APPLICATION OF DEONTIC LOGIC IN ROLE–BASED ACCESS CONTROL

GRZEGORZ KOŁACZEK*

* Institute of Control and Systems Engineering, Technical University of Wrocław
ul. Wybrzeże S. Wyspiańskiego 27, 50–370 Wrocław, Poland
e-mail: kolacz@ists.pwr.wroc.pl

The paper presents a short overview of the foundations of the Role-Based Access Control Modal Model and its properties. In particular, the translation of these model formulae to the first-order logic formulae in a form of Horn's clauses is analysed. The automation of processes and mechanisms related to access control on the basis of logical automated reasoning and the PROLOG language are described.

Keywords: formal logic, access control, RBAC, system security, reasoning automation

1. Introduction

The aim of access control is protection of system resources against unauthorised access. It is a process by which the use of the system resources is regulated according to the security policy (Shirey, 2000). In the contemporary information systems there are three main types of access control: Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based Access Control (RBAC). Discretionary Access Control is an access control service that enforces a security policy based on the identity of system entities and their authorisations to access system resources. It is "discretionary" in the sense that each entity might have access rights that permit the entity, by its own preference, to enable another entity to access some resources (NCSC, 1985). Mandatory Access Control is an access control service that enforces a security policy based on comparing (a) security labels (which indicate how sensitive or critical system resources are) with (b) security clearances (which indicate whether system entities are eligible to access certain resources). This type of access control is called "mandatory" because an entity that has clearance to access a resource may not, just by its own decision, enable another entity to access that resource (NCSC, 1985). Finally, Role-Based Access Control is a form of identity-based access control where the system entities that are identified and controlled are functional positions in an organisation (Sandhu *et al.*, 1994).

In the area of system security, as well as in access control, an important topic is the global security and evaluation of security functions. The latest set of standards for evaluating information technology products and systems is included in the document called "The Common Criteria". This document specifies seven evaluation assurance levels, where the highest level of assurance is called "formally verified designed and tested". In the context of "The Common Criteria", the system should be supported by formal tools that would guarantee the formal specification and verification of system security requirements (CCIB, 1999).

Mandatory and Discretionary Access Control mechanisms are supported by several well-known and tested formal models like Bell La-Padula (Denning, 1982; Sandhu, 1992) while models for Role-Based Access Control are still being developed and verified. The existing propositions are incomplete or do not provide the required functionality (Barkley *et al.*, 1997; Chen and Sandhu, 1996; Ferraiolo and Barkley, 1997; Sandhu 1996; 1997; 1998; Sandhu *et al.*,1997; 1999).

The aim of this paper is to present the foundations and properties of a new formal model for Role-Based Access Control. The novelty of the proposition is the application of deontic logic as a language for description of access control policies. Its consequence is the ability to automate implementation of the security policy.

2. Role-Based Access Control Modal Model

The first step required by all access control policies is the identification of a set of entities that may be active within the system and a set of activities. During the next steps, on the basis of the system security policy, relations between the elements of these two sets should be established.

Let us denote by $E = \{\mathrm{entity}_1, \mathrm{entity}_2, \dots, \mathrm{entity}_n\}$ the set of entities, and by $A = \{\mathrm{action}_1, \mathrm{action}_2, \dots, \mathrm{action}_m\}$ the set of their activities. There are three possibilities for each $\mathrm{action}_k \in A$ in relation to entities from the set E:

$$\mathrm{action}_k \text{ is permitted,} \tag{1}$$

$$\mathrm{action}_k \text{ is obliged,} \tag{2}$$

$$\mathrm{action}_k \text{ is forbidden.} \tag{3}$$

In deontic logic it is possible to describe this relation using the modal operators: $\boldsymbol{P}$ *– it is permitted,* $\boldsymbol{O}$ *– it is obliged* and $\boldsymbol{F}$ *– it is forbidden*. According to these operators, the sentences (1)–(3) can be formulated in the following way:

$$\boldsymbol{P}\,\mathrm{action}_k, \tag{4}$$

$$\boldsymbol{O}\,\mathrm{action}_k, \tag{5}$$

$$\boldsymbol{F}\,\mathrm{action}_k. \tag{6}$$

The formalism of deontic logic is useful for access control because its basic notions are also fundamental for the access control policy that describes what is permitted, obligatory and forbidden for a particular entity within the system area. The application of deontic logic in the process of access control allows a formal description and a formal analysis of the above-mentioned notions. The first attempt to build a formal theory of normative concepts (permission, obligation, prohibition) was made by Mally (1926), but most of the contemporary interest in deontic logic has been stimulated by von Wright's paper 'Deontic Logic' (von Wright, 1951).

