RC 21673 (97655) 22 February 2000
Computer Science/Mathematics

IBM Research Report

Multi-Organizational Mandatory Access Controls for Commercial Applications

Paul A. Karger
IBM Research Division
Thomas J. Watson Research Center
P. O. Box 704
Yorktown Heights, NY 10598

Research Division
Almaden - Austin - Beijing - Delhi - Haifa - T.J. Watson - Tokyo - Zurich

Multi-Organizational Mandatory Access Controls for Commercial Applications

Paul A. Karger
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598

22 February 2000

Paper submitted to the 23rd National Information Systems Security Conference
Keywords: mandatory access controls, lattice security model, universal access classes, organizational access classes, Bell and LaPadula model

ABSTRACT

This paper extends mandatory access controls to meet multi-organizational commercial security requirements. It defines a universal access class that can represent the security needs of two or more independent organizations that may be cooperating on a joint proprietary project. It can distinguish information that is proprietary to each of the organizations and information that is shared between these organizations, but must remain secret from all others. The paper shows how the current way the US Department of Defense (DoD) and Department of Energy (DoE) share classified information does not sufficiently generalize for the commercial world. By contrast, the new universal access class scheme can adequately model both the commercial world and the requirements of the DoD and DoE.

1.0 Introduction

For lattice security models to be successful in a commercial Internet environment, one needs to support potentially billions of different secrecy categories to allow each corporation in the world to define a reasonably large number of its own. Just as IP Version 4 had to expand its address representation in IP Version 6 to support sufficient network addresses, any kind of lattice security model must support billions of categories. By contrast, a single system that supports a lattice model might only support a small

number of categories. For example, Multics, the first commercial system to support a lattice security model permitted only eight secrecy levels and eighteen categories [7]. These numbers were chosen to meet the needs of the Air Force Data Services Center (AFDSC), the first military organization to use Multics security to protect classified information against potentially hostile attack. The categories were represented as a simple 18-bit field, with one bit for each category. This number of categories was sufficient to meet AFDSC needs, but even at that time, this number was clearly insufficient to meet the needs of an intelligence agency that uses huge numbers of categories.

Of course, any one machine would only need a small number of categories, but world-wide, there must be an unambiguous representation of such categories to ensure that controlled sharing is possible between any two organizations. This requirement was first elucidated in [6, chapter 10] and in [5]. In such a world-wide lattice security model, there could easily be millions of different categories, and the bit map with one bit per category would quickly become impractical. Therefore, the category list representation was proposed in [6, chapter 10].

This paper examines the requirements of both defense organizations and commercial organizations and proposes a new scheme for inter-organizational access classes that can better model the real world in which the lattice security model of one organization may not map well into the lattice security model of another organization, yet the two organizations may still wish to connect to the Internet and ensure that their respective lattice security policies are properly enforced. They may even wish to permit an exchange of certain sensitive documents, in accordance with mutually agreed upon non-disclosure agreements which in turn could result in documents that must be marked with lattice attributes from both organizations.

2.0 What is Really Required?

2.1 Defense Requirements

The traditional view of lattice security models has been based on the US Department of Defense's (DoD's) use of lattice security. The DoD has a single set of secrecy levels: Unclassified, Confidential, Secret, and Top Secret. They also have a very large number of categories, primarily used within the intelligence community, but also used to protect nuclear war plans, cryptography, etc. Most data is so-called collateral data that is not in any category at all, but some data may be in multiple categories. For example, a single document might be classified Secret with categories apples, bananas, and cherries[1]. To read such a document, a person must have a secret security clearance, and further must be authorized all three categories. A person with a Top Secret clearance but only authorized

[1] Since many real category names are themselves sensitive information, we use artificial category names for this example.

apple and banana information, would not be allowed to read the document, because he or she is not authorized for cherry information.

