Foundation for a Time Interval Access Control Model

Francis B. Afinidad, Timothy E. Levin, Cynthia E. Irvine, and Thuy D. Nguyen

Computer Science Department, Naval Postgraduate School
Monterey, CA 93943, USA
{fbafinid, levin, irvine, tdnguyen}@nps.edu

Abstract. A new model for representing temporal access control policies is introduced. In this model, temporal authorizations are represented by time attributes associated with both subjects and objects, and a "time interval access graph." The time interval access graph is used to define constraints on the temporal relations between subjects and objects. Interval algebra is used to define and analyze the time interval access graph.

1 Introduction

In many commercial and military environments, time is often a critical factor for making decisions regarding authorization or access to information. The value or sensitivity of data and processes has become more dependent upon time attributes. Thus, future information systems will need to support system-wide security policies that incorporate time as a decision factor. To this end, a *Time Interval Access Control* (TIAC) model has been developed.

A significant contribution of the TIAC model is that it provides formal semantics to express temporal authorization policies, in which temporal attributes of subjects and objects are used to determine authorized accesses. The TIAC model differs from previously proposed models such as the *Temporal Authorization Model* by Bertino et al. [5, 6] and the *Temporal Data Authorization Model* by Gal and Atluri [4, 7], primarily in its ability to specify temporal relations between subjects and objects.

Another contribution of the TIAC model is that it is the first use of interval algebra [3] to express a temporal access control policy. This algebra provides the necessary expressive power to logically describe a temporal access control policy, and a precise and efficient way to computationally reason about the temporal relation between subjects and objects and associated access constraints. Policy enforcement mechanisms and the modeling of the effectiveness of those mechanisms with respect to the type of temporal authorizations describable in TIAC are outside of the scope of this paper (see [1]).

A brief discussion of interval algebra is presented in Section 2. Section 3 provides a description of the TIAC model, where we establish the definition of time intervals and discuss the formal semantics used for representing temporal authorizations and access requests. Finally, future work and conclusions are presented in Section 4.

V. Gorodetsky, I. Kotenko, and V. Skormin (Eds.): MMM-ACNS 2005, LNCS 3685, pp. 406 – 411, 2005.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Foundation for a Time Interval Access Control Model	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School 833 Dyer Road Code SS/CP Monterey, CA 93943-5118**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

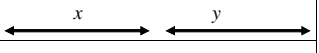
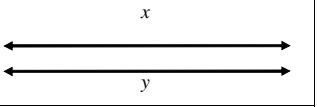
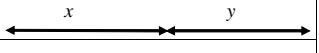
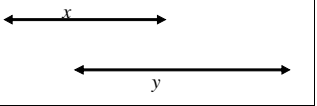
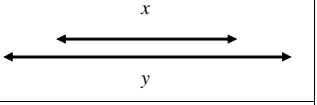
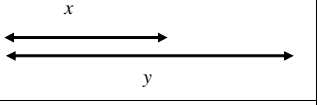
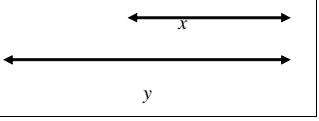
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**6**	

2 Background

Interval algebra [3] provides a means to represent time intervals associated with actions and entities and to computationally reason about their relationships. It defines the possible relations that can hold between two time intervals (see Table 1). These relations are mutually exclusive, in that only one is needed to describe the relative temporal placement of any two time intervals. Interval algebra assumes that the beginning and ending points (signified with "–" and "+" respectively) of an interval do not coincide. For each entry in Table 1, the first line shows the basic relation and the second line shows its inverse relation.

