Conflict of Interest Policies: A General Approach

Jason Crampton, George Loizou

Department of Computer Science, Birkbeck College, University of London
{ccram01,george}@dcs.bbk.ac.uk

Abstract— **We define a conflict of interest policy and show that the definition is sufficiently general to include several well-known generic policies as special cases and to define policies for different environments. We show that such conflict of interest policies can be regarded as members of $\mathcal{P}(\mathcal{P}(X))$, for some set X, where $\mathcal{P}(X)$ denotes the powerset of X, and that such policies can be reduced to a canonical form. The set of canonical conflict of interest policies can be modelled by a subset of $\mathcal{P}(\mathcal{P}(X))$, $\mathcal{A}(\mathcal{P}(X))$. We derive upper and lower bounds for $|\mathcal{A}(\mathcal{P}(X))|$ and for the maximum length of a string that would be required to describe a conflict of interest policy. We also discuss the composition of two conflict of interest policies, an ordering for conflict of interest policies, and possible simplifications in the expression of such policies.**

Keywords— **Conflict of interest, separation of duty, access control model**

I. Introduction

OUR recent work [1], [2], [3] is concerned with modelling the behaviour of a discretionary access control mechanism (ACM) of a computer system using a deductive database. The purpose of this work is to reason about the correctness of the implementation (that is, the configuration of access control lists, say) of an abstract access control policy (ACP). We model the state of the ACM as a set of (access right) triples $M \subseteq O \times S \times R$, where O is the set of objects, S is the set of subjects, and R is the set of access rights supported by the system. Our model is essentially the same as that of Harrison, Ruzzo and Ullman [4] with $\langle o, s, r\rangle \in M$ if, and only if, $r \in [s, o]$ where $[s, o]$ denotes the entry in the protection matrix for subject s and object o.

In [3] a classification of ACPs was presented, and in [1] we discussed the way in which ACPs could be modelled as subsets of $\mathcal{P}(O \times S \times R)$. We observed that a policy, P^+, which specifies the triples that are authorised can be represented as

$$P^+ = \{\{x\} : x \in O \times S \times R\},$$

which is clearly equivalent to

$$P^+ = \{x : x \in O \times S \times R\}.$$

Similarly a policy, P^-, which specifies which triples are forbidden can be represented as

$$P^- = \{x : x \in O \times S \times R\}.$$

P^+ and P^- are similar to the positive authorisation and negative authorisation policies in Ponder [5], from which we have borrowed the superscript notation. However, when one considers separation of duty policies [6], it becomes clear that each element of the policy must be a set of triples. Specifically such a policy must specify those sets of triples which form a conflict of interest. Hence a conflict of interest policy, $P^\oplus$, is represented as

$$P^\oplus = \{A_i \subseteq O \times S \times R : i \in I\} \text{ where } I \text{ is some index set.}$$

Clearly if $|A_i| = 1$, for all $i \in I$, then $P^\oplus$ corresponds to a P^- policy. Thus we can and will use a conflict of interest policy of type $P^\oplus$ to model both P^--type policies and separation of duty policies. Hence we assume a conflict of interest policy defines any scenario which conflicts with the integrity and confidentiality of the system (and not just separation of duty constraints).

There are two ways of implementing a conflict of interest policy - static and dynamic. In the former, the access control mechanism has the requirements of the conflict of interest policy "embedded" into it, while in the latter the ACM prevents the current configuration of the system from violating the conflict of interest policy. For a more detailed account of such considerations and the development of modelling conflict of interest policies, with particular reference to role-based access control (RBAC), see [7].

The first contribution of this paper is to provide a general framework and notation for considering conflict of interest policies. We will see that, in general, the components of a conflict of interest policy are subsets of a set X, and that a conflict of interest policy is therefore a member of $\mathcal{P}(\mathcal{P}(X))$. Since $|\mathcal{P}(\mathcal{P}(X))| = 2^{2^n}$, where $n = |X|$, the number of conflict of interest policies appears to increase doubly exponentially in the size of X, and that the length (or description) of such a policy is potentially very large.

We then demonstrate that a simple observation about the characteristics of conflict of interest policies leads to a natural reduction of elements of $\mathcal{P}(\mathcal{P}(X))$ to a *canonical* representation of conflict of interest policies. We derive upper and lower bounds for the size of the set of all canonical representations, $\mathcal{A}(\mathcal{P}(X))$, and an explicit value for (the length of) the longest canonical representation. The lower bound for $|\mathcal{A}(\mathcal{P}(X))|$ is a corollary of Sperner's Theorem [8], while the result for the upper bound, due to Hansel [9], is proved using a *symmetric chain decomposition* of $\mathcal{P}(X)$ [10], and some elementary theory of partially ordered sets [11]. *En passant* we suggest two methods for combining conflict of interest policies. We also include a table of results for $1 \leqslant |X| \leqslant 8$.

The remainder of this paper is organised as follows. In Section II we introduce some fundamental definitions and notation. In Section III we give some examples of conflict

The work of Jason Crampton is supported by EPSRC Award 98317878.

of interest policies in order to illustrate the generality of our approach. In Section IV we define canonical conflict of interest policies and discuss two binary operations that can be used to compose conflict of interest policies. In Section V we state bounds for $\mathcal{A}(\mathcal{P}(X))$ and for the length of the largest conflict of interest policy. In conclusion we discuss certain simplifications to the model of a conflict of interest policy which lead immediately to an explicit value for the number of conflict of interest policies, and discuss future directions for our work.

II. Preliminaries

Definition 1: Let X be a set. An *environment*, E, is a subset of X.

