ECOOP Workshop on Distributed Object Security

Christian D. Jensen¹, George Coulouris², and Daniel Hagimont³

¹ Université Joseph Fourier (Grenoble I) Christian.Jensen@imag.fr
² Queen Mary & Westfield College George.Coulouris@dcs.qmw.ac.uk
³ INRIA Rhône-Alpes Daniel.Hagimont@inrialpes.fr

1 Introduction

The purpose of this workshop was to provide a forum for discussion of security problems relating to distributed object-oriented programming environments. As object-oriented technology is becoming more widely deployed, security has become a pressing issue. Object-Oriented programming languages and object-based systems generally offer a convenient set of abstractions for security, such as strong typing, well-defined interfaces and encapsulation of data. However, they also introduce a number of new problems, such as deciding on the granularity of protection in fine-grained object systems and the possible ambiguities arising from polymorphism and dynamic binding, e.g., can a compromised class be substituted for a valid one.

Distribution of objects on a network accentuates the existing problems and introduces a whole range of new security issues that have to be resolved, notably problems arising from mobility of instances or classes. Resolution of these problems is especially important if the objects are to be made accessible on the Internet or through the World Wide Web.

Reusability is one of the traditional virtues of object-oriented systems. However, security problems may arise when objects are reused in an execution context that is different from the context of the original implementation, e.g., the authentication and authorization required by an object modeling a bank account is very different, depending on whether its methods are being invoked from within the banks database or by a home-banking client on the Internet.

This workshop was held on the 20th of July 1998 prior to the ECOOP conference in Brussels. It was organized in collaboration with the 4th Workshop on Mobile Object Systems (this year focusing on security of mobile computations on the Internet). There were a close collaboration between the two organizing committees and joint proceedings were published and made available to the workshop participants.

All papers presented at the workshop can be found in the electronic form at the workshop web site:

http://sirac.inrialpes.fr/~jensen/owdos-program.html

S. Demeyer and J. Bosch (Eds.): ECOOP'98 Workshop Reader, LNCS 1543, pp. 273-276
© Springer-Verlag Berlin Heidelberg 1998
The rest of this chapter is organised as follows. Section 2 gives an overview of each of the sessions held at the workshop. Section 3 gives some final remarks from the workshop organisers. These two sections are directly followed by one page abstracts of each of the papers presented at the workshop. The abstracts are organised in the order they where presented in the workshop.

2 Workshop Sessions

The workshop was divided into four main sessions: “Capabilities and Object Views”, “Reflection”, “Trust Management” and “Secure Storage and Key-Management”.

Each session started with presentations of the accepted papers and a few minutes for questions after each presentation. After all presentations in a session, a general discussion were held, on the problems addressed in the papers.

A short overview of each session is given in the following.

2.1 Capabilities and Object Views

This session focuses on implementation and specification of access control policies in distributed object-oriented systems. Common to all presentations in this session, was the notion of an object view. A view is a restriction of the number of allowed operations on an object by anybody who has that view on the object.

The following papers were presented in this session. “Merging Capabilities with the Object Model of an Object-Oriented Abstract Machine” by María Ángeles Díaz Fondón, Darío Álvarez Gutiérrez, Armando García-Mendoza Sáchez, Fernando Álvarez García, Lourdes Tajes Martínez and Juan Manuel Cueva Lovelle (University of Oviedo, Spain) describes a capability based access control mechanism implemented by integration of object views into object references. The second paper, “Mutual Suspicion in a Generic Object-Support System” by Christian Jensen (Université Joseph Fourier, Grenoble, France) and Daniel Hagimont (INRIA Rhône-Alpes, Grenoble, France) describes dynamic matching of object views by mutually suspicious clients and servers. The third paper, “Towards an Access Control Policy Specification Language for CORBA” by Gerald Brose (Freie Universität, Berlin, Germany) addresses the problem of specifying access control policy in a CORBA environment. The last paper, “Security for Network Places” by Tim Kindberg (Queen Mary & Westfield College, London, England) describes the implementation of an intuitive access control model, that allows secure storage and interchange of documents by naïve computer users.

2.2 Reflection

This session includes two papers which propose the use of reflection features in order to manage access control in an object based system. Reflection is a means to overload system mechanisms such as method invocation or code binding. Therefore, it is possible to overload these mechanisms to assign an access control