Towards a Location-Based Mandatory Access Control Model

Indrakshi Ray   Mahendra Kumar

Department of Computer Science

Colorado State University

Fort Collins, CO 80523

Abstract

With the growing use of wireless networks and mobile devices, we are moving towards an era where location information will be necessary for access control. The use of location information can be used for enhancing the security of an application, and it can also be exploited to launch attacks. For critical applications, such as the military, a formal model for location-based access control is needed that increases the security of the application and ensures that the location information cannot be exploited to cause harm. In this paper, we show how the Mandatory Access Control (MAC) model can be extended to incorporate the notion of location. We show how the different components in the MAC model are related with location and how this location information can be used to determine whether a subject has access to a given object. This model is suitable for military applications consisting of static and dynamic objects, where location of a subject and object must be considered before granting access.

1 Introduction

With the increase in the growth of wireless networks and sensor and mobile devices, we are moving towards an age of ubiquitous computing where location information will be an integral part of many applications. Denning, MacDoran [9] and other researchers have described how the use of location information can make applications more secure. For instance, a user should be able to control or fire a missile from specific high security locations only. Verifying the location information in addition to the checks that are performed by traditional methods of authentication and access control will improve the security of the underlying application. Location information, however, can also be misused causing a breach of privacy and security. For example, information about the location of a user can compromise his privacy. If a malicious user knows about the location information of a person, he/she can infer the activities being performed by that person. Protecting the confidentiality, integrity, and availability of location information is of utmost importance. These issues have also been emphasized by the United States government through the "Wireless Protection Act of 2003" from the 108th Congress [1]. This act requires explicit consent from the users before using their location information and other sensitive information. The bill also mandated that the wireless carriers "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the information."

Understanding the security and privacy implications of location information is non-trivial. Researchers [22, 23, 26, 28, 29] are investigating various problems related to the security and privacy of location-based systems. Some researchers in security and privacy have investigated how to maintain the confidentiality of location information and control its disclosure. Others have focussed on validating the location data transmitted by devices, such as, sensors and active badges, and maintaining the integrity of such data. Some have investigated the availability issues for location data. An effective denial of service attack can be launched by either jamming the Global Positioning System (GPS) or by feeding the GPS receiver fake

information [10, 23]. Although all the above problems are important and need to be adequately addressed, we focus only on protecting the confidentiality of location information.

We show how location information can be used to augment traditional access control in order to cater to more sophisticated applications. Few examples will help to motivate our work. In a military application, if a computer containing top secret information is placed in a public place, then the computer should automatically become inaccessible. A critical application, that is involved with the firing of missiles, may have the following requirements: A user should be able to control or fire a missile from specific high security locations only. Moreover, the missile can be fired only when it is in a certain location. For such critical applications, we need additional checks, such as verification of the location of the user and the location of the missile, that must be satisfied before the user is granted access. Such checks based on location are not provided by the traditional access control models, such as Discretionary Access Control (DAC) or Mandatory Access Control (MAC).

The above examples illustrate how the use of location information can increase the security of an application. The misuse of location information can also cause a breach of security. Thus, the use of location information must be carefully controlled to prevent malicious users from launching attacks. Such attacks may have disastrous consequences for critical applications, such as the military. In short, formal models are needed for performing location-based access control. One can reason about such formal models to ensure that the use of location information is as intended.

In this paper we propose one such formal model that is suitable for military applications. Rather than developing such a model from scratch, we illustrate how the MAC model proposed by Bell-LaPadula [2] can be extended to incorporate the concept of location. We show how to control the disclosure of location information of subjects and objects in order to prevent any illegal information flow. We illustrate how the different components in MAC are related with location and how location impacts these different components. Finally, we show how this location information can be used to determine whether a subject has access to a given object. The correct behavior of the model is formulated in terms of constraints that must be satisfied by any application using this model.

The remainder of the paper is organized as follows. Section 2 provides some background information. Specifically, Section 2.1 summarizes the MAC model on which our work is based and Section 2.2 enumerates some approaches to location representation and determination. Section 3 illustrates how we represent location in our model, how locations can be associated with security levels, and how to protect location information. Section 4 shows how the different components of MAC are related with location and the constraints that location-based access control imposes on these components. Section 5 mentions some work related to this area. Section 6 concludes the paper with pointers to future directions.

2   Background

2.1   Mandatory Access Control

Since our work is based on MAC, we present the main features of the MAC model. The Mandatory Access Control framework that we use is adapted from the Bell-LaPadula model [2]. The Bell-LaPadula model is defined in terms of a security structure $(\mathbf{L}, \preceq)$ where $\mathbf{L}$ represents the set of security levels, and $\preceq$ is an ordering relation defined on these levels. The ordering relation is known as the dominance relation and it is reflexive, transitive and anti-symmetric. $L_i \preceq L_j$ signifies that level L_i is dominated by L_j and L_i is referred to as the dominated relation and L_j as the dominating relation. Two levels L_i and L_j are incomparable if neither $L_i \preceq L_j$ nor $L_j \preceq L_i$.

The main components of this model are objects, users, and subjects. Objects contain or receive information. Each object in the Bell-LaPadula model is associated with a security level which is called the classification of the object. Users, in this model, refer to human beings. Each user is also associated with

a security level that is referred to as the clearance of the user. A user can log in at any security level that is dominated by the security clearance of the user. Each user is associated with one or more subjects. Subjects are the processes that are executed on behalf of some user logged in at a specific security level. The security level of the subject is the same as the level at which the user has logged in.