In general an environment will change over time. If necessary we could write $E(t)$ to denote an environment at time point $t \in \mathbb{N}$, where $\mathbb{N}$ is the set of natural numbers. An environment is evaluated with respect to a conflict of interest policy. For example, the set of triples encoded by a protection matrix forms an environment, and the set X in this context is $O \times S \times R$.

Definition 2: A *conflict of interest policy* on X is a set of subsets of X. Let α be a conflict of interest policy. Then $\alpha = \{A_1, A_2, \dots\}$ where $A_i \subseteq X$, for all $i > 0$. In other words, $\alpha \in \mathcal{P}(\mathcal{P}(X))$.

Definition 3: An environment, E, *satisfies* the conflict of interest policy, α, if, and only if, for all $A \in \alpha$, $A \cap E \subset A$ (where $\subset$ denotes proper subset). In other words, α is satisfied if, and only if, no member of α is contained in E. (We will also say E *violates* α if E does not satisfy α. E violates α if, and only if, there exists $A \in \alpha$ such that $A \subseteq E$.)

In other words, a conflict of interest policy specifies which sets of elements in X cannot all simultaneously be present in the environment. Note that with the above definitions, if $\{x\} \in \alpha$, then α prohibits x from entering E.

Example 1: Let $X = \{1, 2, 3\}$, $\alpha_1 = \{\{1, 2\}, \{2, 3\}\}$, $\alpha_2 = \{\{1\}, \{2, 3\}\}$, $E_1 = \{1, 3\}$, $E_2 = \{2\}$. The table below summarises which environments satisfy which policies.

	α_1	α_2
E_1	✓	✗
E_2	✓	✓

Definition 4: Let α, β be two conflict of interest policies. We say β is *stronger* (respectively *weaker*) if fewer (respectively more) environments satisfy β than α. We will also say that β is more (respectively less) *restrictive* than α.

Remark 1: From the example above, we can see that given two conflict of interest policies α and β such that for all $B \in \beta$, there exists $A \in \alpha$ with $B \subseteq A$, then β is a stronger policy than α.

Proposition 1: Suppose $\alpha = \{A_1, \dots, A_n\}$ and $A_i \subset A_j$ for some $1 \leqslant i, j \leqslant n$, and define $\alpha' = \alpha \setminus \{A_j\}$ where $\setminus$ denotes set difference. Then an environment, E, satisfies α if, and only if, E satisfies α'.

Proof: "$\Rightarrow$" Follows immediately from the fact that $\alpha' \subset \alpha$.

"$\Leftarrow$" The proof proceeds by contradiction. Suppose that E satisfies α' but does not satisfy α. Clearly $A_j \subseteq E$ is the only possible way in which E does not satisfy α. However, by construction, $A_i \subset A_j \subset E$, and hence E does not satisfy α'. ■

Definition 5: A pair $\langle P, \leqslant \rangle$ is a *partially ordered set* or *poset* if for all $p, q, r \in P$

- $p \leqslant p$,
- $p \leqslant q$ and $q \leqslant p$ implies $p = q$,
- $p \leqslant q$ and $q \leqslant r$ implies $p \leqslant r$.

In other words $\leqslant$ is a binary relation on P which is reflexive, anti-symmetric and transitive, respectively. We will write $p < q$ if, and only if, $p \leqslant q$ and $p \neq q$; and $p \parallel q$ if, and only if, $p \nleqslant q$ and $p \ngeqslant q$.

Definition 6: If $\langle P, \leqslant \rangle$ is a poset, then $Q \subseteq P$ is a *chain* if for all $q_1, q_2 \in Q$ either $q_1 \leqslant q_2$ or $q_2 \leqslant q_1$. Q is an *antichain* if for all $q_1, q_2 \in Q : q_1 \parallel q_2$. We denote the set of antichains by $\mathcal{A}(P)$.

Definition 7: Given a poset, $\langle P, \leqslant \rangle$, and $p, q, \in P$, we say q covers p, denoted $p \lessdot q$, if $p < q$ and $p \leqslant r < q$ implies $p = r$.

III. Examples of Conflict of Interest Policies

In this section we will illustrate the application of our approach using two different access control models. In the first set of examples we assume the protection matrix model, and in the second a role-based access control model (RBAC). In both examples we indicate the sets which correspond to X and E. We focus our attention on static conflict of interest policies. We conclude the section with a brief discussion of RSL99 [7], a logical language for expressing separation of duty constraints within the RBAC96 [12] models.

A. The Protection Matrix Model

Let M denote the protection matrix, O the set of objects, S the set of subjects and R the set of access modes. We will write $[s, o] \subseteq R$ to denote the access modes available to subject s for object o. (Most systems which employ this model use access control lists, corresponding to a row in M, or capability lists, corresponding to a column in M, to represent the matrix [3].) In this case $X = O \times S \times R$ and (for static conflict of interest policies) E is the set of triples encoded by M. (The environment in the dynamic case is the set of active triples which have been invoked by subjects and granted by the access control mechanism.)

Suppose now that $o_1, o_2 \in O$, $S = \{s_1, \dots, s_n\}$ and $x \in R$ where x denotes "execute" access. We now give some simple examples of conflict of interest policies.

- Subject s_1 is prohibited from executing o_1.

$$\alpha_1 = \{\{\langle o_1, s_1, x \rangle\}\}$$

α_1 is satisfied provided $x \notin [s_1, o_1]$. This is a trivial example of a negative authorisation policy.

