

Security for OODBMS (Or Systems)

Ravi Sandhu
George Mason University
Fairfax, VA 22030-4444

A symbiotic integration of security and object-oriented technologies is critical for the maturing, and widespread acceptance, of object-oriented database systems. Security is clearly an essential requirement in large-scale multi-user information systems. At the same time, the real security concerns of an enterprise can be properly addressed only at a semantic level such as offered by object-oriented systems.

Security means different things to different people. It has become generally accepted that there are three major security objectives, as follows.

1. Secrecy is concerned with improper disclosure of information.
2. Integrity is concerned with improper modification of information or processes.
3. Availability is concerned with improper denial of access to information or services from the system.

Recently, it has also become apparent that there is a fourth security objective which is quite distinct from the above.

4. Protection of intellectual property rights is concerned with the improper usage of information assets.

Object-oriented systems offer substantial advantages in all four aspects of security. The most obvious benefit is in the area of integrity. Objects offer a protected interface, consisting of the methods applicable to the particular class of which the object is an instance. In the more sophisticated models it is possible to ensure that sequences of operations on an object must satisfy application-dependent semantic properties.

In the secrecy arena, object-oriented systems suggest a paradigm of controlling information flow by regulating the flow of messages between objects. Research in this area indicates that it is essential to distinguish between method invocations which can change the state of an object, and those that cannot. It also becomes necessary to introduce asynchronism in computations which are otherwise logically sequential.

The availability and intellectual property areas have not received much study in the object-oriented (or for that matter, any other) context. The initial work that has been done does indicate similar benefits in these two areas as have been demonstrated in the integrity and confidentiality arenas.

A truly semantic data model cannot omit the increasingly important security requirements of enterprise-wide information systems. At the same time, security services must be made available at the semantic level where individual users see them as a benefit to their job functions rather than as an hindrance. A symbiosis between security and object-oriented technologies therefore is an appealing prospect.

BIOGRAPHY

Ravi Sandhu is Associate Chairman of the Information and Software Systems Engineering Department at George Mason University. He earlier served on the Computer and Information Science faculty at the Ohio State University in Columbus. He holds the PhD degree from Rutgers University, and the BTech and MTech degrees from IIT Bombay and Delhi. His principal research and teaching interests are in Information Systems Security particularly in Database Management Systems, Distributed Systems and Computer Security Models. He has published over 60 technical papers on computer security in refereed journals, conference proceedings and books. He is currently Program Co-Chairman of the First ACM Conference on Computer and Communications Security (1993), General Chairman of the Seventh IEEE Computer Security Foundations Workshop (1994), and an editor of the Journal of Computer Security.