The mandatory access control policies in the Bell-LaPadula model are specified in terms of subjects and objects and the security levels of these subjects and objects. Let the function L map an entity to its security-level. The policies for reading and writing objects are given by the Simple Security and Restricted-$\star$ Properties. We use the Restricted-$\star$ properties instead of the $\star$ property for reasons of integrity. The Simple Security Property and the Restricted-$\star$ properties are defined below.

1. *Simple Security Property*: A subject S is allowed to read object O only if the security level of the subject $L(S)$, dominates the security level of the object $L(O)$, that is, $L(O) \preceq L(S)$.

2. *Restricted-$\star$ Property*: A subject S is allowed to write to an object O only if the security level of the object $L(O)$ equals the security level of the subject $L(S)$, that is, $L(O) = L(S)$.

2.2 Location Determination and Representation

In this section we give some background on how location can be determined and represented. First, we discuss location determination and then talk about location representation.

2.2.1 Location Determination

In location-based access control, it is extremely important to accurately determine the location of users and objects. There are different technologies for doing this. In the following we describe two ways in which the location can be accurately determined.

1. **Location Determination through GPS:**
   The location of an object or user can be determined through the GPS system. The object whose location we are trying to determine must have a GPS locating device which communicates with different satellite constellations to determine its location. The GPS covers a very wide area and the location information is accurate to within a few meters [9]. Although the GPS was originally used only by military organizations, it is now being used by commercial organizations as well.

2. **Location Determination through Infra-Red Sensors:**
   If an organization is located inside a building, infra-red sensors can be used for location detection. In such cases, the infra-red sensors occupy fixed positions within a building. All the sensors are interconnected by means of a fast communication network. To determine the location of a user or an object, each user or an object must be attached with an infra-red transponder which periodically transmits infra-red messages to the sensors [16]. The messages sent across the sensors are encrypted for reasons of security. This approach is suitable for applications where location precision is important.

2.2.2 Location Representation

There are three ways in which location can be represented. Each of these is discussed below.

1. **Universal Geometrical Co-ordinates**
   In this approach a location is represented as a set of n-dimensional co-ordinates where $n = 2$ or 3. For instance, the GPS system represents a location by its latitude and longitude [20][27]. The reference frame of such a co-ordinate system is the universe and no two distinct places can have the same

co-ordinates. The set of co-ordinates representing a large location may be very big. In such cases, instead of storing the set of all co-ordinates, we can store a few co-ordinates and some information from which the rest of the co-ordinates can be calculated. For instance, if the location is a sphere we store the center of the sphere and the radius. The advantage of representing locations using co-ordinates is that it is easy to perform mathematical operations on location data. The disadvantage is that the location data is hard to interpret.

2. **Symbolic Representation**
   In this approach each location is represented using a symbolic name. Examples include USA, Colorado, Larimer County and Fort Collins. Different locations are arranged in the form of a hierarchy to enable one to reason about location information, such as, if one location is contained in another or whether two locations overlap. The advantage of this approach is that the information about location can be easily interpreted by the users. The disadvantage is that managing the information is non-trivial. For instance, when the physical location associated with a symbolic name changes, the hierarchical relationships need to be recalculated. Also, finding relationships between locations, such as, if one location is contained within another, is more time consuming than using geometrical co-ordinates. Moreover, certain operations, such as the calculation of the distance between two locations, cannot be performed using the symbolic approach.

3. **Hybrid Representation**
   The geometrical and the symbolic representations have different advantages and disadvantages. A hybrid approach can be used which combines the advantages of the geometric and the symbolic representations. In such cases a mapping has to be maintained between the symbolic names and the geometric coordinates [20]. The users' can pose queries using the symbolic location which will internally be converted to a query using the geometric location and evaluated, the result will be converted to a symbolic name and returned to the user.

3   Our Approach to Location Formalization

In order to perform location-based access control, we need to perform operations on location information and protect the location information. In this section we formalize the concept of location, discuss the relationship of location with security levels, and show how the location information can be protected.

   We begin by formalizing the concept of location. Locations can be specified at different levels of granularity. The smallest granularity of location is a point. A location is formally defined as follows.

Definition 1 [Location] A location Loc_i is a non-empty set of points $\{p_i, p_j, \ldots, p_n\}$.

   We define two kinds of relations that may exist between a pair of locations. The first is the containment relation and the second one is the equality relation. The containment relation formalizes the idea whether one location is enclosed by another. The equality relation determines whether a given pair of locations are the same. These are formally defined below.

Definition 2 [Containment Relation] Location Loc_j is said to be contained in Loc_k, denoted as, $Loc_j \subseteq Loc_k$, if the following condition holds: $\forall p_i \in Loc_j, p_i \in Loc_k$. The location Loc_j is called the contained location and Loc_k is referred to as the containing or the enclosing location.