- No subject can execute both o_1 and o_2.

$$\alpha_2 = \{\{\langle o_1, s, x \rangle, \langle o_2, s, x \rangle\} : s \in S\}$$

α_2 is satisfied provided $x \notin ([s, o_1] \cap [s, o_2])$ for all $s \in S$. This is a trivial example of a separation of duty policy.

- There is no "super-user".

$$\alpha_3 = \bigcup_{i=1}^{n} \{O \times \{s_i\} \times R\}$$

- No subject is permitted to execute any file.

$$\alpha_4 = \{\{\langle o, s, x\rangle\} : o \in O, s \in S\}$$

α_4 is satisfied if for all $o \in O$ and for all $s \in S$, $x \notin [s, o]$.

If we combine the features of α_1 and α_2 we see that the composite policy $\alpha' = \alpha_1 \cup \alpha_2 \setminus \{\langle o_1, s_1, x\rangle, \langle o_2, s_1, x\rangle\}$ since $\{\langle o_1, s_1, x\rangle\} \subseteq \{\langle o_1, s_1, x\rangle, \langle o_2, s_1, x\rangle\}$ (see Proposition 1).

B. The Role-Based Access Control Model

We assume the existence of a set of roles, $R = \{r_1, \ldots, r_n\}$, a set of users, $U = \{u_1, \ldots, u_m\}$, and a user-role assignment relation, $UA \subseteq U \times R$, [12]. We will denote the set of roles to which a user, u, is assigned by ρ_u. In this case $X = U \times R$ and (in the static case) $E = UA$. (The environment in the dynamic case is the "active" user-role assignments determined by the sessions which a user is running [12].)

- User u_1 cannot be assigned to role r_1. (Strangely this type of constraint or policy is rarely mentioned in RBAC literature. The administrative model URA97 provides constraints which can prevent users being assigned to roles, but these constraints are usually articulated in terms of existing user-role assignments [13]. It is not immediately obvious how such constraints could be used to implement a policy which precludes particular user-role assignments.)

$$\beta_1 = \{\{\langle u_1, r_1\rangle\}\}$$

- No user can be assigned to both roles r_1 and r_2.

$$\beta_2 = \{\{\langle u, r_1\rangle, \langle u, r_2\rangle\} : u \in U\}$$

This is the classic separation of duty policy encountered in RBAC literature, and is usually expressed as the pair $\langle r_1, r_2\rangle$.

- Users u_1 and u_2 cannot occupy both or one of each of the two roles r_1 and r_2. This kind of policy was identified in [7] and aims to prevent collusion between two (or more) individuals to compromise system security.

$$\begin{aligned}\beta_3 = \{&\{\langle u_1, r_1\rangle, \langle u_1, r_2\rangle\}, \{\langle u_2, r_1\rangle, \langle u_2, r_2\rangle\},\\ &\{\langle u_1, r_1\rangle, \langle u_2, r_2\rangle\}, \{\langle u_1, r_2\rangle, \langle u_2, r_1\rangle\}\}\end{aligned}$$

It should be mentioned that most RBAC models include a role hierarchy [12], [14], [15], [16] which impacts on conflict of interest policies. The most detailed discussion of separation of duty constraints and their realisation within a functioning access control system is found in [17] (which is a realisation and refinement of the NIST model outlined in [15]). The RBAC database includes two relations *ssd* and *dsd* for static and dynamic separation of duty constraints, respectively. These constraints are assumed to be simply mutually exclusive pairs of roles.

We now discuss the additional constraints identified in [17] which *ssd* (and *dsd*) must satisfy in a role-based context. The *ssd* relation must be irreflexive and symmetric. The irreflexivity condition is introduced to prevent a mutually exclusive pair $\langle r, r\rangle$ from being entered into the *ssd* relation. The assumption being that such a pair would only have the meaning that no user could be assigned to the role r. We would argue that, as in policy β_1, there is a useful place for such constraints when one includes a user component. (The symmetric condition is introduced in order to establish certain logical equivalences between constraints in the NIST model in the presence of a role hierarchy, and to thereby reduce the number of logical tests in the implementation of the database update operations.)

Furthermore, if $\langle r_1, r_2\rangle \in ssd$ then

1. $\{r_1, r_2\} \in \mathcal{A}(R)$ where the role hierarchy is interpreted as a poset $\langle R, \leqslant\rangle$. (This constraint is not articulated in this way in [17].) It is obvious that this is necessary when one considers that if, without loss of generality, $r_1 \leqslant r_2$ and $\langle r_1, r_2\rangle \in ssd$ then no user can be assigned to r_2 or any role senior to it.
2. $\uparrow r_1 \cap \uparrow r_2 = \emptyset$ where $\uparrow r = \{r' \in R : r' \geqslant r\}$ denotes the set of roles senior to r and is borrowed from the "up-set" notation of poset theory [11]. This is because if $r \in \uparrow r_1 \cap \uparrow r_2$ no user can be assigned to the role r. It is less easy to justify this constraint, particularly if finer granularity is allowed in the specification of users as in our examples above.

We can of course describe the relations *ssd* and *dsd* within our framework, but the environment becomes more difficult to describe. (Specifically for each user, u, we have a separate environment, ρ_u, the set of roles u is assigned.) In short, we believe the NIST approach (and the broadly similar approach adopted in the Role Graph Model [14]) to separation of duty policies omits the vitally important user perspective.