Table 1. Basic temporal relationships

RELATION	PREDICATE FORM	SYMBOL	RELATION ON ENDPOINTS	PICTORIAL MEANING
x before y y after x	BEFORE(x,y) AFTER(y,x)	< >	($x+ < y-$)	
x equals y y equals x	EQUALS(x,y) EQUALS(y,x)	= =	($x- = y-$) ∧ ($x+ = y+$)	
x meets y y met by x	MEETS(x,y) MET_BY(y,x)	m mi	$x+ = y-$	
x overlaps y y overlapped by x	OVERLAPS(x,y) OVERLAPPED_BY(y,x)	o oi	($x- < y-$) ∧ ($x+ > y-$) ∧ ($x+ < y+$)	
x during y y includes x	DURING(x,y) INCLUDES(y,x)	d di	($x- > y-$) ∧ ($x+ < y+$)	
x starts y y started by x	STARTS(x,y) STARTED_BY(y,x)	s si	($x- = y-$) ∧ ($x+ < y+$)	
x finishes y y finished by x	FINISHES(x,y) FINISHED_BY(y,x)	f fi	($x- > y-$) ∧ ($x+ = y+$)	

A set of time intervals and their required or allowed interrelationships can be represented using a directed graph (also known as an *interval algebra network*, or *IA network*), in which each vertex represents an individual time interval and each directed edge represents the relationship(s) between a pair of vertices.

3 TIAC Model

The TIAC model provides a formal semantic framework to extend existing authorization models with policies (e.g., restrictions) regarding the temporal relationships between subjects (e.g., user), objects (e.g., data) and the *time of access*.

In this section, a discussion of time and intervals provides a foundation for the TIAC model. Then the elements that make up the TIAC model are described. These elements are: 1) temporal entities, 2) the time interval access graph, 3) temporal authorizations, 4) access requests, and 5) the evaluation of access requests.

3.1 Time and Intervals

Time is assumed to be a set of discrete points, $\boldsymbol{T}$, which is isomorphic to the natural numbers and is linearly ordered with respect to the < relation. Points in $\boldsymbol{T}$ are used in representing time intervals.

Time intervals are represented using half-open intervals denoted as $\tau = [t\text{-}, t\text{+})$ where $t\text{-} < t\text{+}$. Half-open intervals are used so that there are no semantic ambiguities about the point where two time intervals meet. A *unit time interval* is the smallest expressible interval. It has a duration of one where $t\text{+} = t\text{-} + 1$. When referring to the *current* time a unit time interval is used. For discussion purposes, the current time will be referred to as $now.\tau$ where $now.\tau = [now\text{-}, now\text{+})$.

Time intervals are associated with subjects and objects, and temporal access control policies (restrictions regarding the relationships between intervals) are reasoned about using interval algebra.

3.2 Temporal Entities

Temporal entities are represented using the concept of subjects and objects similar to those discussed by Graham et al., Lampson, and Weissman [8, 9, 10]. Subjects and objects each have an associated time interval (attribute), which is used for making access control decisions.

In the following definitions, $\mathbf{S}_{\boldsymbol{\tau}}=\{s_1, s_2,\ldots s_n\}$ is the set of temporal subjects, and $\mathbf{O}_{\boldsymbol{\tau}}=\{o_1,o_2,\ldots o_n\}$ is the set of temporal objects (i.e., the passive entities that hold data or information and are accessed by temporal subjects).

Definition 1 (Temporal Object, Temporal Subject). *A temporal entity α is an object $o \in \boldsymbol{O}_{\boldsymbol{\tau}}$, or a subject $s \in \boldsymbol{S}_{\boldsymbol{\tau}}$, with which is associated a time interval $\tau = [t\text{-}, t\text{+})$ where:*

$\alpha.\tau$	*designates the time interval associated with α*
$\alpha.t\text{-}$	*designates the time point at the beginning of interval $\alpha.\tau$*
$\alpha.t\text{+}$	*designates the time point at the end of interval $\alpha.\tau$*

The time interval associated with a subject or object may be used to describe access constraints based on a temporal policy. For example, a time interval could be used to represent when a subject is valid or when an object may be accessed. Using interval algebra, it is possible to express policies regarding the temporal relations between a subject, an object, and a reference time interval such as $now.\tau$.

3.3 Time Interval Access Graph φ

The TIAC model introduces the time interval *access graph, φ*. φ is a consistent instantiation of a three-vertex IA network that defines access constraints on the temporal relations between subjects and objects, and a reference time interval (τ_{ref}). A consistent version of any three-node access graph can be efficiently determined [1, 2, 3].