Definition 3 [Equality Relation] Two locations Loc_i and Loc_j are equal, denoted as $Loc_i = Loc_j$ if $Loc_i \subseteq Loc_j$ and $Loc_j \subseteq Loc_i$.
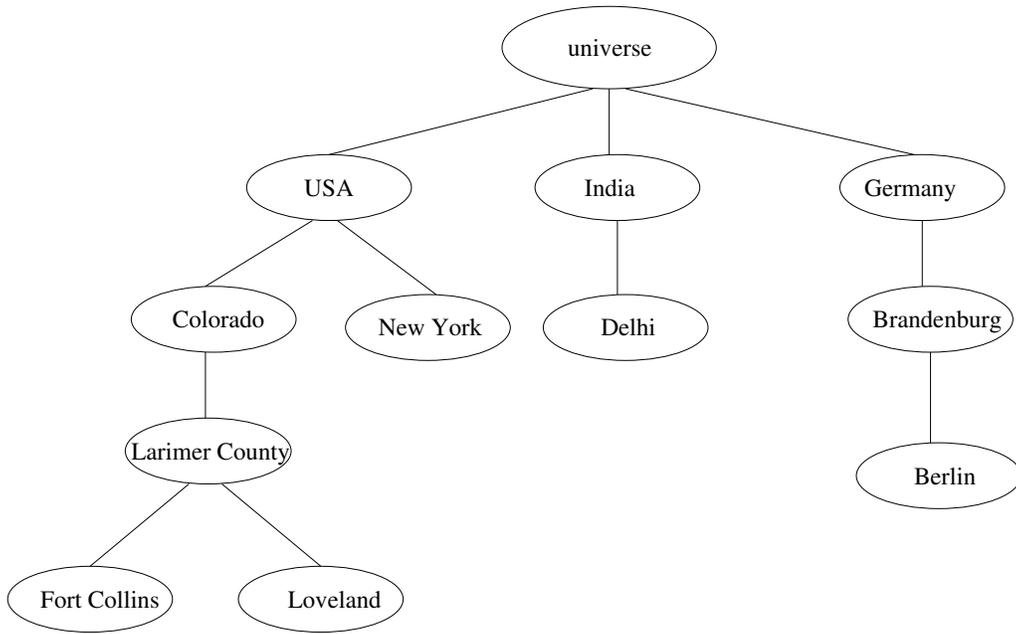
Figure 1: Example of a Location Hierarchy

We denote the set of all locations as **Loc**. The locations form a partial order where the ordering is described by the containment relation $\subseteq$. Since the set of locations **Loc** form a partial order, they can be arranged in the form of a hierarchy. If $Loc_i \subseteq Loc_j$ and $Loc_i \neq Loc_j$, then Loc_j is higher up in the hierarchy than Loc_i and Loc_j is said to be an ancestor of Loc_i. If $Loc_i \subseteq Loc_j$ and there is no Loc_k such that $Loc_i \subseteq Loc_k \subseteq Loc_j$, then Loc_j is said to be the parent of Loc_i. The root of this hierarchy is occupied by a special location termed "*universe*" that contains every other location. An example of location hierarchy is given in Figure 1.

3.1 Association of Location with Security Level

In the real-world, locations are associated with security levels. This is done to ensure that only personnel with the appropriate clearance level can enter a particular location. For instance, public places are associated with a security level of "unclassified" and can admit any person. On the other hand, a room containing top secret information has a security level of "top secret". Only people with security clearance of top secret can enter such a room.

Each location is associated with a single security level. Each security level can be associated with multiple locations. Two locations related by the containment relation may have different security levels. Specifically, a location contained in another might have a higher classification level than the enclosing location. For instance, a building might be designated as top secret but the street in which this building is located is unclassified. A top secret building, on the other hand, will not have any unclassified rooms. This we capture as a constraint in our model which requires that the security level of a containing location is dominated by the security level of a contained location. This constraint is formally specified below:

Constraint 1 $\forall Loc_i, Loc_j \in \mathbf{Loc} \bullet Loc_i \subseteq Loc_j \Rightarrow L(Loc_j) \preceq L(Loc_i)$

The above constraint implies that if a location is made up of other locations, then the security level of the location is dominated by the greatest lower bound of the security levels of the contained locations.
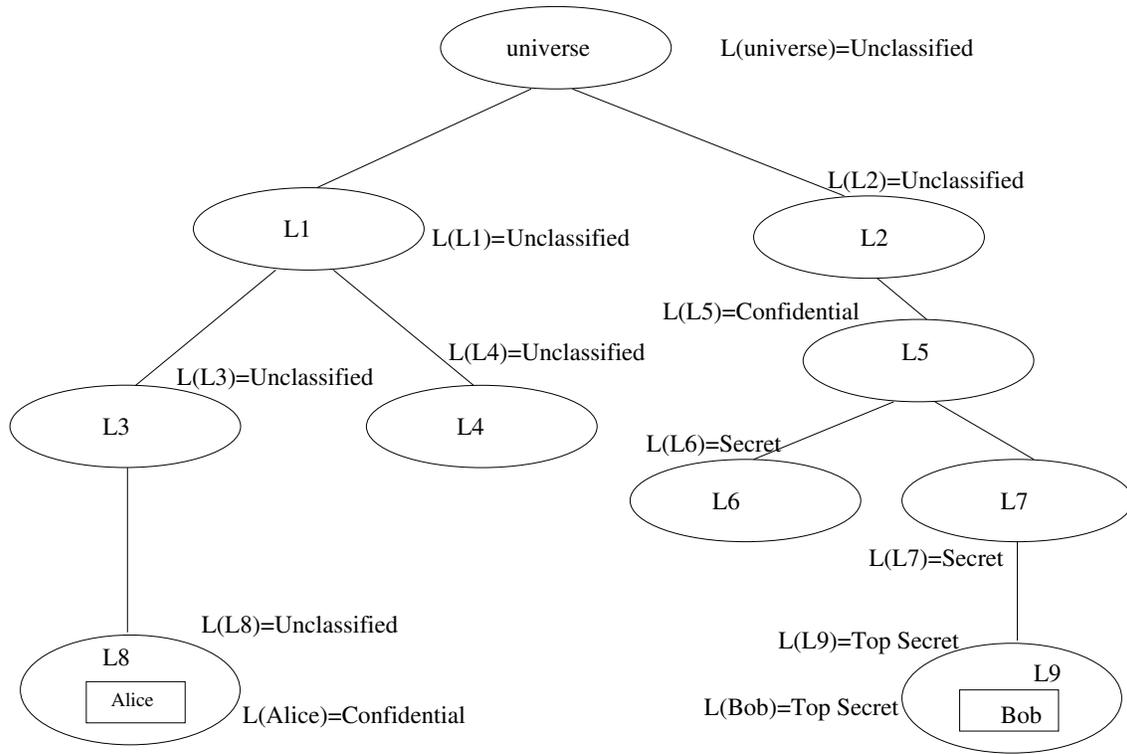
Figure 2: Example of Location Visibility