C. The RSL99 Language

A more flexible and wide-ranging discussion of separation of duty policies was presented in [7], and included policies in which users were a factor in policy specification. The paper introduces a logical language, RSL99, in which separation of duty policies are expressed. For example, the RSL99 statement

$$|\mathtt{roles}^*(\mathtt{OE(U)} \cap \mathtt{OE(CR)})| \leqslant 1 \qquad (1)$$

expresses the constraint that for the collection of sets of roles, `CR`, no user can be assigned more than one role in any of the sets contained in `CR`. In other words, in our terminology, (1) states the conditions for satisfaction of the conflict of interest policy `CR`. Therefore, we would argue that we could simply express this policy as a set of mutually exclusive pairs. We pursue this line of thought in Section VI.

IV. Canonical Conflict of Interest Policies

Definition 8: Given a conflict of interest policy $\alpha = \{A_1, A_2, \ldots, A_n\} \in \mathcal{P}(\mathcal{P}(X))$ where $A_i \subset A_j$ for some $1 \leqslant i,j \leqslant n$, we say α can be *reduced* to $\alpha' = \{A_1, A_2, \dots, A_{j-1}, A_{j+1}, \dots, A_n\} \in \mathcal{P}(\mathcal{P}(X))$.

By Proposition 1, this reduction has no impact on the expressiveness of the policy. Hence we introduce the following definition.

Definition 9: We will write $\alpha \downarrow \alpha'$ if α' is a reduction of α, and $\alpha \downarrow^* \alpha'$ if there exists a sequence of reductions such that

$$\alpha = \alpha_1 \downarrow \alpha_2 \downarrow \cdots \downarrow \alpha_k = \alpha', \ k \geqslant 1,$$

and no further reductions can be applied to α_k; α' is called a *canonical representation* of the conflict of interest policy α.

Remark 2: Note that $\langle \mathcal{P}(X), \subseteq \rangle$ is a poset, and that a canonical representation of a conflict of interest policy is a member of $\mathcal{A}(\mathcal{P}(X))$. We will denote the set $\mathcal{A}(\mathcal{P}(X))$ by $\mathcal{A}_n$ where $n = |X|$.

We will simply say that α' is a canonical conflict of interest policy. In the remainder of this paper we will only consider canonical conflict of interest policies.

Proposition 2: For all $\alpha \in \mathcal{P}(\mathcal{P}(X))$, $\alpha', \alpha'' \in \mathcal{A}(\mathcal{P}(X))$,

$$\alpha \downarrow^* \alpha' \text{ and } \alpha \downarrow^* \alpha'' \text{ implies } \alpha' = \alpha''.$$

That is, there is a unique canonical representation for any policy α.

Proof: (By contradiction) Suppose $A' \in \alpha'$ and $A' \notin \alpha''$. Then there exists $A'' \in \alpha''$ such that $A' \subset A''$ since A' has been eliminated from α''. Hence $A'' \notin \alpha'$ since $A' \in \alpha'$. Therefore, since A'' has been eliminated from α', there exists $A''' \in \alpha'$ such that $A'' \subset A'''$. This is a contradiction, since $A' \subset A'' \subset A'''$ and $A', A''' \in \alpha'$. Hence all $A' \in \alpha'$ also belong to α''. The converse argument shows that all $A'' \in \alpha''$ also belong to α'. ■

Definition 10: Let $\alpha, \beta \in \mathcal{A}_n$. Then $\alpha \leqslant \beta$ if, and only if, for all $A \in \alpha$ there exists $B \in \beta$ such that $A \subseteq B$. As usual we will write $\alpha < \beta$ if $\alpha \leqslant \beta$ and $\alpha \neq \beta$.

Proposition 3: $\langle \mathcal{A}_n, \leqslant \rangle$ is a poset.

Proof: We need to prove that $\leqslant$ is reflexive, anti-symmetric and transitive. It is clear that the first and third of these properties hold. We prove $\leqslant$ is anti-symmetric by contradiction. Suppose that $\alpha \leqslant \beta$ and $\beta \leqslant \alpha$, but $\alpha \neq \beta$. Without loss of generality we can choose $A \in \alpha$ such that $A \notin \beta$. Since $\alpha \leqslant \beta$, there exists $B \in \beta$ such that $A < B$. Furthermore, $B \notin \alpha$ since $\alpha \in \mathcal{A}_n$ and hence contains no chain. Therefore, there exists $C \in \alpha$ such that $B < C$ since $\beta \leqslant \alpha$. Hence $A < B < C$ with $A, C \in \alpha$, but α is an antichain. ■

Bearing in mind Remark 1, we see that $\alpha \leqslant \alpha'$ implies α is more restrictive than α'. Note that $\langle \mathcal{P}(\mathcal{P}(X)), \leqslant \rangle$ is not a poset, since, for example, $\{\{1\},\{1,2\}\} \leqslant \{\{1,2\}\}$ and $\{\{1,2\}\} \leqslant \{\{1\},\{1,2\}\}$ but $\{\{1,2\}\} \neq \{\{1\},\{1,2\}\}$.

Definition 11: Given two conflict of interest policies, α and α', we define the following operations:

$$\begin{aligned} \alpha \times \alpha' &= \alpha'', \quad \text{where } \alpha \cup \alpha' \downarrow^* \alpha''; \\ \alpha + \alpha' &= \alpha'', \quad \text{where } \alpha \cup \alpha' \uparrow^* \alpha'' \end{aligned}$$

and $\uparrow$ denotes the reduction obtained by omitting the subset rather than the superset in Definition 8.

Clearly the operations $+$ and $\times$ are associative, commutative, and closed. Furthermore, the policies $\{\emptyset\}$ and $\{X\}$ are identity elements for $+$ and $\times$, respectively. That is, the set of canonical conflict of interest policies and either of the above operations forms a monoid [18]. The operation $\times$ is intended to merge two policies by including the stronger aspects of the two policies, and $+$ combines two policies by including the weaker aspects of the two policies.