Definition 2 (Time Interval Access Graph φ). *The time interval access graph φ is a consistent instantiation of a three-vertex IA network* $\boldsymbol{G = (V, E)}$ *where*:

$\boldsymbol{V}$	$\{s.\tau, o.\tau, \tau_{ref}\}$
$\boldsymbol{E}$	$\{(s.\tau, o.\tau), (\tau_{ref}, s.\tau), (\tau_{ref}, o.\tau)\}$
$\boldsymbol{R}$	$\{<, >, d, di, o, oi, m, mi, s, si, f, fi, =\} \cup \varnothing$
$\gamma: \boldsymbol{E} \rightarrow \wp(\boldsymbol{R})$	*a disjunctive set function that specifies the temporal relations allowed between a pair of vertices*

For example, φ could be instantiated with the following:

$s.\tau = [5, 20)$, $o.\tau = [10, 15)$, and $\tau_{ref} = [11, 12)$
$\gamma(s.\tau, o.\tau) = \{includes\}$, $\gamma(\tau_{ref}, s.\tau) = \{starts \vee during\}$, and $\gamma(\tau_{ref}, o.\tau) = \{during\}$

3.4 Temporal Authorizations

Policies often distinguish between different "modes" in which a subject may access an object (e.g., observe, modify, execute, append). A *temporal authorization* $\boldsymbol{A_\varphi}$ is a mapping of a subject-object pair to a set of mode-φ pairs, which completely defines the temporal authorization policy for the subject with respect to that object. For simplicity of presentation, it is assumed herein that there is only one mode-φ pair per subject-object pair.

Definition 3 (Temporal Authorization). *A temporal authorization* $\boldsymbol{A_\tau}$ *is defined as a 4-tuple (s, o, m, φ) where:*

$s \in \boldsymbol{S_\tau}$	*temporal subject*
$o \in \boldsymbol{O_\tau}$	*temporal object*
$m \subset \boldsymbol{M}$	*allowed mode(s) of access*
φ	*time interval access graph that describes the temporal restrictions on the use of o*

A temporal authorization $\mathbf{A_\tau} = (s, o, m, \varphi)$ states that a subject *s* is allowed *m* access to object *o* as restricted by the time interval access graph *φ*. For a given policy instantiation, $\boldsymbol{\Omega_\tau}$ is the set of temporal authorizations.

3.5 Access Requests

A temporal subject, to gain access to a temporal object, initiates an *access request* for a given *mode* of access to occur at a particular time. In the most general form, temporal requests would specify an arbitrary time in the past, present and future. For simplicity in this discussion, requests will be characterized relative to $now.\tau$. There

are two types of access requests: *general access requests* and *duration access requests*.

Definition 4 (General Access Request). *A general access request* $\boldsymbol{R_{g\tau}}$ *is a 4-tuple (s, o, m, now.*τ*) where:*

$s \in \boldsymbol{S_\tau}$ *is a temporal subject*
$o \in \boldsymbol{O_\tau}$ *is a temporal object*
$m \subset \boldsymbol{M}$ *is a mode(s) of access*
$now.\tau$ *is the time of access request*

A general access request $\boldsymbol{R_{g\tau}}(s, o, m, now.\tau)$ states that a subject s requests m access to object o at time $now.\tau$. Implicit in this form of request is that the subject would be granted access for the maximum duration allowed by the access graph φ associated with s and o (if any exists).

Definition 5 (Duration Access Request). *A duration access request* $\boldsymbol{R_{d\tau}}$ *is a 5-tuple (s, o, m, now.*τ*,* δ*) where:*

$s \in \boldsymbol{S_\tau}$ is a temporal subject
$o \in \boldsymbol{O_\tau}$ is a temporal object
$m \subset \boldsymbol{M}$ is the mode(s) of access
$now.\tau$ *is the time of the access request*
δ *is the requested duration of access*

A duration access request $\boldsymbol{R_{d\tau}}(s, o, m, now.\tau, \delta)$ states that a subject s requests m access to object o for a duration δ.