The formal model using deontic logic for role-based access control is composed of three parts (Kołaczek, 2001):

(a) *Syntax of the model language*. It is based on the first-order logic syntax where three additional modal operators are added: $\boldsymbol{P}$, $\boldsymbol{O}$, $\boldsymbol{F}$.

(b) *Semantic of the model language*. It is based on the Krippke semantic of possible world where the world accessibility relation is serial.

(c) *The language application rules*:

- access permissions, obligations, prohibitions and access request are formulated in the language of the model,
- all the formulae used by the access control mechanisms must be in the form of Horn's clauses,
- if Reg is a set of formulae describing permitted, prohibited and obligatory activities and this set is defined for a particular entity (entity_k), then this entity may perform all activities described by the formulae that are the logical consequences of the set Reg.

3. Translation of Modal Formulae to Conjunctions of Horn Clauses

There are several tools that support the automation of reasoning in the first-order logic. One of them is PROLOG that uses Horn's clauses and the resolution method. This means that the ability to translate formulae of the Role-Based Access Control Modal Model into first-order formulae in the form of Horn's clauses would open the application of PROLOG and the resolution method also for access control and the access management process.

The following theorem states that it is possible to translate a particular class of Role-Based Access Control Modal Model formulae into a form of the first-order Horn clauses. This theorem makes use of the definition of a semi-functional translation.

The semi-functional translation (T_{sf}) of a modal logic is a projection that assigns modal formulae and possible worlds to formulae of the first-order logic in the following way (Bolc *et al.*, 1995; 1998):

$$T_{\mathrm{sf}}(\phi, x) = P(x),$$

where ϕ is an atomic proposition and P is the corresponding predicate;

$$T_{\mathrm{sf}}(\boldsymbol{O}\phi, x) = \forall\, y \big[R(x,y) \rightarrow T_{\mathrm{sf}}(\phi, y)\big],$$

where R is a possible world accessibility relation;

$$T_{\mathrm{sf}}(\boldsymbol{P}\phi, x) = \exists\, f \big[T_{\mathrm{sf}}(\phi, f(x))\big],$$

where f is a function corresponding to the relation of possible world accessibility.

Theorem 1. $T_{\mathrm{sf}}(\phi, w)$ *is a conjunction of Horn's clauses iff a formula obtained after deleting all modal operators from the formula* f *is a conjunction of Horn's clauses, where:* ϕ *is a formula of the Role-Based Access Control Modal Model,* $T_{\mathrm{sf}}(\phi, w)$ *means a semi-functional translation of* ϕ*, and* w *stands for a world selected from a set of possible worlds (the Krippke model).*

Proof. The proof of this theorem is based on the structural induction. From the definition of the semi-functional translation it is known that:

> The semi-functional translation $T_{\mathrm{sf}}(\phi, w)$ preserves all classical quantifiers and conjunctions, e.g. $T_{\mathrm{sf}}(\neg a, x) = \neg T_{\mathrm{sf}}(a, x)$, $T_{\mathrm{sf}}(a \vee b, x)$, $T_{\mathrm{sf}}(a, x) \vee T_{\mathrm{sf}}(b, x)$, etc. (7)

> The number of positive literals in $T_{\mathrm{sf}}(\phi, x)$ is equal to the number of positive literals in formula ϕ. (8)

Step 1. The proof for the formulae of type: ϕ, $\boldsymbol{O}\phi$, $\boldsymbol{P}\phi$. Let ϕ be a literal. Then:

- ϕ: it is the form of a conjunction of Horn's clauses,
- $\boldsymbol{O}\phi$: after deleting the modal operator, the formula $\boldsymbol{O}\phi$ is reduced to ϕ and so it is in the form of a conjunction of Horn's clauses,
- $\boldsymbol{P}\phi$: the same as in the case of the operator $\boldsymbol{O}$.

Lemma 1. *If after deleting the modal operators the formulae f, $\boldsymbol{O}\phi$ and $\boldsymbol{P}\phi$ are in the form of conjunctions of Horn's clauses, then $T_{\mathrm{sf}}(\phi, x)$, $T_{\mathrm{sf}}(\boldsymbol{O}\phi, x)$ and $T_{\mathrm{sf}}(\boldsymbol{P}\phi, x)$ are in the form of conjunctions of Horn's clauses.*

Proof of Lemma 1. According to the definition of the semi-functional translation, the following sentences are true:

(a) $T_{\mathrm{sf}}(\phi, x) = P(x)$ is in the form of a conjunction of Horn's clauses,

(b) $T_{\mathrm{sf}}(\boldsymbol{O}\phi, x) = \forall\, y[R(x,y) \to T_{\mathrm{sf}}(\phi, y)] = \forall\, y[\neg R(x,y) \vee T_{\mathrm{sf}}(\phi, y)] = \forall\, y[\neg R(x,y) \vee P(y)]$ is in the form of a conjunction of Horn's clauses,

(c) $T_{\mathrm{sf}}(\boldsymbol{P}\phi, x) = \exists\, f[T_{\mathrm{sf}}(\phi, f(x))] = \exists\, f P(f(x))$ is in the form of a conjunction of Horn's clauses.