The constraint also implies that the location *universe* has a security level that is dominated by all the other security levels. These two conditions are written formally as follows.

1. $L(Loc) \preceq glb(L(Loc_i))$ where $Loc_i \subseteq Loc$ and $1 \leq i \leq n$

2. $L(universe) \preceq L_k$ where $L_k \in \mathbf{L}$ and $\mathbf{L}$ is the set of all security levels.

3.2 Access to Location Information

The information about location is sensitive in nature. The location information of a user or an object should not be disclosed in an uncontrolled way for reasons of privacy and security. For instance, the information about the location of weapons should not be disclosed to everyone. Alternately, if several top secret clearance users are in a top secret location and this information is revealed then this may cause a security breach.

Let us illustrate this with an example. Alice and Bob are two users having confidential level and top secret level clearance respectively. Alice logs on at the confidential level and queries about the location of Bob. Bob is in a top secret location. If his location information is revealed to Alice, then Alice might infer about the activities of Bob.

One might argue that since the location of Bob is top secret, the information about Bob's location should be treated as a top secret object. However, we cannot treat the location information as any top secret object. In general a secret level subject should not be aware of any top secret level object, but in this case the secret level subject (executing on behalf of Alice) is aware of the existence of this object (location of Bob). Thus, she can pose queries about this object and expect some answers in return. What answer should be given to Alice? Not giving an answer to Alice is not an option because the absence of an answer can be used as a covert channel or an inference channel.

In general, this problem will occur when a subject queries about the location information of an entity and the security level of the location information dominates the level of the subject. Our solution to this problem is to return an answer to the subject about the location information. The answer that is returned to the subject in response to a query about the location of an entity is referred to as the *visible location*. The formal definition of location visibility is given below.

Definition 4 [Visible Location] The *visible location* of an entity E, denoted as Loc_{v_E}, is the location information that is returned to the subject S in response to a query about the location of the entity E. The actual location of entity E is denoted by Loc_E. Loc_{v_E} should satisfy the following properties:

1. $L(Loc_{v_E}) \preceq L(S)$

2. $Loc_E \subseteq Loc_{v_E}$

3. $\nexists Loc_x \bullet (L(Loc_x) \preceq L(S) \wedge Loc_E \subseteq Loc_x \subseteq Loc_{v_E})$

The first property states that the security level of the subject S should dominate the security level of the visible location Loc_{v_E}. The second property says that the visible location Loc_{v_E} should contain the actual location Loc_E. The third property states that if Loc_{v_E} is the visible location, then there is no location contained in Loc_{v_E} that satisfies the first two properties. In other words, the third property ensures that the nearest ancestor location having a security level that is dominated by the level of the subject is the visible location.

We give a very simple algorithm that evaluates the visibility of the location. The algorithm goes up the location hierarchy to search for the containing location whose security level is dominated by the subject.

Algorithm 1 Evaluating the Visible Location
Input: (i) $L(S)$ – the level of the subject for which we are determining the visible location, (ii) LH – location hierarchy, and (iii) Loc_E – actual location of entity.
Output: Loc_{v_E} – visible location suitable for subject S

begin
      $node = Loc_E$
      while $(L(node) \npreceq L(S))$
            $node = getParent(node, LH)$ /* gets the parent of Loc_E from LH */
      return node
end

Suppose the example involving Alice and Bob have location hierarchies as shown in figure 2. When Alice logged in at the confidential level queries the location of Bob, then the actual location of Bob *L9* should not be disclosed because he is in a top secret location. Proceeding up the hierarchy, we find location *L7* cannot be disclosed either because its level dominates the level of the subject initiated by Alice. We then proceed to the next containing location which is *L5*. The security level of *L5* is dominated by the level of the subject executing on behalf of Alice, so *L5* will be returned to the user. Note that, although *L2* satisfies the first two properties of visible location, it does not satisfy the third property and so it is not a valid visible location.

Theorem 1 The algorithm for finding the visible location is correct.