3.6 Evaluation of Access Requests

An access request is evaluated as follows: the set of temporal authorizations $\boldsymbol{\Omega_\tau}$ is searched for a matching subject-object pair. If no match is found, access is denied. If a match is found, the requested mode is compared to the allowed mode, and then the time interval access graph φ is interpreted relative to the requested interval, to grant or deny access. This process is specified in the boolean functions ***Eval_g*** and ***Eval_d***.

$\boldsymbol{Eval\_g}(\boldsymbol{R_{g\tau}}(s, o, m, now.\tau)) \Rightarrow \exists\ (s', o', m', \varphi) \in \boldsymbol{\Omega_\tau}(s = s' \wedge o = o' \wedge m \subset m' \wedge \varphi =$ true when evaluated using $s.\tau$, $o.\tau$, and $now.\tau$)

$\boldsymbol{Eval\_d}(\boldsymbol{R_{d\tau}}(s, o, m, now.\tau, \delta)) \Rightarrow \exists\ (s', o', m', \varphi) \in \boldsymbol{\Omega_\tau}(s = s' \wedge o = o' \wedge m \subset m' \wedge \varphi =$ true when evaluated using $s.\tau$, $o.\tau$, and $now.\tau + \delta$)

Note: $now.\tau + \delta = [now\text{-}, now\text{-} + \varphi)$

4 Conclusion and Future Research

In this short paper, we have presented the TIAC model as a novel way to specify temporal access control policies. This model is able to formally specify temporal

constraints on time attributes associated with subjects and objects, and a reference time interval such as time of access.

Several areas related to TIAC are still being investigated. We are considering the formal semantics for creating and deleting temporal authorizations as well as the policy implications of the tranquility of temporal attributes associated with subjects and objects. In general, a *set* of mode-φ pairs can be associated with each subject-object pair in order to be able to express a different policy for each mode of access, but that extension to the TIAC model is left for future work.

We also plan to generalize this model so that it could specify an access request that uses a different reference time interval other than current time, which would allow the model to check for previous, current, and future authorizations. This research is also being extended to determine a set of useful temporal access control policies that can be expressed using the TIAC model. Finally, we are considering other enhancements to the TIAC model that involve extending the TIAC model concept to support the specification of event-based security policies.

References

1. Afinidad, F.B.: An Interval Algebra-Based Temporal Access Control Protection Architecture. Dissertation, Naval Postgraduate School, Monterey, CA (2005)
2. Afinidad, F.B., Levin, T.E., Irvine, C.E., and Nguyen, T.D.: Toward Building A Time Interval Access Control (TIAC) Model. Naval Postgraduate School, NPS Technical Report NPS-CS-05-006 (June 2005)
3. Allen, J.F.: Maintaining Knowledge About Temporal Intervals. Communications of the ACM, Vol. 26, no. 11 (November 1983) 832–843
4. Atluri, V. and Gal, A.: An Authorization Model for Temporal and Derived Data: Securing Information Portals. ACM Transactions on Information and System Security, Vol. 5, no. 1 (February 2002) 62–94
5. Bertino, E., Bettini, C. and Samarati, P.: A Discretionary Access Control Model with Temporal Authorizations. Proceedings of the 1994 Workshop on New Security Paradigms (1994) 102–107
6. Bertino, E., Bettini, C. and Samarati, P.: A Temporal Authorization Model. Proceedings of the 2nd ACM Conference on Computer and Communications Security (1994) 126–135
7. Gal, A. and Atluri, V.: An Authorization Model for Temporal Data. Proceedings of the 7th ACM Conference on Computer and Communications Security, November 1-4 (2000) 144–153
8. Graham, G.S. and Denning, P.J.: Protection – Principles and Practice. Proceedings of the Spring Joint Computer Conference, May 16–18 (1972) 417–429
9. Lampson, B.W.: Protection. Proceedings of the 5th Princeton Symposium on Information Sciences and Systems (March, 1971) pp. 437–443, reprinted in Operating Systems Review, Vol. 8, no. 1 (January 1974) 18–24
10. Weissman, C.: Security Controls in the ADEPT-50 Time-Sharing System. Proceedings of the Fall Joint Computer Conference, November 18–20 (1969) 119–133