Example 2: Let $X = \{1,2,3\}$. We have, for example,

$$\begin{aligned} \{\{1\},\{2,3\}\} &< \{\{1,2\},\{2,3\}\} \\ &< \{\{1,2\},\{1,3\},\{2,3\}\} \\ &< \{\{1,2,3\}\}, \end{aligned}$$

$$\begin{aligned} \{\{1\},\{2,3\}\} \times \{\{2\},\{1,3\}\} &= \{\{1\},\{2\}\}, \\ \{\{1\},\{2,3\}\} + \{\{2\},\{1,3\}\} &= \{\{1,3\},\{2,3\}\}. \end{aligned}$$

Note that

$$\begin{aligned} \{\{1\},\{2\}\} &< \{\{1\},\{2\},\{3\}\} \\ &= \inf\{\{\{1\},\{2,3\}\},\{\{2\},\{1,3\}\}\}. \end{aligned}$$

In [19] we explicitly derive binary operations $\vee$ and $\wedge$ such that $\langle \mathcal{A}_n, \leqslant \rangle$ is a finite distributive lattice [11]. In fact, $\alpha + \alpha' = \alpha \vee \alpha' = \sup\{\alpha, \alpha'\}$. However, in general, $\alpha \times \alpha' \leqslant \alpha \wedge \alpha' = \inf\{\alpha, \alpha'\}$, where $\sup\{\alpha, \alpha'\}$ and $\inf\{\alpha, \alpha'\}$ are the *least upper bound* and *greatest lower bound* [11], respectively, of α and α'. Figure 1 shows the lattices $\langle \mathcal{P}(X), \subseteq \rangle$ and $\langle \mathcal{A}(\mathcal{P}(X)), \leqslant \rangle$ for $X = \{1,2,3\}$.

V. Structural Complexity Results

Definition 12: The *length* of a conflict of interest policy is defined by the function $l : \mathcal{A}_n \to \mathbb{N}$ where

$$l(\alpha) = \begin{cases} 0 & \alpha = \emptyset, \\ \displaystyle\sum_{A \in \alpha} |A| & \text{otherwise.} \end{cases}$$

The length of a conflict of interest policy is a measure of the complexity of describing it (by a string, for example).

Theorem 1 (Sperner's Theorem [8]) For all $\alpha \in \mathcal{A}_n$,

$$|\alpha| \leqslant \binom{n}{\lfloor n/2 \rfloor},$$

with equality if, and only if,

$$\alpha = \begin{cases} \{A \subseteq X : |A| = \frac{n}{2}\} & n \text{ even}, \\ \{A \subseteq X : |A| = \frac{n-1}{2}\} & \text{or} \\ \{A \subseteq X : |A| = \frac{n+1}{2}\} & n \text{ odd}. \end{cases}$$

We now state and prove an analogous result, for the length of a conflict of interest policy.

Lemma 1: For all $\alpha \in \mathcal{A}_n$,

$$l(\alpha) \leqslant \lceil n/2 \rceil \binom{n}{\lceil n/2 \rceil},$$

with equality if, and only if,

$$\alpha = \begin{cases} \{A \subseteq X : |A| = \frac{n}{2}\} & \text{or} \\ \{A \subseteq X : |A| = \frac{n+2}{2}\} & n \text{ even}, \\ \{A \subseteq X : |A| = \frac{n+1}{2}\} & n \text{ odd}. \end{cases} \qquad (2)$$

Proof: We first note that the three definitions of α given in (2) belong to $\mathcal{A}_n$ and have the required length. This is justified by the fact that

$$(n-r)\binom{n}{r} = (r+1)\binom{n}{r+1} \text{ for all } 0 \leqslant r < n,$$

and that when n is even $\lceil n/2 \rceil = n/2$. Hence, when n is even,

$$(n-r)\binom{n}{r} = (r+1)\binom{n}{r+1}$$

is equivalent to

$$\frac{n}{2}\binom{n}{n/2} = \left(\frac{n}{2}+1\right)\binom{n}{(n/2)+1}.$$

We now follow the approach of the original proof of Sperner's Theorem [8].

Let $\beta \in \mathcal{A}_n$ be any policy with maximal length. We will prove that $\beta = \alpha$. Define

$$\lfloor \beta \rfloor = \{B \in \beta : |B| = l\} \quad \text{where} \quad l = \min_{B \in \beta} |B|,$$
$$\gamma = \{C \subseteq X : \text{there exists } B \in \lfloor \beta \rfloor \text{ such that } B \lessdot C\};$$

$$\lceil \beta \rceil = \{B \in \beta : |B| = u\} \quad \text{where} \quad u = \max_{B \in \beta} |B|,$$
$$\delta = \{D \subseteq X : \text{there exists } B \in \lceil \beta \rceil \text{ such that } D \lessdot B\}.$$

Define

$$\beta' = (\beta \setminus \lceil \beta \rceil) \cup \delta.$$

Then, for all $\beta \in \mathcal{A}_n$,

$$\beta' \in \mathcal{A}_n, \tag{3}$$

and, for all $u \geqslant \frac{n+2}{2}$,

$$l(\beta') \geqslant l(\beta) \quad \text{with equality if } u = \frac{n+2}{2}. \tag{4}$$

Analogous results can be proved for $\beta'' = (\beta \setminus \lfloor \beta \rfloor) \cup \gamma$ (These are left as an exercise for the interested reader.)