The Department of Energy (DoE) Weapons Laboratories use a similar security model, but their secrecy levels are different from the DoD's, because they were authorized under different legislation. DoE levels are Secret, L, Top Secret, Q Nonsensitive, and Q Sensitive [2]. The DoE also uses a large number of categories. The most significant point, however, is that the secrecy levels are different from DoD levels. Secret and Top Secret come from the DoD classification scheme, while L and Q are DoE-specific.[2] An L clearance implies access to DoD Secret information, and Q clearance implies access to DoD Top Secret information.

When one looks at lattice security models in international treaty organizations (such as NATO), the lattice becomes yet more complex, as different countries have their own definitions of secrecy levels.

The DoD lattice security model has undergone much evolution since the early 1970s when the Multics representation was developed. The list of categories representation has been adopted in the MISSI Access Control Concept [3] as their *Security Tag Type 2 (Enumerated Type)*. The Multics-style of one bit per category is the MISSI *Security Tag Type 1 (Restrictive Bit Map Type)*.[3]

2.2 Commercial Requirements

Most commercial organizations have less well organized security models than do defense organizations. However, most companies do recognize at least two levels of sensitive information – Company Confidential and non-confidential information. Some companies have more than two levels. For example, IBM used to have several levels of confidential information (Internal Use Only, IBM Confidential, IBM Confidential – Restricted, and IBM Registered Confidential), although that was recently reduced to just IBM Confidential. Few companies use formal categories, with the exception of personnel-related data.

However, if two or more companies are cooperating on a project, with mutual non-disclosure agreements covering confidential information, this cooperation can be expressed in a category-based security model that identifies which documents contain company A confidential information, which contain company B confidential information,

[2] The purpose of this paper is NOT to criticize how DoD and DoE map their classification systems together. The present scheme has been in use for many years and clearly meets the needs of these two cabinet-level departments. The purpose of this paper is to show that the mapping scheme that DoD and DoE have devised, while well-suited for their specific needs, does not generalize well to the broader requirements of the commercial world.

[3] MISSI also supports a *Permissive Bit Map Type* that are used for release markings and caveats and a *Free Form Field* that is used for informational purposes only. These types of markings are beyond the scope of this paper. Examples of their use can be found in Appendix A of [3]

and which contain information confidential to both A and B. Category combinations happen when documents contain confidential information from multiple companies, just as in defense applications.

2.3 Combining Defense and Commercial Requirements

Imagine a multi-application smart card carried by a DoD employee. It might contain DoD classified information, because it controls access to sensitive areas inside the Pentagon. Since the employee works with nuclear weapons, it might also contain DoE classified information. The smart card might also be the employee's government travel card, carrying proprietary information of a corporate credit card company. It might also have a frequent flier application with proprietary information of an airline. That application in turn works with applications that store proprietary information of three different competing rental car companies and five competing hotel chains. The lattice security model on the card must encode security information for all of these organizations.[4]

3. Universal Access Classes

To meet all of these requirements, we must define a world-wide lattice security model that supports a very large number of organizations, at least thousands of categories per organization, and recognition that the hierarchical levels of one organization may have no meaningful mapping to that of another organization. This last requirement is the primary difference from the proposals in [6] and [5]. Those proposed a single set of levels together with a list of up to 2^{32} categories. To meet all of these requirements, we need a more complex definition of an access class. (Note: all access classes will be assumed to be secrecy access classes for the remainder of this document. Integrity access classes will work the same, but for simplicity, this paper will only deal with secrecy.)

A *universal access class* consists of a set of one or more organizational access classes, such that the organizational ID (defined below) of each organizational access class is unique. Table 1 shows a universal access class that contains *N* organizational access classes.

---

[4] The underlying assumption is that this is a VERY secure smart card whose operating system can effectively protect DoD classified information from the frequent flyer applications that have been written by completely uncleared programmers. The purpose of this paper is to examine what kind of lattice security model would such a hypothetical, high-assurance operating system require. The example is smart-card based, because this paper has been written as part of a secure smart card project. However, the model is in no way limited to only smart card applications.