Proof 1 For proving the correctness of the algorithm, we need to show that the location returned by the algorithm satisfies all the properties listed in Definition 4. The while loop in the algorithm gets executed

until the first property is satisfied. Each iteration of the while loop traverses up the location hierarchy to fetch a containing location. By Constraint 1 the security level of the containing location is dominated by the security level of the contained location. The security level of the root node is dominated by all the other security levels including the level of the subject. This guarantees that eventually a location will be found whose level is dominated by the level of the subject. In other words, this guarantees termination of the while loop thereby ensuring the satisfaction of the first property. Since we traverse up the location hierarchy to find the visible location, the second property will also be satisfied. Note that, the while loop is exited as soon as a containing location is found whose security level is dominated by the level of the subject. This ensures the satisfaction of the third property.

Theorem 2 The complexity for finding visible location is $O(n)$ where n is the maximum number of edges from the leaf to the root of the location hierarchy LH.

Proof 2 The algorithm in the worst case travels from the leaf to the root and returns the root as the visible location. The number of nodes traversed equals n and so the worst case complexity is $O(n)$.

4 Extending MAC to Incorporate Location-Based Access Control

In this section we show how MAC can be extended to incorporate location-based access control. The different components of MAC are *user*, *subject*, *object* and *operations*. We discuss how each of these components are associated with location. Figure 3 illustrates how these components are related with location. The multiplicity of these relationships are indicated by presence or absence of an arrowhead. The absence of an arrowhead indicates a multiplicity of "one" and the presence of arrowhead indicates a multiplicity of "many". We formalize these relationships and list the constraints imposed by our model.

4.1 Users

We assume that each user carries a locating device which is able to track the location of a user. The association between user and location is indicated by the edge labeled with *UserLocation* in Figure 3. Each user is associated with a location at any given instant of time. However, a single location may be associated with multiple users. For reasons of security, a user is permitted to enter a location whose security level is dominated by the clearance level of the user. This is enforced as a constraint in our model.

Constraint 2 $L(Loc_U) \preceq L(U)$ where U is a user and Loc_U is the location of the user.

4.2 Subjects

In our model, the location of a subject is checked before granting the subject access to some object. This provides additional protection and ensures that no remote hacker can impersonate an authorized user and execute operations on his behalf. Thus, each subject is associated with a location which is the same as the the location of the user that initiated the subject. A single location, however, can be associated with multiple subjects. This relationship is indicated by the labeled edge *SubjectLocation* in Figure 3.

We have said that the location of a subject is the same as the location of the user that initiated the subject. However, one point needs to be mentioned. A top secret user can enter unclassified areas, but we should not allow top secret subjects to be executed in unclassified locations. This is because permitting top secret subjects to execute in unclassified locations can cause a security breach. For instance, the unclassified locations can have hidden devices that track the activities taking place in this location. If a top secret level activity is taking place in this location, it can be recorded and this information passed on to unclassified
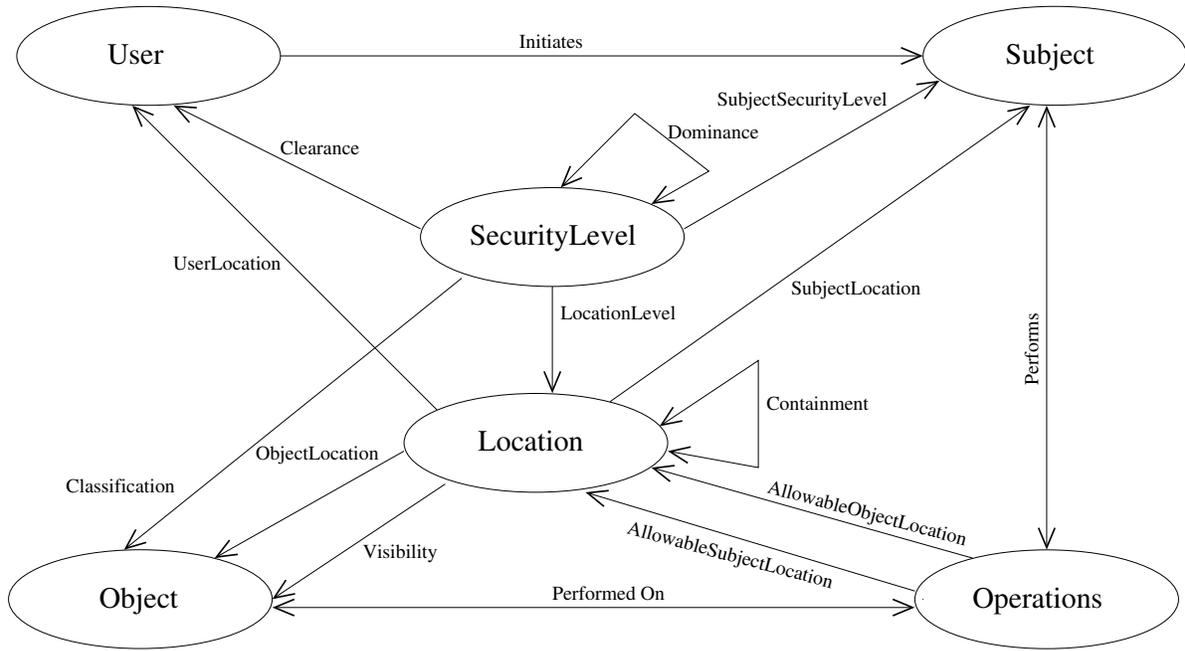
Figure 3: Relationship of MAC Components with Location

subjects. Thus, a top secret level user can initiate a top secret subject only in a top secret location. However, allowing a top secret user to initiate an unclassified subject from a top secret location does not pose any problem.