We prove (3) by contradiction. Therefore, suppose $\beta' \notin \mathcal{A}_n$. Then there exists $D \in \delta$ such that $B \subseteq D$ for some $B \in \beta \setminus \lceil \beta \rceil$. However, this implies that there exists $B' \in \lceil \beta \rceil$ such that $D \subseteq B'$ by construction of δ, and hence that $B \subset B'$ and $\beta \notin \mathcal{A}_n$.

We prove (4) by counting N, the number of pairs $\langle B, D \rangle$ such that $B \in \lceil \beta \rceil$, $D \in \delta$ and $D \lessdot B$, in two different ways. For a particular $B \in \lceil \beta \rceil$ there are exactly u such subsets D (obtained by omitting one of the u elements of B). For a particular $D \in \delta$ there are $n-(u-1)$ possible subsets B which cover D, since $|D| = u-1$. However, not all of these are necessarily in $\lceil \beta \rceil$. Therefore, we have

$$u|\lceil \beta \rceil| = N \leqslant (n-u+1)|\delta|. \tag{5}$$

Hence

$$\frac{|\delta|}{|\lceil \beta \rceil|} \geqslant \frac{u}{n-u+1} \geqslant \frac{u}{u-1} \tag{6}$$

since

$$u \geqslant \frac{n+2}{2} \quad \text{implies} \quad n-u+1 \leqslant u-1.$$

Therefore, by (6),

$$\begin{aligned} l(\beta') &= l(\beta) - u|\lceil \beta \rceil| + (u-1)|\delta| \\ &\geqslant l(\beta) \text{ with equality when } u = \frac{n+2}{2}. \end{aligned}$$

Since, by assumption, β has maximal length, (3) and (4) imply

$$u \leqslant \frac{n+2}{2} \text{ and, analogously, } l \geqslant \frac{n}{2}.$$

We now have three cases:
n odd: whence $u = l = \lceil n/2 \rceil$ and $\beta = \alpha$;
n even, $l = u$: whence either $u = l = \frac{n}{2}$ or $u = l = \frac{n+2}{2}$ and $\beta = \alpha$;
n even, $l < u$: whence we derive a contradiction as follows. Since $l(\beta)$ is assumed to be maximal and

$$l(\beta) \leqslant l(\beta') \leqslant \lceil n/2 \rceil \binom{n}{\lceil n/2 \rceil} \tag{7}$$

we must have equality in (7), and hence equality in (5). In other words, for each $C \in \gamma$ every superset B of C must be in $\lceil \beta \rceil$. Now choose some $B \in \beta \setminus \lceil \beta \rceil$ and $C \in \gamma$ such that $|B \cap C|$ is a maximum. Since $|B| = |C| = u-1$ ($|B| = u-1$ as $l = u-1$) and $B \neq C$, there exists some $b \in B \setminus C$ and some $c \in C \setminus B$. Hence, because we require equality in (5), $C \cup \{b\} \in \lceil \beta \rceil$, $C' = C \cup \{b\} \setminus \{c\} \in \gamma$ and $|B \cap C'| = |B \cap C| + 1$, contradicting the maximality of $B \cap C$.

■

Definition 13: For $0 \leqslant r \leqslant n$, we define $\mathcal{A}_n^r \subset \mathcal{A}_n$ as follows:

$$\mathcal{A}_n^r = q\{\alpha \in \mathcal{A}_n : \max_{A \in \alpha}(|A|) = r\}$$

In other words $\mathcal{A}_n^r$ is the set of all conflict of interest policies each of which has a largest set of cardinality r.

Example 3: Let $X = \{1, 2, 3\}$. Then

$$\begin{aligned} \mathcal{A}_3^2 = \{ &\{\{1,2\}\}, \{\{1,3\}\}, \{\{2,3\}\}, \\ &\{\{1\},\{2,3\}\}, \{\{2\},\{1,3\}\}, \{\{3\},\{1,2\}\}, \\ &\{\{1,2\},\{1,3\}\}, \{\{1,2\},\{2,3\}\}, \{\{1,3\},\{2,3\}\}, \\ &\{\{1,2\},\{1,3\},\{2,3\}\}\}. \end{aligned}$$

Lemma 2: For all $0 \leqslant r \leqslant n$ there exists $\alpha \in \mathcal{A}_n^r$ such that $|\alpha| = \binom{n}{r}$.

Proof: Let $\alpha = \{A \subseteq X : |A| = r\}$. The result follows immediately. ■

Corollary 1: Let $\phi(n) = |\mathcal{A}_n|$ and $\nu = \binom{n}{\lfloor n/2 \rfloor}$. For all $n \geqslant 1$,

$$\phi(n) \geqslant \sum_{r=0}^{n} 2^{\binom{n}{r}} - (n+1) \geqslant 2^{\nu}.$$

Proof: We first note that

$$\phi(n) = \sum_{r=0}^{n} |\mathcal{A}_n^r| \geqslant |\mathcal{A}_n^{\lfloor n/2 \rfloor}|.$$

n	$\phi(n)$
1	2
2	5
3	19
4	167
5	7580
6	7828354
7	2414682040998
8	56130437228687557907788

TABLE I
$\phi(n)$ FOR $1 \leqslant n \leqslant 8$

Furthermore, by Lemma 2, there exists $\alpha \in \mathcal{A}_n^r$ such that $|\alpha| = \binom{n}{r}$ for all $0 \leqslant r \leqslant n$, and every subset of α belongs to $\mathcal{A}_n^r$. The number of ways of choosing such subsets (excluding the empty set) is $2^{\binom{n}{r}} - 1$. Hence

$$\phi(n) \geqslant \sum_{r=0}^{n} (2^{\binom{n}{r}} - 1) = \sum_{r=0}^{n} 2^{\binom{n}{r}} - (n+1).$$