Count of Organizational Access Classes = N
Organizational Access Class 1
Organizational Access Class 2
…
Organizational Access Class N

Table 1. Universal Access Class

We define an *organizational access class* as a 3-tuple consisting of an organizational ID, an organizational secrecy level, and a list of zero or more organizational categories. An organizational access class is shown in Table 2.

Organizational ID	Organizational Secrecy Level
Count of Organizational Categories = P	
Organizational Category 1	
Organizational Category 2	
…	
Organizational Category P	

Table 2. Typical Organizational Access Class

The *organization ID* should consist of two fields, a country code, and an organization number, as shown in Table 3. These should be similar to those defined in ISO/IEC 7816-5 [1]. The organizational secrecy level can be a small integer – 0 to 15 should be sufficient, permitting it to be stored in only 4 bits. Organizations within the US DoD are known to already need thousands of categories, so organizational category numbers should be preferably be represented as 32-bit integers. One could make a case that 24-bit integers are sufficient, but 16-bit integers are clearly too small.

Country Code	Organization Number

Table 3. Organization ID

We reserve one access class with organizational ID 0, organizational level 0, and zero organizational categories to be the level system-low. The level system-high is an access class with one entry for each organizational ID, and for each organizational ID entry, the secrecy level is the highest permitted, and the list of categories includes all categories defined for that organization.

3.1 Comparing Universal Access Classes

Universal access classes form a lattice that could be used in the Bell and LaPadula model [4]. Two access classes can be compared as follows:

Universal access class A is less than or equal to universal access class B if and only if: For each organizational ID in A, there exists a corresponding organizational ID in B, and for each such pair of organizational IDs in A and B, the organizational secrecy level of A is less than or equal to the organizational secrecy level of B, and the set of organizational categories of A is an improper subset of the organizational categories of B.

Universal access class A is equal to universal access class B iff the set of organizational access classes in A and B are exactly identical.

Universal access class B is greater than or equal to universal access class A iff universal access class A is less than or equal to universal access class B.

If universal access classes A and B have neither a less than or equal to, equal to, nor greater than or equal to relationship, then they are disjoint or incomparable.

3.2 Typical Usage

While these universal access classes can be very large, the typical usage will actually be quite compact. Most files contain information from only one organization. Files that contain multiple organization's data will be relatively rare. Furthermore most files in the US DoD have only a secrecy level and no categories. It is anticipated that most files in a commercial context will have only one category.

4.0 Mapping the World-Wide Model into a Limited Memory System

The access classes defined in the world-wide model can potentially require a large amount of space to represent. In any system with a limited amount of memory (such as a smart card), it will be essential to map those access classes to a very small representation that could be stored with each file. As first proposed in chapter 10 of [6], a system can simply assign a short integer to each universal access class that is actually in use, and always look up the integer whenever an access class comparison is required. A typical system might only need a few dozen category combinations at any one time, so the size of the mapping table could be very small indeed. On a smart card system, the short integer need be no bigger than a single 8-bit byte, and the table of mappings could be stored as a sorted list in a file that only maps the access classes in actual use.

5.0 Using Universal Access Classes

5.1 Using Universal Access Classes in the DoD and DoE

Universal access classes can easily represent the current DoD and DoE classification systems in what appears to be a clearer approach than the current mapping strategy. The DoD and the DoE would each be assigned an organizational ID. The DoD's secrecy levels would be Unclassified, Confidential, Secret, and Top Secret. The DoE's secrecy levels would be L, Q non-sensitive, and Q sensitive. If desired, a DoE employee could administratively be assigned a universal clearance that contained two organizational clearances. If the employee had only an L clearance, then the employee could be granted a DoD secret clearance. If the employee had a Q clearance, then the employee could be granted a DoD Top Secret clearance. The new universal scheme could also allow for a DoE employee who was not automatically granted DoD access, unlike the current system.[5]