■

Lemma 2. *If after deleting the modal operators formulae ϕ, $\boldsymbol{O}\phi$ and $\boldsymbol{P}\phi$ are not in the form of conjunctions of Horn's clauses, then $T_{\mathrm{sf}}(\phi, x)$, $T_{\mathrm{sf}}(\boldsymbol{O}\phi, x)$ and $T_{\mathrm{sf}}(\boldsymbol{P}\phi, x)$ are not in the form of conjunctions of Horn's clauses.*

Proof of Lemma 2. Because ϕ is a literal, it is always a Horn's clause, so there is a contradiction and this case need not be considered any further. ■

Step 2. The proof for the formulae of type: $\boldsymbol{O}\phi \to \psi$, $\psi \to \boldsymbol{O}\phi$, $\psi \wedge \boldsymbol{O}\phi$, $\psi \vee \boldsymbol{O}\phi$, $\boldsymbol{P}\phi \to \psi$, $\psi \to \boldsymbol{P}\phi$, $\psi \wedge \boldsymbol{P}\phi$, $\psi \vee \boldsymbol{P}\phi$.

Let ψ be a complex formula for which the following is true:

$T_{\mathrm{sf}}(\psi, x)$ is in the form of a conjunction of Horn's clauses iff after deleting all modal operators from ψ, it is in the form of a conjunction of Horn's clauses. (9)

Furthermore, let ϕ be a literal. (10)

Lemma 3. *If after deleting modal operators the formulae $\boldsymbol{O}\phi \to \psi$, $\psi \to \boldsymbol{O}\phi, \dots$ are in the form of conjunctions of Horn's clauses, then $T_{\mathrm{sf}}(\boldsymbol{O}\phi \to \psi, x)$, $T_{\mathrm{sf}}(\psi \to \boldsymbol{O}\phi, x), \dots$ are in the form of conjunctions of Horn's clauses.*

Let us assume that after deleting the modal operators from the formulae

$$\begin{aligned} &\boldsymbol{O}\phi \to \psi,\ \psi \to \boldsymbol{O}\phi,\ \psi \wedge \boldsymbol{O}\phi,\ \psi \vee \boldsymbol{O}\phi, \\ &\boldsymbol{P}\phi \to \psi,\ \psi \to \boldsymbol{P}\phi,\ \psi \wedge \boldsymbol{P}\phi,\ \psi \vee \boldsymbol{P}\phi, \end{aligned} \tag{11}$$

they are in the form of Horn's clauses.

Proof of Lemma 3.

(a) After deleting the modal operators, $\psi \vee \boldsymbol{O}\phi$ is reduced to the formula $\psi \vee \phi$,

$$\begin{aligned} T_{\mathrm{sf}}(\psi \vee \boldsymbol{O}\phi, x) &= T_{\mathrm{sf}}(\psi, x) \vee T_{\mathrm{sf}}(\boldsymbol{O}\phi, x) \\ &= T_{\mathrm{sf}}(\psi, x) \vee \forall\, y\big[\neg R(x,y) \vee P(y)\big]. \end{aligned}$$

Let ψ be in a conjunction normal form, so that

$$\psi = K_1 \wedge K_2 \wedge \dots \wedge K_n, \tag{12}$$

$$\psi \vee \phi = (K_1 \wedge K_2 \wedge \dots \wedge K_n) \vee \phi, \tag{13}$$

$$\psi \vee \phi = (K_1 \vee \phi) \wedge (K_2 \vee \phi) \wedge \dots \wedge (K_n \vee \phi), \tag{14}$$

where $K_1, K_2, \dots, K_n$ are clauses.

