should be. Special attention here has been given to systems of relational type in which the information is represented by ternary relations or by binary relations. In lemmas 5 and 6 we have established a kind of duality between normal global states, on one hand, and role-states and permission-states, on the other hand. Hence role-states and permission-states can be considered as counterparts of normal global states. The main drawback is that there are many global states γ that are not isomorphic to any global states $\mathfrak{g}(r(\gamma),p(\gamma))$ defined over their associated role-state $r(\gamma)$ and permission-state $p(\gamma)$. By lemma 5, such global states are non normal. In reference models for role-based access control described by recent studies [4, 6], the information is usually represented by binary relations. Seeing that there is no real justification to impose the normality condition on global states, we believe that systems in which the information is represented by ternary relations are more suitable for characterizing the links between roles, users and sessions or permissions, objects and actions than systems in which the information is represented by binary relations.

5 A decision problem

Let us consider the decision problem PLAY BETWEEN ROLES AND USERS: given a global state $\gamma = (R,P,have,U,S,O,A,play,concern)$, a role r and a user u, determine whether $play^{\gamma}_{RU}(r,u)$ or not. To solve it, we use the algorithm informally described below:

```
for all $s$ in $S$ do
    test whether $play(r, u, s)$
```

It is clear that this algorithm correctly solves PLAY BETWEEN ROLES AND USERS and that it can be implemented in a $\log n$ space-bounded Turing machine, seeing that positive integers are represented in binary and the length of such a representation is logarithmic in the represented number. Hence, PLAY BETWEEN ROLES AND USERS belongs to the complexity class L. It is easy to check that similar algorithms can be applied to the following decision problems as well: PLAY BETWEEN ROLES AND SESSIONS, PLAY BETWEEN USERS AND SESSIONS, CONCERN BETWEEN PERMISSIONS AND OBJECTS, CONCERN BETWEEN PERMISSIONS AND ACTIONS and CONCERN BETWEEN OBJECTS AND ACTIONS.

6 Conclusion

This paper has had as its goal the formulation of a framework for describing the actions legally carried out by users by means of an access-matrix model based on roles and permissions. Slightly departing from the frameworks investigated in role-based access control, we believe that systems in which the information is represented by ternary relations are more suitable for monitoring accesses to objects than systems in which the information is represented by binary relations. Examining the feasibility of deciding several computational problems that are concerned with states and global states, we demonstrate that our slight departure does not make things more difficult.

As for future work, we plan to study the feasibility of proving properties about the changes to the global state of a protection system modeled by a set of commands specified by sequences of primitive operations like create role r, destroy role r etc. Not surprisingly, there will be no complete decision procedure adequate for proving all elementary properties about global state transitions. Complete decision procedures, however, probably exist when constrained sets of commands are investigated like, for instance, in mono-operational protection systems [10]. Unfortunately, families of protection systems for which complete decision procedures exists constitute a relatively unknown issue altough it has been considered with a notable interest [7, 13, 14, 17]. We are currently integrating new ideas to provide families of protection systems for which the security problem is tractable.

Acknowledgments

My research is partly supported by the project "Développement de systèmes informatiques par raffinement des contraintes sécuritaires" of the action "Sécurité informatique".

References

[1] Beresnevichiene, Y.: A role and context based security model. University of Cambridge, Computer Laboratory, Technical Report **558** (2003).

[2] Bishop, M.: Computer Security: Art and Science. Addison-Wesley (2003).

[3] Denning, D.: Cryptography and Data Security. Addison-Wesley (1982).

[4] Ferraiolo, D., Barkley, J., Kuhn, D.: A role-based access control model and reference implementation within a corporate intranet. ACM Transactions on Information And System Security **2** (1999) 34–64.

[5] Ferraiolo, D., Kuhn, D., Chandramouli, R.: Role-Based Access Control. Artech House (2003).

[6] Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D., Chandramouli, R.: Proposed NIST standard for role-based access control. ACM Transactions on Information And System Security **4** (2001) 224–274.

[7] Gong, L., Qian, X.: Computational issues in secure interoperation. IEEE Transactions on Software Engineering **22** (1996) 43–52.

[8] Harrison, M.: Theoretical issues concerning protection in operating systems. Advances in Computers **24** (1985) 61–100.

[9] Harrison, M., Ruzzo, W.: Monotonic protection systems. In DeMillo, R., Dobkin, D., Jones, A., Lipton, R. (Editors): Foundations of Secure Computation. Academic Press (1978) 337–363.

[10] Harrison, M., Ruzzo, W., Ullman, J.: Protection in operating systems. Communications of the ACM **19** (1976) 461–471.

[11] Papadimitriou, C.: Computational Complexity. Addison-Wesley (1994).

[12] Pieprzyk, J., Hardjono, T., Seberry, J.: Fundamentals of Computer Security. Springer-Verlag (2003).

[13] Sandhu, R.: The schematic protection model: its definition and analysis for acyclic attenuating schemes. Journal of the ACM **35** (1988) 404–432.

[14] Sandhu, R.: Undecidability of safety for the schematic protection model with cyclic creates. Journal of Computer and System Sciences **44** (1992) 141–159.

[15] Sandhu, R.: Lattice-based access control models. Computer **26** (1993) 9–19.

[16] Sandhu, R., Coyne, E., Feinstein, H., Youman, C.: Role-based access control models. Computer **29** (1996) 38–47.

[17] Soshi, M.: Safety analysis of the dynamic-typed access matrix model. In Cuppens, F., Deswarte, Y., Gollmann, D., Waidner, M. (Editors): Computer Security — ESORICS 2000. Springer-Verlag, Lecture Notes in Computer Science **1895** (2000) 106–121.