These requirements are summarized in the constraint given below. The first conjunct enforces the restriction that the level of the subject S initiated by user U is dominated by the user's clearance level. The second conjunct specifies that the location of the subject is the same as the location of the user who initiated the subject. The third conjunct requires that the user can initiate a subject in a location that dominates the level of the subject.

Constraint 3 $L(S) \preceq L(U) \; \wedge \; Loc_S = Loc_U \; \wedge \; L(S) \preceq L(Loc_S)$ where S is the subject initiated by user U, Loc_U is the location of the user and Loc_S is the location of the subject.

4.3 Objects

Objects can be physical or logical. Example of physical object is a computer. Files are examples of logical objects. Physical objects have devices that transmit their location information. Logical objects are stored in physical objects. The location of a logical object is the location of the physical object containing the logical object. Logical objects, such as, a distributed database, can be contained in different physical objects. In such cases the location of the logical object is the set of points associated with these different physical objects. As shown by the association *ObjectLocation* in Figure 3, each location can be associated with many objects, but an object is associated with only one location.

To protect an object, it should be stored in locations whose security level dominates the level of the object. For instance, documents labeled top secret should not be stored in unclassified locations; otherwise, people not having a security clearance may have access to this object. This is enforced as a constraint in our model.

Constraint 4 $L(O) \preceq L(Loc_O)$ where O is the object and Loc_O is the location of the object.

An object can be composed of other objects. Let object O be composed of objects $O_1, O_2, \ldots, O_n$. Suppose the individual objects have different security classifications and the security level associated with O_i is $L(O_i)$. The security classification of object O must dominate the security classification of each of these individual objects. In other words, $lub(L(O_1), L(O_2), \ldots, L(O_n)) \preceq L(O)$. The different components, O_1, $O_2, \ldots, O_n$, of a composite object O may be stored in different locations. Let $Loc_{O_1}, Loc_{O_2}, \ldots, Loc_{O_n}$ be the different locations associated with these components. These locations can be associated with different security levels. Since locations $Loc_{O_1}, Loc_{O_2}, \ldots, Loc_{O_n}$ are contained in Loc_O, by Constraint 1 $(L(Loc_O) \preceq glb(L(Loc_{O_1}), L(Loc_{O_2}), \ldots, L(Loc_{O_n}))$) To summarize, the following constraint gives the relationships that must be satisfied by any composite object.

Constraint 5 $(lub(L(O_1), L(O_2), \ldots, L(O_n)) \preceq L(O)) \ \wedge \ (L(Loc_O) \preceq glb(L(Loc_{O_1}), L(Loc_{O_2}), \ldots, L(Loc_{O_n}))$ where O_i is a component of composite object O and Loc_{O_i} is the location of O_i and $1 \leq i \leq n$.

4.4 Operations

The operations that a subject performs on an object are classified either as *Read* or *Write*. A read operation on an object discloses the contents of the objects, but does not modify it. A write operation, on the other hand, alters the contents of the object. The Simple Security and the Restricted-$\star$ Property specifies the necessary conditions needed to read or write objects. These conditions, based on security levels, are not enough for performing location-based access.

In location-based access control we must ensure that the subjects and the objects are in specific locations before authorizing the operations. To incorporate location-based access control, we associate every operation op with two locations: allowable subject location Loc_{op_sub} and allowable object location Loc_{op_obj}. These associations are indicated by the edges labeled *AllowableSubjectLocation* and *AllowableObjectLocation* in Figure 3. The location of the subject must be contained in the allowable subject location Loc_{op_sub} and the location of the object must be contained in the allowable object location Loc_{op_obj} in order to get access. Also, the security level of Loc_{op_obj} should be dominated by the level of the object because an object cannot be contained in a location whose level is dominated by the level of the object. Similarly, a subject must be in a location whose security level dominates the level of the subject.

For MAC, operation op can either be a read or a write. The read operation is allowed if the following constraint is satisfied. The first conjunct gives the Simple Security Property. The second and third conjunct verifies whether the subject and the object are located in the allowable locations. The fourth conjunct verifies that the allowable location for the object has a security level that dominates the level of the object. The fifth conjunct verifies that the allowable location for the subject dominates the level of the subject.

Constraint 6 $L(O) \preceq L(S) \wedge Loc_S \subseteq Loc_{read\_sub} \wedge Loc_O \subseteq Loc_{read\_obj} \wedge L(O) \preceq L(Loc_{read\_obj}) \wedge L(S) \preceq L(Loc_{read\_sub})$ where S is the subject wanting to read object O, Loc_S, Loc_O represent the actual locations of the subject, object respectively and Loc_{read_sub}, Loc_{read_obj} give the allowable locations for subject and object in order to perform the read operation.

The constraints for the write operations are similar, except that the Simple Security property is replaced by the Restricted-$\star$ property. These are given below.