5.2 Using Universal Access Classes Commercially

In a commercial setting, imagine a frequent flyer application in which a car rental company wishes to share certain selected information with a partner airline, but not with another car rental company that is also partnered with the same airline. Assume the car rental companies in question are Cheapo Rentals and Extravagant Rentals, and the airline is Nocturnal Aviation. The data that Cheapo wishes to share with Nocturnal Aviation would be marked with a universal access class containing organizational access classes of both Nocturnal and Cheapo. Processes running on the system would have to be cleared

[5] The current DoE scheme may allow for DoE-only clearances already. The author of this paper is NOT intimately familiar with the DoE scheme, and does not mean to imply limitations that may not in fact be present.

for both Nocturnal and Cheapo information, and those processes would not have access to Extravagant information.

6.0 Administering the Creation of Access Classes

Administering the creation of access classes must be performed by some trusted third party. ISO/IEC 7816-5 [1] defines such an organization for smart card application IDs. This same organization could also administer access classes. It will be crucial that the trusted third party provide digitally signed certificates to prove that a particular access class together with its organizational IDs is genuine. Application IDs will also require such digital signatures, although the standard does not currently provide for them.

7.0 Conclusions

We have seen that to make effective use of mandatory access controls in a commercial environment, we need a more complex representation of access classes than has traditionally been used in military systems. However, a simple extension of the military systems to define a universal access class that consists of a set of organizational access classes results in a lattice model that meets all of the standard requirements of the Bell and LaPadula model [4]. The primary difference between these new universal access classes and previous strategies is the recognition that each organization may not only have its own set of categories, but may also have its own set of secrecy levels that cannot be easily mapped to the secrecy levels of other organizations. The approach that the US Departments of Defense and Energy have developed for mapping their classification markings does not sufficiently generalize to meet the needs of commercial organizations. However, the new universal access classes can represent the current DoD and DoE systems in a backwards compatible fashion.

References

1. *Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers*, ISO/IEC 7816-5, 1994, International Standards Organization.

2. *Personnel Security Program*, DOE 5631.2C, 15 September 1992, Department of Energy: Washington, DC. URL: http://www.explorer.doe.gov:1776/pdfs/doe/doetext/oldord/5631/o56312c.pdf

3. *SDN.801: MISSI Access Control Concept and Mechanisms,* MCCB-04.02.029, ON636216, Revision C, 12 May 1999, National Security Agency: Ft. Meade, MD. URL: http://www.armadillo.huntsville.al.us/Fortezza_docs/sdn801c.pdf

4. Bell, D.E. and L.J. LaPadula, *Computer Security Model: Unified Exposition and Multics Interpretation,* ESD-TR-75-306, June 1975, The MITRE Corporation, Bedford, MA: HQ Electronic Systems Division, Hanscom AFB, MA.

5. Karger, P.A. *The Lattice Security Model in a Public Computing Network*. in **ACM 78: Proceedings 1978 Annual Conference**. 4-6 December 1978. Washington, DC: Association for Computing Machinery. p. 453-459.

6. Karger, P.A., *Non-Discretionary Access Control for Decentralized Computing Systems,* MIT/LCS/TR-179, May 1977, Laboratory for Computer Science, Massachusetts Institute of Technology: Cambridge, MA. URL: http://ncstrl.mit.edu:80/Dienst/UI/2.0/Describe/ncstrl.mit_lcs%2fMIT%2fLCS%2fTR-179

7. Whitmore, J., A. Bensoussan, P. Green, D. Hunt, A. Kobziar, and J. Stern, *Design for Multics Security Enhancements,* ESD-TR-74-176, December 1973, Honeywell Information Systems, Inc., HQ Electronic Systems Division: Hanscom AFB, MA. URL: http://csrc.nist.gov/publications/history/whit74.pdf