According to (11), the formulae $(K_1 \vee \phi), (K_2 \vee \phi), \dots, (K_n \vee \phi)$ must be Horn's clauses. On the other hand, from (7) it follows that

$$\begin{aligned} T_{\mathrm{sf}}(\psi \vee \boldsymbol{O}\phi, x) &= T_{\mathrm{sf}}(\psi, x) \vee T_{\mathrm{sf}}(\boldsymbol{O}\phi, x) \\ &= T_{\mathrm{sf}}(K_1 \wedge K_2 \wedge \dots \wedge K_n, x) \vee T_{\mathrm{sf}}(\boldsymbol{O}\phi, x) \\ &= \big(T_{\mathrm{sf}}(K_1, x) \wedge T_{\mathrm{sf}}(K_2, x) \wedge \dots \wedge T_{\mathrm{sf}}(K_n, x)\big) \\ &\quad \vee T_{\mathrm{sf}}(\boldsymbol{O}\phi, x) \\ &= \big(T_{\mathrm{sf}}(K_1, x) \vee T_{\mathrm{sf}}(\boldsymbol{O}\phi, x)\big) \wedge \big(T_{\mathrm{sf}}(K_2, x) \\ &\quad \vee T_{\mathrm{sf}}(\boldsymbol{O}\phi, x)\big) \\ &\quad \wedge \dots \wedge \big(T_{\mathrm{sf}}(K_n, x) \vee T_{\mathrm{sf}}(\boldsymbol{O}\phi, x)\big). \end{aligned} \tag{15}$$

From (7), (8) and (12) we conclude that the formulae $T_{\mathrm{sf}}(K_1, x), T_{\mathrm{sf}}(K_2, x), \dots, T_{\mathrm{sf}}(K_n, x)$ are clauses with the same number of positive literals as the formulae $K_1, K_2, \dots, K_n$. Because $T_{\mathrm{sf}}(\boldsymbol{O}\phi, x) = \forall\, y[\neg R(x,y) \vee P(y)]$ is a clause with only one positive literal, from (15) and (14) we get that (15) is also a conjunction of Horn's clauses and, finally, so is $T_{\mathrm{sf}}(\psi \vee \boldsymbol{O}\phi, x)$.

(b) After deleting the modal operators, $\psi \wedge \boldsymbol{O}\phi$ is reduced to the formula $\psi \wedge \phi$,

$$\begin{aligned} T_{\mathrm{sf}}(\psi \wedge \boldsymbol{O}\phi, x) &= T_{\mathrm{sf}}(\psi, x) \wedge T_{\mathrm{sf}}(\boldsymbol{O}\phi, x) \\ &= T_{\mathrm{sf}}(\psi, x) \wedge \forall\, y\big[\neg R(x,y) \vee P(y)\big]. \end{aligned}$$

Because the semi-functional translation of the formula $\psi \wedge \boldsymbol{O}\phi$ is a conjunction of two elements and both of them are in the form of conjunctions of Horn's clauses, $T_{\rm sf}(\psi \wedge \boldsymbol{O}\phi, x)$ is also in the form of a conjunction of Horn's clauses.

(c) After deleting the modal operators, $\boldsymbol{O}\phi \rightarrow \psi$ is reduced to the formula $\phi \rightarrow \psi \equiv \psi \vee \neg\phi$,

$$\begin{aligned}
&T_{\rm sf}(\boldsymbol{O}\phi \rightarrow \psi, x)\\
&\quad = T_{\rm sf}(\neg\boldsymbol{O}\phi \vee \psi, x)\\
&\quad = T_{\rm sf}(\boldsymbol{P}\neg\phi \vee \psi, x)\\
&\quad = T_{\rm sf}(\boldsymbol{P}\neg\phi, x) \vee T_{\rm sf}(\psi, x)\\
&\quad = \exists\, f T_{\rm sf}\big(\neg\phi, f(x)\big) \vee T_{\rm sf}(\psi, x)\\
&\quad = \exists\, f \neg T_{\rm sf}\big(\phi, f(x)\big) \vee T_{\rm sf}(\psi, x)\\
&\quad = \exists\, f \neg P\big(f(x)\big) \vee T_{\rm sf}(\psi, x).
\end{aligned}$$

Since $\phi \rightarrow \psi \equiv \psi \vee \neg\phi$, this is an instance of an alternative to Lemma 3.

Following the reasoning from Lemma 3, we can get the equations

$$\psi \vee \neg\phi = (K_1 \vee \neg\phi) \wedge (K_2 \vee \neg\phi) \wedge \cdots \wedge (K_n \vee \neg\phi) \tag{16}$$

and

$$\begin{aligned}
&T_{\rm sf}(\boldsymbol{O}\phi \rightarrow \psi, x)\\
&\quad = T_{\rm sf}(\psi \vee \neg\boldsymbol{O}\phi, x)\\
&\quad = \big(T_{\rm sf}(K_1, x) \vee \neg T_{\rm sf}\big(\phi, f(x)\big)\big)\\
&\qquad \wedge \big(T_{\rm sf}(K_2, x) \vee \neg T_{\rm sf}\big(\phi, f(x)\big)\big)\\
&\qquad \wedge \cdots \wedge \big(T_{\rm sf}(K_n, x) \vee \neg T_{\rm sf}\big(\phi, f(x)\big)\big).
\end{aligned}\tag{17}$$

According to (11), the formula (16) is a conjunction of Horn's clauses. Because each element of the conjunction in the formula (17) has the same number of positive and negative literals as the elements of the formula (16), $T_{\rm sf}(\boldsymbol{O}\phi \rightarrow \psi, x)$ is also in the form of a conjunction of Horn's clauses.

