
Access Matrix

George W. Dinolt
CS 4605

Access Matrix Elements

- Subjects
- Objects
- Access Modes

How to Model the Access Matrix

The Base Sets

SUB – The set of Subjects

OBJ – The set of Objects

AM – The Access Modes

SL – The Security Labels

The functions of the Model

$$sl_o : OBJ \rightarrow \mathcal{SL}$$

$$sl_s : SUB \rightarrow \mathcal{SL}$$

The Access Matrix

	s_1^*	s_2	s_3	...	s_k
o_1^\dagger	r	rw	re	...	r
o_2	x	a	r	...	
o_3	r	a		...	r
...			...		
o_m	rX	rX	rX	...	rX

Modeling the Access Matrix

$$\mathit{Elements} = \mathit{SUB} \times \mathit{OBJ} \times \mathit{AM}$$

$$\mathit{ASETS} = 2^{\mathit{Elements}\dagger} = \{x : x \subseteq \mathit{Elements}\}$$

$$\mathit{Secure} : \mathit{ASETS} \rightarrow \{\mathit{true}, \mathit{false}\}$$

State and Changing State

A system is a sequence of members of $ASSETS$, it is a sequence of “arrays.”

$$SYSTEM = \{seq : \mathbb{N} \rightarrow ASSETS\}$$

Secure System

Let $A \in \mathcal{ASSETS}$ and let $s \in \mathcal{SYSTEM}$.

s is *secure* with respect to A if and only if

$$\forall n \in \mathbb{N} : s(n) \subseteq A$$

Secure Systems

If $sys \in \mathcal{SYSTEM}$ and $n \in \mathbb{N}$, $sys(n) \in \mathcal{SETS}$ is the state of the execution path sys at n .

If $A \in \mathcal{SETS}$, the set

$$\{sys : sys(n) \subseteq A \forall n \in \mathbb{N}\}$$

is the set of all possible secure systems with respect to A .

Notation

Suppose $A \in \mathcal{A}S\mathcal{E}T\mathcal{S}$ is the set of allowed accesses for some $sys \in \mathcal{S}Y\mathcal{S}T\mathcal{E}M$. We call $sys(n) \subseteq A$ the set of *current* accesses of the system sys at n . The system sys (with respect to the allowed set A) is secure if and only if $sys(n) \subseteq A$ for all n .

State Transforms

$$OP = \{add, delete\}$$

$$transform : Element \times OP \times ASSETS \rightarrow ASSETS$$

$$transform(e, add, X) = X \cup \{e\}$$

$$transform(e, delete, X) = X \setminus \{e\}$$

Secure Transforms

Suppose $A, X \in \mathcal{ASETS}$ and $X \subseteq A$. Then for all $e \in A$,

$$\text{transform}(e, \text{add}, X) \subseteq A$$

$$\text{transform}(e, \text{delete}, X) \subseteq A$$

Sequences from transforms

Let $seq : \mathbb{N} \rightarrow \mathcal{ASETS}$ be a sequence defined below.

$$seq(0) = \emptyset$$

$$\forall i > 0, \exists e \in Elements \wedge \exists op \in \mathcal{OP}$$

$$seq(i) = transform(e, op, seq(i - 1))$$

Secure Sequences

Let $A \in \mathcal{ASSETS}$, seq be defined as above and
 $seq(i) \subseteq A$.

$\forall e \in Elements, transform(e, delete, seq(i)) \subseteq A$.

If $\forall e \in A, transform(e, add, seq(i)) \subseteq A$.

Security Labels

Suppose \mathcal{SL} is *totally ordered*[¶] and *finite*^{||}

Security Policy: $\forall s \in SUB, o \in OBJ$

s can read $o \iff sl_o(o) \leq sl_s(s),$

s can write $o \iff sl_s(s) \leq sl_o(o)$

[¶]Every pair of elements is comparable

^{||}Can be represented by a subset of the Integers

Label Order

- Let $S\mathcal{L} = \{l_1, l_2, l_3, \dots, l_n\}$
- Assume $l_1 < l_2 < l_3 < \dots < l_n$

Subjects and Objects

- We can name the subjects $SUB = \{s_1, s_2, s_3, \dots\}$ so that $sl_s(s_1) \leq sl_s(s_2) \leq sl_s(s_3) \leq \dots$
- We can name the objects $OBJ = \{o_1, o_2, o_3, \dots\}$ so that $sl_o(o_1) \leq sl_o(o_2) \leq sl_o(o_3) \leq \dots$

Access Matrix Structure

	s_0	s_1	s_2	s_3	s_4	s_5
o_0	rwX	rwX	r	r	r	r
o_1	rwX	rwX	r	r	r	r
o_2	W	W	rwX	rwX	r	r
o_3	W	W	rwX	rwX	r	r
o_4	W	W	W	W	rwX	rwX
o_5	W	W	W	W	rwX	rwX

Ordered Access Matrix

	s_1	s_2	s_3	\dots
o_1				
o_2		r		
o_3				
\dots		\dots		

Suppose I know that $r \in (s_2, o_2)$ entry, what can I say about the other entries?

Policy in Access Matrix

- The Policy is embodied in the structure of the Access Matrix.
- The Security Labels are a way of organizing the subjects and objects in the array.
- Any execution trace that is a subset of the “labeled access matrix” will satisfy the “read down/write up” policy.