OOPSLA 1993

Addendum to the Proceedings

Washington, DC—26 September–1 October, 1993

Panel Session

Integrating Security Technology and Object-Oriented Technology

Panel Chair:

Bhavani Thuraisingham
The MITRE Corporation

Panelists:

T. C. Ting, University of Connecticut
Peter Sell, Department of Defense
Ravi Sandhu, George Mason University
Thomas Keefe, Pennsylvania State University

1. Introduction

Object-oriented systems are gaining increasing popularity due to their inherent ability to represent conceptual entities as objects, which is similar to the way humans view the world. This power of representation has led to the development of new generation applications such as Multimedia information processing, Artificial Intelligence, CAD/CAM, and Process control systems. In addition to the power of representation, object-oriented approaches are also being used to design software components and to interconnect heterogeneous database systems.

However, the increasing popularity of object-oriented systems should not obscure the need to maintain security of operation. That is, it is important that such systems operate securely in order to overcome any malicious corruption of data as well as to prohibit unauthorized access to and use of classified data. For applications such as C4I, it is also important to provide multilevel security. Consequently, multilevel secure object-oriented systems are needed in order to ensure that users cleared to different security levels access and share a database with data at different security levels in such a way that they obtain only the data classified at or below their level. Recently several research efforts have been reported on incorporating multilevel security into object-oriented systems. In addition, much work has also been done on incorporating discretionary security into object-oriented systems. With discretionary security, users are granted access to the objects based on their identification. Many commercial products enforce some discretionary access control measures.

While progress has been made on applying security to object-oriented systems, object-oriented technology is also being applied to design secure applications. The main focus has been on medical applications and multilevel secure applications.

In order to promote the exchange of ideas on security for object-oriented systems between the security community and object-oriented community, we organized a panel on integrating security technology and object-oriented technology at the OOPSLA'93 Conference. The panel addressed two aspects. First one was on incorporating multilevel security as well as discretionary security into object-oriented systems to produce secure object-oriented systems. The second aspect was on the use of object-oriented design and modeling techniques for designing secure applications. This was the first panel on security to be part of an OOPSLA Conference. The position papers of the panel chair and the panelists were published in the OOPSLA'93 Conference Proceedings. In this paper, we describe the presentations of the panel chair, the panelists, and the discussions that took place at the panel.

2. Presentations

The panel chair Dr. Bhavani Thuraisingham opened the session with a discussion of the developments on integrating security and object-oriented technologies. She discussed the developments incorporating security into object-oriented systems as well as the use of object-oriented technology for designing secure applications. She also stated some of the novel areas that are being explored, such as security for extended relational systems and ACTOR-based systems. The four panelists were subsequently introduced.

The first panelist was Prof. T. C. Ting of the University of Connecticut. T. C. started his presentation with a discussion of MAC (mandatory access control) and DAC (discretionary access control) and the differences between them. He mentioned that while MAC has received much attention, DAC should be an important consideration in designing secure applications. DAC

could actually be much broader and include the need-to-know concept also. DAC should also include statements as to how to use the data and also content and context dependent access to the data. T. C. stressed that security requirements should be considered at the onset of the application design and not as an afterthought. He then went on to explain where object-oriented technology would come into play. He stated that concepts in object-oriented models such as encapsulation could facilitate the design of secure applications. He described a methodology that he and his colleagues have developed at the University of Connecticut called User Role-based System (URBS). The key feature in URBS is to use roles for separation of duty. He stated that the notion of group may not be sufficient and went on to explain how roles would satisfy some DAC requirements.

The second panelist was Mr. Peter Sell of the Department of Defense. Peter described how Rumbaugh et. al.'s OMT could be extended to design multilevel secure database applications. He then discussed the essential points of a methodology called MOMT (multilevel object modeling technique). The analysis phase of MOMT consists of an object model, dynamic model, and a functional model. The object model of MOMT extends the object model of OMT with support for handling different classification levels. The dynamic model captures scenarios and points potential security problems to the designer. The functional model uses data flow diagrams and subsequently generates the methods and the execution levels of the methods. Peter explained the concepts with examples.