(d) After deleting the modal operators, $\psi \rightarrow \boldsymbol{O}\phi$ is reduced to the formula $\psi \rightarrow \phi$,

$$\begin{aligned}
T_{\rm sf}(\psi \rightarrow \boldsymbol{O}\phi, x) &= T_{\rm sf}(\psi, x) \rightarrow T_{\rm sf}(\boldsymbol{O}\phi, x)\\
&= T_{\rm sf}(\psi, x) \rightarrow \forall\, y\big[\neg R(x, y) \vee P(y)\big]\\
&= \neg T_{\rm sf}(\psi, x) \vee \forall\, y\big[\neg R(x, y) \vee P(y)\big].
\end{aligned}$$

This case can be reduced to an alternative of formulae according to $\psi \rightarrow \phi \equiv \neg\psi \vee \phi$, cf. Lemma 3. ■

Lemma 4. *If after deleting the modal operators the formulae $\boldsymbol{O}\phi \rightarrow \psi$, $\psi \rightarrow \boldsymbol{O}\phi, \ldots$ are not in the form of Horn's clauses, then $T_{\rm sf}(\boldsymbol{O}\phi \rightarrow \psi, x), T_{\rm sf}(\psi \rightarrow \boldsymbol{O}\phi, x), \ldots$ are not in the form of conjunctions of Horn's clauses.*

Assume that after deleting the modal operators, the formulae

$$\begin{array}{llll}
\boldsymbol{O}\phi \rightarrow \psi, & \psi \rightarrow \boldsymbol{O}\phi, & \psi \wedge \boldsymbol{O}\phi, & \psi \vee \boldsymbol{O}\phi,\\
\boldsymbol{P}\phi \rightarrow \psi, & \psi \rightarrow \boldsymbol{P}\phi, & \psi \wedge \boldsymbol{P}\phi, & \psi \vee \boldsymbol{P}\phi
\end{array}\tag{18}$$

are not in the form of conjunctions of Horn's clauses.

Proof of Lemma 4.

(a) After deleting the modal operators, $\psi \vee \boldsymbol{O}\phi$ is reduced to the formula $\psi \vee \phi$, and

$$\begin{aligned}
T_{\rm sf}(\psi \vee \boldsymbol{O}\phi, x) &= T_{\rm sf}(\psi, x) \vee T_{\rm sf}(\boldsymbol{O}\phi, x)\\
&= T_{\rm sf}(\psi, x) \vee \forall\, y\big[\neg R(x, y) \vee P(y)\big].
\end{aligned}$$

Let ψ be in a conjunction normal form, so that

$$\psi = K_1 \wedge K_2 \wedge \cdots \wedge K_n, \tag{19}$$

$$\psi \vee \phi = (K_1 \wedge K_2 \wedge \cdots \wedge K_n) \vee \phi, \tag{20}$$

$$\psi \vee \phi = (K_1 \vee \phi) \wedge (K_2 \vee \phi) \wedge \cdots \wedge (K_n \vee \phi), \tag{21}$$

where $K_1, K_2, \ldots, K_n$ are clauses.

According to (18), at least one of the formulae $(K_1 \vee \phi), (K_2 \vee \phi), \ldots, (K_n \vee \phi)$ is not a Horn clause.

On the other hand, we have

$$\begin{aligned}
&T_{\rm sf}(\psi \vee \boldsymbol{O}\phi, x) = T_{\rm sf}(\psi, x) \vee T_{\rm sf}(\boldsymbol{O}\phi, x)\\
&\quad = T_{\rm sf}(K_1 \wedge K_2 \wedge \cdots \wedge K_n, x) \vee T_{\rm sf}(\boldsymbol{O}\phi, x)\\
&\quad = \big(T_{\rm sf}(K_1, x) \wedge T_{\rm sf}(K_2, x)\\
&\qquad \wedge \cdots \wedge T_{\rm sf}(K_n, x)\big) \vee T_{\rm sf}(\boldsymbol{O}\phi, x)\\
&\quad = \big(T_{\rm sf}(K_1, x) \vee T_{\rm sf}(\boldsymbol{O}\phi, x)\big)\\
&\qquad \wedge \big(T_{\rm sf}(K_2, x) \vee T_{\rm sf}(\boldsymbol{O}\phi, x)\big)\\
&\qquad \wedge \cdots \wedge \big(T_{\rm sf}(K_n, x) \vee T_{\rm sf}(\boldsymbol{O}\phi, x)\big).
\end{aligned}\tag{22}$$