Constraint 7 $L(O) = L(S) \wedge Loc_S \subseteq Loc_{write\_sub} \wedge Loc_O \subseteq Loc_{write\_obj} \wedge L(O) \preceq L(Loc_{write\_obj}) \wedge L(S) \preceq L(Loc_{write\_sub})$ where S is the subject wanting to write object O, Loc_S, Loc_O represent the actual locations of the subject, object respectively and Loc_{write_sub}, Loc_{write_obj} give the allowable locations for subject and object in order to perform the write operation.

5 Related Work

Location determination and representation is discussed in various works [4, 12, 13, 18, 19]. Lee, Xu, Zheng and Lee [20] describe different methods to represent location. They propose two representations for location: the Geometrical model and the Symbolic model. They also describe how different types of location-based queries can be processed.

Security and privacy issues pertaining to pervasive computing has been explored in details by Campbell et al. [5]. Sampemane et al. [24] present a new access control model for active spaces. Active space denotes the computing environment integrating physical spaces and embedded computing software and hardware entities. The active space allows interactive exchange of information between the user and the space. Environmental aspects are adopted into the access control model for active spaces, and the space roles are introduced into the implementation of the access control model based on RBAC. The model supports specification of mandatory policies in which system administrator maintains the access matrix and discretionary policies in which users create and update security policies for their devices.

Harter and Hooper [16] describe a distributed location management system for an active office. In their approach the active office is equipped with infra-red sensors and other hardware needed to capture location information. Personnel carry infra-red transponders called badges which communicate with the sensors to obtain the location for the person. The authors present a detailed architecture of this location system.

Covington et al. [8] introduce environment roles in a generalized RBAC model (GRBAC) to help control access control to private information and resources in ubiquitous computing applications. The environment roles differ from the subject roles in RBAC but do have similar properties including role activation, role hierarchy and separation of duty. In the access control framework enabled by environment roles, each element of permission assignment is associated with a set of environment roles, and environment roles are activated according to the changing conditions specified in environmental conditions, thus environmental properties like time and location are introduced to the access control framework. In a subsequent work [7], Covington et al. describes the Context-Aware Security Architecture (CASA) which is an implementation of the GRBAC model. The access control is provided by the security services in the architecture. In CASA, polices are expressed as roles and managed by the security management service, authentication and authorization services are used to verify user credentials and determine access to the system resources. The environmental role activation services manage environmental role activation and deactivation according to the environment variables collected by the context management services.

The geographic location and privacy working group of the Internet Engineering Task Force has proposed some ideas about how location information objects should be made and privacy policies formulated [26]. It allows people to let others track their location through the location objects they publish. Gunter and May [15] formalize privacy system and describe how it can be used in location-based services. They argue why the traditional Graham/Denning's model [14] is not adequate for specifying privacy policies and propose a new model that can be used to express and reason about privacy.

Denning and MacDoran [9] propose many motivating examples as to why location-based security is important for applications. Their argument is that use of location information can enhance the security of applications. The authors discuss how location-based authentication can be achieved using GPS and a tool called Cyberlocator.

Hengartner and Steenkiste [17] design an access control mechanism for a people location system. The authors say that an individual is associated with two kinds of location policies. The first are the location policies that are specified by individuals. The second are the policies that are specified by institutions. For instance, if a person is at the mall, his individual location policies are in effect. When he is at work, the institutional policies of the organization are in effect. The access control policy relies on the use of digital certificates. When a user requests the location of another entity, his digital certificates are checked to make sure that he is given the information that he is entitled to view.

Leonhardt and Magee [21] discuss how location-based access can be provided over existing matrix-based access control models and mandatory access control models. The proposed approach consists of three parts: controlling access, controlling visibility and controlling anonymity. The visibility policy specifies what location information gets returned to the user who is querying about the location of an entity. The anonymity policy specifies what information gets returned to the user querying about some other user. The access policy specifies how location information can be used to control access. Although this paper has presented some nice ideas, it lacks details and formalisms. For instance, the authors do not discuss how the different components of an access control model are impacted by location and what constraints are necessary on the location-based model. In our work we try to address these issues and complement the above mentioned work.

6   Conclusion

In this paper we have proposed a location-based mandatory access control model that is suitable for military applications. In our model, the access a subject has on an object is determined by security levels of the subject and object as well as their location. We are therefore able to provide more security than the MAC model. We have extended the MAC model by incorporating the notion of location and identifying what relationship location has with the other components of the MAC model. We also analyzed the impact that location has on these components and formalized acceptable behavior in the form of constraints that must be satisfied.

A lot of work remains to be done. In future, we plan to propose a set of necessary properties for location-based access control models, and formally show that our model does indeed satisfy these properties. This model did not consider the temporal aspects of location. For instance, the location of a user or the location of a mobile object changes with time. We need to incorporate how location information changes with time and what impact this has on the underlying model. This work focused on a model suitable for military applications. In future, we plan to augment the access control models used for commercial applications, such as Chinese-Wall [3, 25], Clark-Wilson [6], and Role-Based Access Control [11], to enable them to perform location-based access.

Acknowledgment

References

[1] The Wireless Privacy Protection Act, 2003.

[2] D. E. Bell and L. J. LaPadula. Secure computer system:unified exposition and MULTICS. Technical Report ESD-TR-75-306, The MITRE Corporation, Bedford, MA, 1976.

[3] D. F. C. Brewer and M. J. Nash. The Chinese Wall Security Policy. In *Proceedings of the IEEE Symposium on Security and Privacy* , pages 215–228, Oakland, CA, USA, May 1989.