The third panelist was Prof. Ravi Sandhu of George Mason University. Ravi started his presentation by stating that security has multidimensional objectives. They are: secrecy, integrity, availability, and control of usage of information assets. Secrecy deals with users only getting the information that they are authorized to know. Integrity deals with protecting the information from unauthorized modification. Availability deals with the information being accessible especially in critical situations. Control of usage of assets is a recent objective and it deals with controls on how the information is used (such as copyright laws for software). These objectives conflict with one another, and when a system is designed, it must be determined as to which objectives are important. Ravi also pointed out that security does not stand by itself. It is coupled with functionality and ease of use. Again one needs to achieve a balance between these feature. In designing a system, first a policy must be specified. Subsequently the mechanism to implement the policy is designed. Finally, assurance will determine how well the design meets the objectives. Ravi then went on to discuss application independent vs application dependent security. With application independent security, one usually uses primitives such as read and write. This way, one could get higher assurance as there are fewer primitives. With application dependent security, the primitives are defined in terms of the application. For a banking application, one could use the primitives debit and credit. With more primitives, achieving higher assurance may be difficult. Since object-oriented applications are rich in semantics, the main issue here is whether one can obtain higher assurance. Although encapsulation might provide better security, if this feature is bypassed, then the system is not secure. Ravi ended his presentation with an important question: "Is the object-oriented approach really better for security?"

The fourth panelist was Prof. Thomas (Tom) Keefe of Pennsylvania State University. He started his presentation with a discussion of some security terms. Then he took a simple object model which is basically a directed graph and discussed some of the security features. There are three concerns. One is the object ID. What does one mean by classifying the object ID? Does one classify the name itself or the relationship to another object? He then talked about modifiable vs. unmodifiable objects. In the case of a modifiable object, its value can be changed only if its new level dominates the old level. With unmodifiable objects, one would create several copies of the objects which may not be good for large databases. Tom finally addressed the issues of transactions. If transactions are single-level transactions, then they will execute at a single security level. This may limit their use. For example, with such transactions, one cannot debit money from one account and credit money to another account if the two accounts are at different security levels. So, the other choice is to have multilevel transactions. Such transactions are more useful, but may require some trust. With respect to the object model, the question is, what impact will multilevel transactions have on method execution?

3. Discussion

In the discussion that took place following the panel presentations, the panelists answered the questions that were posed. Below we state some of the questions and the answers given by the various panelists.

The first question was the following. "With method invocation, wouldn't it be difficult to obtain high assurance?" Ravi replied that the idea is to minimize the trusted code. This is the case in the case of application programs such as mail systems. Only thing is that we don't usually worry about such programs as we do not consider them to be part of the system, whereas in an object-oriented system, one considers methods to be part of the model. That is, similar problems exist with non object-oriented systems also. T. C. added that encapsulation is the key and that this feature should not be bypassed. Ravi then stated that one could develop a secure object-oriented system with the strict enforcement of Bell and LaPadula policy, but this may not be realistic

Another question was whether it would be between to use static languages like ADA rather than languages like Smalltalk. Ravi replied that with languages like ADA, the question is do you trust your compiler. Trusting a compiler is a big issue. T. C. stated that features like polymorphism needs to be explored further to see if there are potential security problems.

Another question was whether there were client-server systems which enforce security, and whether these system use Kerberos. Ravi replied that there are systems such as DCE, Telnet, and Rlogin which probably use Kerberos. Bhavani stated that most object-oriented database management systems are based on client-server architectures and enforce discretionary security.

A member of the audience remarked that some critical systems are developed using a subset of ADA.

Similarly secure object-oriented systems could be developed using a subset of C++. He also commented on T. C.'s presentation on the distinction between groups and roles. He felt that role is a policy and group is an implementation of the policy. T. C. described some of the key points in the URBS model and also stated that with the class hierarchy one could get the group concept, but groups alone were not sufficient for the separation of duty.

Another related question was whether the role/group relationship is similar to the class/subclass relationship. T. C. replied that this could be the case. For example there could be a group, of medical staff with individual roles such as nurse, doctor, etc.

Another question was to discuss the security impact on inheritance. Tom explained some of the different cases. For example, if one assumes that the class hierarchy is strictly monotonically nondecreasing, then all of the methods of the superclass may be inherited. But if this is not the case, then there might some problems. Bhavani stated that at the OOPSLA'93 Conference Workshop on Security for Object-Oriented Systems, there was a discussion as to whether such a restriction should be imposed on the class hierarchy. She then quoted a paper that was presented. Ravi mentioned that in the paper quoted it was stated that additional trust may be needed if one is to avoid such a restriction.

There was a question specifically for Peter. It was stated that some of the restrictions placed on the MOMT methodology was not necessary. Peter replied that MOMT has a lot more than what was presented, but also added that some issues do need more investigation. T.C. mentioned that the problems mentioned were not specific to MOMT, but will be present for any methodology for secure applications and gave an example.

The last question was on the use of encryption and whether it might alleviate some of the trusted code. The panelists all felt that encryption was needed and that one should pay more attention to encryption. However, encryption alone was not sufficient.

Finally the panelists stressed how important it is that security should be considered at the onset and not as an afterthought. With respect to the object-oriented approach, one needs to take a step back and examine whether it is really better for security.