From (7), (8) and (19) it follows that the formulae $T_{\rm sf}(K_1, x), T_{\rm sf}(K_2, x), \ldots, T_{\rm sf}(K_n, x)$ are clauses with the same number of positive literals as the formulae $K_1, K_2, \ldots, K_n$. Then from (22) and (21) we get that (22) is not a conjunction of Horn's clauses and, finally, neither is $T_{\rm sf}(\psi \vee \boldsymbol{O}\phi, x)$.

(b) After deleting the modal operators, $\psi \vee \boldsymbol{O}\phi$ is reduced to the formula $\psi \wedge \phi$, and

$$\begin{aligned}
T_{\rm sf}(\psi \wedge \boldsymbol{O}\phi, x) &= T_{\rm sf}(\psi, x) \wedge T_{\rm sf}(\boldsymbol{O}\phi, x)\\
&= T_{\rm sf}(\psi, x) \wedge \forall\, y\big[\neg R(x, y) \vee P(y)\big].
\end{aligned}$$

The formula $\psi \wedge \phi$ is not in the form of a conjunction of Horn's clauses iff ψ is not in such a form. Because, from (9), $T_{\text{sf}}(\psi, x)$ is not in the form of a conjunction of Horn's clauses, neither is $T_{\text{sf}}(\psi \wedge \boldsymbol{O}\phi, x) = T_{\text{sf}}(\psi, x) \wedge T_{\text{sf}}(\boldsymbol{O}\psi, x)$.

(c) After deleting the modal operators, $\boldsymbol{O}\phi \rightarrow \psi$ is reduced to the formula $\phi \rightarrow \phi$, and

$$\begin{aligned}
&T_{\text{sf}}(\boldsymbol{O}\phi \rightarrow \psi, x)\\
&\quad = T_{\text{sf}}(\neg\boldsymbol{O}\phi \vee \psi, x)\\
&\quad = T_{\text{sf}}(\boldsymbol{P}\neg\phi \vee \psi, x)\\
&\quad = T_{\text{sf}}(\boldsymbol{P}\neg\phi, x) \vee T_{\text{sf}}(\psi, x)\\
&\quad = \exists\, f T_{\text{sf}}\big(\neg\phi, f(x)\big) \vee T_{\text{sf}}(\psi, x)\\
&\quad = \exists\, f \neg T_{\text{sf}}\big(\phi, f(x)\big) \vee T_{\text{sf}}(\psi, x)\\
&\quad = \exists\, f \neg P\big(f(x)\big) \vee T_{\text{sf}}(\psi, x).
\end{aligned}$$

Since $\phi \rightarrow \psi \equiv \psi \vee \neg\phi$, this is a particular instance of an alternative to Lemma 4.

On the analogy of the reasoning from Lemma 4, we get the equations

$$\psi \vee \neg\phi = (K_1 \vee \neg\phi) \wedge (K_2 \vee \neg\phi) \wedge \cdots \wedge (K_n \vee \neg\phi), \quad (23)$$

$$\begin{aligned}
&T_{\text{sf}}(\boldsymbol{O}\phi \rightarrow \psi, x)\\
&\quad = \Big(T_{\text{sf}}(K_1, x) \vee \neg T_{\text{sf}}\big(\phi, f(x)\big)\Big)\\
&\qquad \wedge \Big(T_{\text{sf}}(K_2, x) \vee \neg T_{\text{sf}}\big(\phi, f(x)\big)\Big)\\
&\qquad \wedge \cdots \wedge \Big(T_{\text{sf}}(K_n, x) \vee \neg T_{\text{sf}}\big(\phi, f(x)\big)\Big). \quad (24)
\end{aligned}$$

According to (18), the formula (23) is not a conjunction of Horn's clauses. Because each element of the conjunction in the formula (24) has the same number of positive and negative literals as the elements of the formula (23), $T_{\text{sf}}(\boldsymbol{O}\phi \rightarrow \psi, x)$ is not in the form of a conjunction of Horn's clauses.