[4] Jay Cadman. Deploying Commercial Location-Aware System. In *Proceedings of the Workshop on Location-Aware Computing (UbiComp)*, Seattle,Washington,USA, October 2003.

[5] R. Campbell, J. Al-Muhtadi, P. Naldurg, G. Sampemane, and M.D. Mickunas. Towards Security and Privacy for Pervasive Computing. In *Proceeding of the International Symposium on Software Security*, Tokyo, Japan, 2002.

[6] D. R. Clark and D. R. Wilson. A Comparison of Commercial and Military Computer Security Policies. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 184–194, Oakland, CA, USA, May 1987.

[7] Michael J. Covington, Prahlad Fogla, Zhiyuan Zhan, and Mustaque Ahamad. A Context-Aware Security Architecture for Emerging Applications. In *Proceedings of the Annual Computer Security Applications Conference*, pages 249–260, Las Vegas, NV, USA, December 2002.

[8] Michael J. Covington, Wende Long, Srividhya Srinivasan, Anind Dey, Mustaque Ahamad, and Gregory Abowd. Securing Context-Aware Applications Using Environment Roles. In *Proceedings of the 6th ACM Symposium on Access Control Models and Technologies*, pages 10–20, Chantilly, VA, USA, May 2001.

[9] Dorothy E. Denning and Peter F. MacDoran. Location-Based Authentication:Grounding Cyberspace for Better Security. In *Proceedings of the Computer Fraud and Security,Elsevier Science Ltd*, February 1996.

[10] P. Enge and P. Misra. Scanning the Issues/Technology. *Proceedings of the IEEE, Special Issue on GPS*, 87(1):11, January 1999.

[11] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. Proposed NIST Standard for Role-Based Access Control. *ACM Transaction on Information and System Security*, 4:224–274, 2001.

[12] Dieter Fox, Jeffrey Hightower, Henry Kauz, Lin Liao, and Donald J. Patterson. Bayesian Techniques for Location Estimation. In *Proceedings of the Workshop on Location-Aware Computing (UbiComp)*, Seattle,Washington,USA, October 2003.

[13] Richard James Glassey and Robert Ian Ferguson. SpaceSemantics: An Architecture for Modeling Environments. In *Proceedings of the Workshop on Location-Aware Computing (UbiComp)*, Seattle,Washington,USA, October 2003.

[14] G.S. Graham and P.J. Denning. Protection: Principle and Practices. In *Proceedings of the AFIPS Spring Joint Computer Conference*, pages 4127–429, 1972.

[15] Carl A. Gunter, Michael J. May, and Stuart G. Stubblebine. A Formal Privacy System and its Application to Location Based Services. In *Proceedings of the Workshop on Privacy Enhancing Technologies*, Toronto, Canada, May 2004.

[16] Andy Harter and Andy Hopper. A distributed location system for the active office. *IEEE Network*, 8(1), January 1994.

[17] Urs Hengartner and Peter Steenkiste. Implementing Access Control to People Location Information. In *Proceeding of the Symposium on Access Control Methodologies and Technologies (SACMAT)*, Yorktown Heights,California,USA, June 2004.

[18] Jeffrey Hightower. From Position to Place. In *Proceedings of the Workshop on Location-Aware Computing (UbiComp)*, Seattle,Washington,USA, October 2003.

[19] John Krumm. Probabilistic Inferencing for Location. In *Proceedings of the Workshop on Location-Aware Computing (UbiComp)*, Seattle,Washington,USA, October 2003.

[20] Dik Lun Lee, Jianliang Xu, Baihua Zheng, and Wang-Chien Lee. Data management in location-dependent information services. *IEEE Pervasive Computing*, 1(3):65–72, July-Sept. 2002.

[21] Ulf Leonhardt and Jeff Magee. Security Consideration for a Distributed Location Service. *Network and Systems Management*, 6(1):51–70, March 1998.

[22] A. Perrig, J. Stankovic, and D. Wagner. Security in Wireless Sensor Networks. *Communications of the ACM, Special Issue: Wireless Sensor Networks*, 47(6):53–57, 2004.

[23] John A. Volpe National Transportation Systems Center Report. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, August 2001.

[24] Geetanjali Sampemane, Prasad Naldurg, and Roy H. Campbell. Access Control for Active Spaces. In *Proceedings of the Annual Computer Security Applications Conference*, pages 343–352, Las Vegas, NV, USA, December 2002.

[25] R. S. Sandhu. Lattice-Based Enforcement of Chinese Walls. *Computers & Security*, 11(8):753–763, December 1992.

[26] H. Schulzrinne, J. Morris, H. Tschofenig, J. Cuellar, and J. Polk. Policy Rules for Disclosure and Modification of Geographic Information, 2003.

[27] Steven A. N. Shafer. Location Authorities for Ubiquitous Computing. In *Proceedings of the Workshop on Location-Aware Computing (UbiComp)*, Seattle,Washington,USA, October 2003.

[28] E. Snekkenes. Concepts for Personal Location Privacy Policies. In *Proceedings of the Third ACM Conference on Electronic Commerce*, pages 48–57, 2001.

[29] L. Titkov, S. Poslad, and J. J. Tan. Enforcing Privacy via Brokering within Nomadic Environment. In *Proceedings of the AT2AI-04 Symposium at the 17th European Meeting on Cybernetics and Systems Research*, 2004.