■

Theorem 2 (Hansel [20]) For all $n \geqslant 1$,

$$2^\nu \leqslant |\phi(n)| \leqslant 3^\nu.$$

Proof: The left-hand side of the inequality is proved in Corollary 1. The reader is referred to [20] for the proof of the right-hand side of the inequality. The basic idea is to observe that there is an isomorphism between the set of antichains and the set of filters [11] in a poset, and then to construct a (symmetric chain) decomposition of the poset; this enables the enumeration (with duplicates) of the set of filters. ■

The problem of determining $\phi(n)$ was first posed by Dedekind [21] and is known to be very difficult. The value of $\phi(n)$ for $n \geqslant 9$ is not known. Table I shows values of $\phi(n)$ for $1 \leqslant n \leqslant 8$. This table is reproduced from [11].

We denote the upper and lower bounds obtained in Theorem 2 and Corollary 1 by $\overline{\phi(n)}$ and $\underline{\phi(n)}$, respectively. Table II shows the values (in floating point notation to aid comparison) of $\phi(n)$, $\underline{\phi(n)}$, $\overline{\phi(n)}$ and 2^{2^n} for $1 \leqslant n \leqslant 8$.

VI. Conclusion

We have presented a general framework for the articulation of conflict of interest policies which include negative authorisation policies and separation of duty policies as special cases. We believe our approach offers a more complete characterisation of such policies, and significantly extends the class of policies for role-based access control.

We have not restricted our attention to policies consisting of mutually exclusive pairs, but noted in Section III that separation of duty policies are usually modelled in this way. That is, $\alpha = \{P_1, \ldots, P_n\}$ where $|P_i| = 2$ for $1 \leqslant i \leqslant n$. The only exception we have found is [7], but the subsequent development of the logical language the authors use to express conflict of interest constraints makes it clear that although the A_is may have cardinality greater than two, the policy is violated if any pair $P \subseteq A_i$ for some $A_i \in \alpha$ enters the environment. We note that with this in mind, we can rewrite an arbitrary policy

$$\alpha = \{A_i : i \in I\}$$

as the following

$$\alpha' = \bigcup_{i \in I} \{P_{i_1}, \ldots, P_{i_\mu}\}, \text{ where } i_\mu = \binom{|A_i|}{2}.$$

In other words, we replace each $A_i \in \alpha$ by the set of all pairs of elements in A_i. In terms of the partial order of Definition 10, $\alpha' \leqslant \alpha$ with equality when $|A_i| \leqslant 2$, for all $i \in I$, so α' is, in general, more restrictive than α. Therefore, an arbitrary conflict of interest policy, α, can be expressed as a policy of mutually exclusive pairs, α', which is at least as strong as α. (This assumes that singleton and doubleton sets in α are "replaced" by themselves.) It can easily be seen that there are at most

$$\binom{2^n}{2} = \frac{2^n(2^n-1)}{2} = 2^{n-1}(2^n-1)$$

such policies, and that the longest such policy is

$$2^n(2^n-1).$$

Hence, if the usual assumptions are made about the definition of separation of duty policies, the complexity of such policies can be readily described. However, we feel that the effort involved in investigating the general case has been worthwhile. It has led to us developing a general theorem about finite partially ordered sets and their embedding into a complete lattice of subsets of that set [19], which in turn we hope to use to develop a more sophisticated model of role-based access control.

In the future we will investigate more sophisticated strategies for selection from a symmetric chain decomposition (as in the proof of Theorem 2) in order to improve the upper bound on $\phi(n)$.

Finally, we intend to generalise the definition of symmetric chain decomposition to an arbitrary poset, P, and thereby produce an upper bound for $|\mathcal{A}(P)|$.

References

[1] J. Crampton, G. Loizou, and G. O'Shea, "Evaluating access control," Tech. Rep. BBKCS-9905, Birkbeck College, University of London, 1999.

[2] J. Crampton, G. Loizou, and G. O'Shea, "A logic of access control," *The Computer Journal*, 2000, To appear.

[3] G. O'Shea, *Access Control in Operating Systems*, Ph.D. thesis, Birkbeck College, University of London, July 1997.

[4] M.A. Harrison, W.L. Ruzzo, and J.D. Ullman, "Protection in operating systems," *Communications of the ACM*, vol. 19, no. 8, pp. 461–471, August 1976.

[5] N. Damianou, E.C. Lupu, N. Dulay, and M. Sloman, "Ponder: A language for specifying security and management policies for distributed systems," Tech. Rep. DOC 2000/1, Imperial College, University of London, January 2000.

[6] D.D. Clark and D.R. Wilson, "A comparison of commercial and military computer security policies," in *Proceedings of IEEE Symposium on Security and Privacy*, April 1987, pp. 184–194.

[7] G-J. Ahn and R.S. Sandhu, "The RSL99 language for role-based separation of duty constraints," in *Proceedings of Fourth ACM Workshop on Role-Based Access Control*, Fairfax, Virginia, October 1999, pp. 43–54.

[8] E. Sperner, "Ein Satz über Untermengen einer endlichen Menger," *Mathemathische Zeitschrift*, vol. 27, pp. 544–548, 1928.

[9] G. Hansel, "Sur le nombre des fonctions Booléennes monotones de n variables," *Comptes Rendus Hebdomadaires des Séances Academie des Sciences (Paris Série A et B)*, vol. 262, pp. 1088–1090, 1966.

[10] R.A. Brualdi, *Introductory Combinatorics*, Prentice Hall, New Jersey, 1999.