(d) After deleting the modal operators, $\psi \rightarrow \boldsymbol{O}\phi$ is reduced to the formula $\psi \rightarrow \phi$, and

$$\begin{aligned}
&T_{\text{sf}}(\psi \rightarrow \boldsymbol{O}\phi, x)\\
&\quad = T_{\text{sf}}(\psi, x) \rightarrow T_{\text{sf}}(\boldsymbol{O}\phi, x)\\
&\quad = T_{\text{sf}}(\psi, x) \rightarrow \forall\, y\big[\neg R(x, y) \vee P(y)\big]\\
&\quad = \neg T_{\text{sf}}(\psi, x) \vee \forall\, y\big[\neg R(x, y) \vee P(y)\big].
\end{aligned}$$

This case can be reduced to an alternative of formulae according to the equality $\psi \rightarrow \phi \equiv \neg\psi\varepsilon\phi$, cf. Lemma 4. ■

The proof of Theorem 1 for a dual modal operator $\boldsymbol{P}$ is analogous to the proof presented above. ■

4. Applications of the Model

A complete access control system should support several access control processes. In particular, it should support access control policy derivation from a set of higher-level procedures, verification of the policy consistency and validation of access requests. Additionally, access control systems should support mechanisms related to a particular access control method (Discretionary Access Control, Mandatory Access Control, Role-Based Access Control).

In this context, the Role-Based Access Control Modal Model constitutes a basis for description of access control policies, and for evaluation and automation of access control decisions.

The developers of Role-Based Access Control have distinguished several mechanisms to control access according to the system's and organisational roles. There are three main categories of these mechanisms, which are responsible for:

- definitions of roles,
- definitions of role-entity relations, and
- definitions role-role relations.

The RBAC Modal Model described in this paper and the related possibility of translating formulae from the deontic language of the Role-Based Access Control Modal Model into formulae of first-order logic in the form of Horn's clauses allow application of automated reasoning methods for access control purposes. The proposed model operates on the formulae in the form of Horn's clauses, so PROLOG is an appropriate tool for reasoning automation.

4.1. Example

The security policy in a system with RBAC is described by an identified and defined set of roles. Each subject active within the system area can be assigned to one or more roles, and it gets the authorisation to the set of actions that is a logical consequence of its set of roles.

In RMM the roles are defined by logical formulae. For example, let the role Role_1 be assigned to the subject Subject_1. Role_1 is defined by the following two formulae:

Role_1:

$$\begin{aligned}
&\forall\ \text{pd}\ \forall\ \text{pl}\ \ \text{Range}(\text{pl}, \text{Directory\_A}, \text{Directory\_B})\\
&\quad \wedge \text{Plays}(\text{pd}, \text{Assistant}) \rightarrow \boldsymbol{P}\text{Read}(\text{pd}, \text{pl}),
\end{aligned}$$

$$\begin{aligned}
&\forall\ \text{pd}\ \ \text{Position}(\text{pd}, \text{Admin})\\
&\quad \rightarrow \neg\boldsymbol{P}\text{Add\_role}(\text{pd}, \text{Assistant}).
\end{aligned}$$

Apart from the role definition, logical values of several system variables must be set for the current system state. For example,

$$\mathrm{Range(File\_a, Directory\_A, Directory\_B)} \equiv \text{TRUE},$$

$$\mathrm{Range(File\_b, Directory\_A, Directory\_B)} \equiv \text{FALSE},$$

$$\mathrm{Position(Subject\_1, Admin)} \equiv \text{FALSE},$$

$$\mathrm{Plays(Subject\_1, Assistant)} \equiv \text{TRUE}.$$

While the security policy is defined and the values of the system variables are known, it is possible to verify the access requests. For example, an answer to the question about the possibility to access File_a by Subject_1 can be looked for. To give an answer to this question, an appropriate logical program should be generated. The logical program is a result of semi-functional translation of the formulae defining roles and system variable values. In the example considered, the logical program is as follows:

$$\mathrm{Range(x, File\_a, Directory\_A, Directory\_B)} \Leftarrow$$

$$\Leftarrow \mathrm{Range(x, File\_b, Directory\_A, Directory\_B)}$$

$$\Leftarrow \mathrm{Position(Subject\_1, Admin)}$$

$$\mathrm{Plays(x, Subject\_1, Assistant)} \Leftarrow$$

$$R(x, f(x)) \Leftarrow$$

$$\mathrm{Read(f(x), pd, pl)} \Leftarrow \mathrm{Range(x, pl, Directory\_A,}$$

$$\mathrm{Directory\_B), Plays(x, pd, Assistant)}$$

$$\Leftarrow \mathrm{Position(x, pd, Admin), Add\_role(f(x), pd, pl)}.$$

The formula describing an access request is also translated and it is a question for the logical program *The access request* after semi-functional translation:

$$\Leftarrow \mathrm{Read(y, Subject\_1, File\_a)}.$$

The final answer of the logical program in this example will be “YES”. This means that the action requested by Subject_1 in Role_1 to read from File_a is admissible in the context of the present security policy definition.