[11] B.A. Davey and H.A. Priestley, *Introduction to Lattices and Order*, Cambridge University Press, 1990.

[12] R.S. Sandhu, E.J. Coyne, H. Feinstein, and C.E. Youman, "Role-based access control," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[13] R.S. Sandhu, V. Bhamidipati, E.J. Coyne, S. Ganta, and C.E. Youman, "The ARBAC97 model for role-based administration of roles: Preliminary description and outline," in *Proceedings of Second ACM Workshop on Role-Based Access Control*, Fairfax, Virginia, November 1997, pp. 41–49.

[14] M. Nyanchama and S. Osborn, "The role graph model," in *Proceedings of First ACM Workshop on Role-Based Access Control*, Gaithersburg, Maryland, October 1995, pp. II25–II31.

[15] D.F. Ferriaolo, J.A. Cugini, and D.R. Kuhn, "Role-based access control (RBAC): Features and motivations," in *Proceedings of 11th Annual Computer Security Applications Conference*, New Orleans, Louisiana, December 1995, pp. 241–248.

[16] R.S. Sandhu, D.F. Ferraiolo, and D.R. Kuhn, "The NIST model for role-based access control: Towards a unified standard," http://www.acm.org/sigsac/nist.pdf, 2000.

[17] S.I. Gavrila and J.F. Barkley, "Formal specification for role based access control user/role and role/role relationship management," in *Proceedings of Third ACM Workshop on Role-Based Access Control*, Fairfax, Virginia, October 1998, pp. 81–90.

[18] S. Burris and H.P. Sankappanavar, *A Course in Universal Algebra*, vol. 78 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1981.

[19] J. Crampton and G. Loizou, "Embedding a poset in a lattice," Tech. Rep. BBKCS-0001, Birkbeck College, University of London, May 2000.

[20] K. Engel, *Sperner Theory*, vol. 65 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, England, 1997.

[21] R. Dedekind, "Über Zerlegungen von Zahlen durch ihre grössten gemeinsamen Teiler," in *Festschrift der Techn. Hochsh. Braunschweig bei Gelegenheit der 69. Versammlung deutscher Naturforscher und Ärzte*, 1897, pp. 1–40.

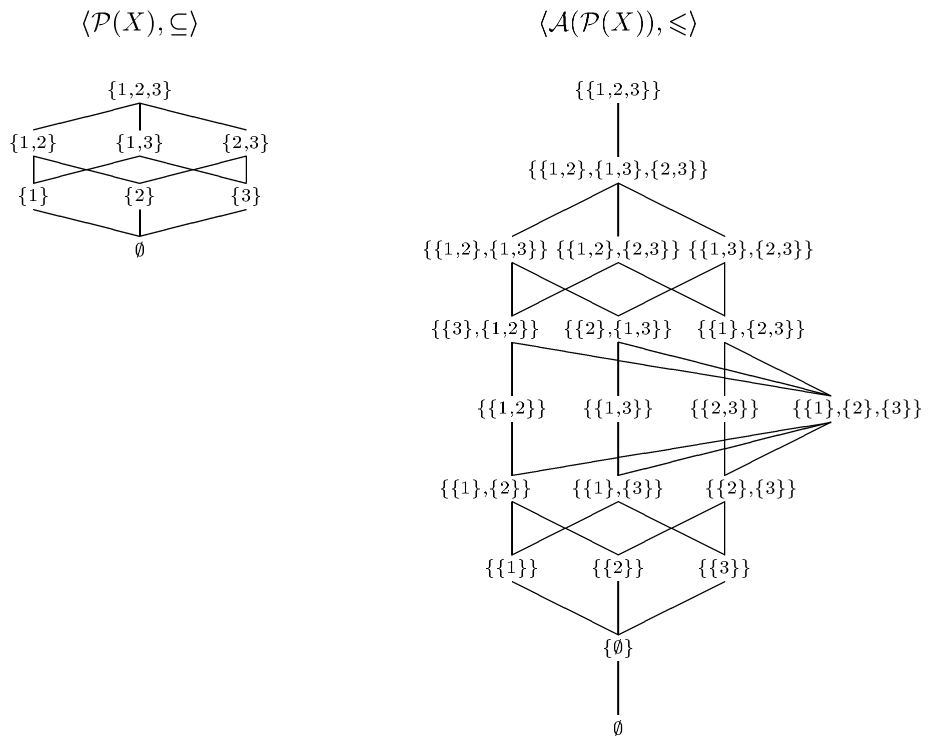

Fig. 1. The Lattices $\langle \mathcal{P}(X), \subseteq \rangle$ and $\langle \mathcal{A}(\mathcal{P}(X)), \leqslant \rangle$ for $X = \{1, 2, 3\}$

n	ν	$\underline{\phi(n)}$	$\phi(n)$	$\overline{\phi(n)}$	2^{2^n}
1	1	2	2	3	4
2	2	5	5	9	16
3	3	16	19	27	256
4	6	95	167	729	65536
5	10	2110	7580	59049	4294967296
6	20	1.114237×10^6	7.828354×10^6	3.486784×10^{12}	1.844674×10^{18}
7	35	6.872367×10^{10}	2.414682×10^{12}	5.003155×10^{16}	3.402824×10^{38}
8	70	1.180736×10^{21}	5.613044×10^{22}	2.503156×10^{33}	1.157921×10^{77}

TABLE II

$\underline{\phi(n)}$, $\phi(n)$, $\overline{\phi(n)}$ AND 2^{2^n} FOR $1 \leqslant n \leqslant 8$