In (Kołaczek, 2001) a precise way of the application of the Role-Based Access Control Modal Model in the process of role definitions, role-entity relations and definitions of role-role relations is indicated. Also, several examples are given illustrating how the proposed model can be used in the process of consistency verification of the defined security policy or during the authorisation of entities.

5. Conclusions

Formal description and verification is one of the most crucial requirements of the high level security. Access control is an integral part of every security policy in an information system and so it also requires an appropriate model to fulfil this requirement. Deontic logic, as it formalises the notions of obligation, prohibition and permission, corresponds in a natural way to the specificity of access control activities. The presented Role-Based Access Control Modal Model allows formal description and analysis of the access control policy and access control requests. Sufficient conditions for translation of modal formulae into first-order Horn’s clauses were presented and analysed. The form of Horn’s clauses raises a possibility of PROLOG application (or other corresponding tools for reasoning automation) in the processes of policy consistency verification, validation of access requests, and other processes related to access control.

References

Barkley J., Cincotta A., Ferraiolo D., Gavrilla S. and Kuhn R. (1997): *Role based access control for the World Wide Web*. — Proc. NIST-NSA Nat. Computer Security Conf., Baltimore, pp. 23–34.

Bolc L., Dziewicki K., Rychlik P., Szałas A. (1995): *Reasoning in Non-Classical Logic. Theoretical Basis*. — Warsaw: Akademicka Oficyna Wydawnicza PLJ.

Bolc L., Dziewicki K., Rychlik P., Szałas A. (1998): *Reasoning in Non-Classical Logic. Reasoning Automation*. — Warsaw: Akademicka Oficyna Wydawnicza PLJ.

Chen F., Sandhu R.S. (1996): *Constraints for role-based access control*. — Proc. ACM Workshop on RBAC, Gaithersburg, USA, pp. 382–390.

CCIB (1999): *Common criteria for information technology security evaluation, Ver. 2.1*. — Common Criteria Implementation Board–99–01.

Denning D.E. (1982): *Cryptography and Data Security*. — Massachusetts: Addison-Wesley.

Ferraiolo D., Barkley F. (1997): *Specifying and managing role-based access control within a corporate Intranet*. — Proc. 2nd ACM Workshop on RBAC, Fairfax, USA, pp. 69–78.

Kołaczek G. (2001): *Model of role based access control mechanism*. — Ph. D. thesis, Technical University of Wrocław, Wrocław, Poland.

Mally E. (1926): *Grundgesetze des Sollens. Elemente der Logik des Willens*. — Graz: Leuschner & Lubensky.

NCSC (1985): *Trusted Computer Security Evaluation Criteria*. — National Computer Security Centre, DOD 5200.28-STD.

Sandhu R. (1992): *Lattice-based enforcement of chinese walls*. — Comp. Security, Vol. 11, No. 8, pp. 753–763.

Sandhu R. (1996): *Role hierarchies and constraints for lattice-based access controls*. — Proc. 4-th Europ. Symp. *Research in Computer Security*, Rome, Italy, pp. 20–25.

Sandhu R. (1997): *Rationale for the RBAC96 family of access control models*. — Proc. 1st ACM Workshop *Role-Based Access Control*, Gaithersburg, USA, pp. 32–38.

Sandhu R. (1998): *Role activation hierarchies*. — Proc. 3-rd ACM Workshop *Role-Based Access Control*, Fairfax, USA, pp. 56–65.

Sandhu R, Bhamidipati V., Coyne E., Ganta S, Youman Ch. (1997): *The ARBAC97 model for role-based administration of roles: Preliminary description and outline*. — Proc. 2nd ACM Workshop *Role-Based Access Control*, Fairfax, USA, pp. 41–50.

Sandhu R, Bhamidipati V., Munawer Q. (1999): *The ARBAC97 model for role-based administration of roles*. — ACM Trans. Inf. Syst. Secur., Vol. 2, No. 1, pp. 105–135.

Sandhu R.S., Coyne E.J., Feinstein H. L., Youman Ch.E. (1994): *Role-based access control: A multi-dimensional view*. — Proc. 10-th *Annual Computer Security Application Conf.*, Greater Orlando, USA, pp. 54–62.

Shirey R. (2000): *Request for Comments 2828*. — The Internet Society, available at `http://www.rfceditor.org.rfc.html`

von Wright G.H. (1951): *Deontic logic*. — Mind, Vol. 60, No. 237, pp. 1–15.

Received: 26 June 2001
Revised: 28 January 2002