

Summary of the working conference

*D. L. Spooner, Chair, IFIP WG 11.3
Rensselaer Polytechnic Institute
Computer Science Department
Troy, New York 12180, U S A
spoonerd@cs.rpi.edu*

IFIP WG 11.3 held its tenth working conference on database security at Villa Olmo, in Como, Italy, on July 22-24, 1996. The conference included the presentation of fourteen refereed papers, two invited talks, two panel sessions, and a group exercise session. This conference restored a long standing tradition of holding the working conference on a waterfront, in this case, Lake Como. By all accounts, the conference was a success.

The conference began with two invited talks. Teresa Lunt (ARPA) discussed "Strategic Directions in Computer Security Research," making the point that there is a growing demand for secure systems, but current secure technologies are often fragile. She identified many areas where additional research is needed, including affordability, generic solutions, richer policies, scalability, and metrics for demonstrating progress. Bhavani Thuraisingham (MITRE) discussed "Date Warehousing, Data Mining, and Security," suggesting that there is much commercial interest in data warehousing and data mining and that the security field needs to look carefully at the implications of these technologies on privacy and security of data.

The next session was on federated systems and included the presentation of three papers. The first paper was presented by Zahir Tari (Royal Melbourne Institute of Technology) and was titled "Security Enforcement in the DOK Federated Database System" (co-author, George Fernandez). Tari discussed a unified security model and an architecture for distributed heterogeneous database systems that integrates many existing security models. The second paper was presented by Martin Olivier (Rand Afrikaans University) and was titled "Integrity Constraints in Federated Databases." Olivier discussed a technique that allows a database system to obtain a certified guarantee of data integrity for the data it receives from another system in a federation. The final paper in the session was presented by Silvana Castano (University of Milan) and was titled "An Approach to Deriving Global Authorizations in Federated Database Systems." Castano discussed issues in computing global authorizations from local authorizations in a federated system.

The next session was a panel discussion chaired by Sushil Jajodia on "Multilevel Secure Transaction Processing: Is It Well Understood?" The panelists were Vijay Atluri (Rutgers University), Thomas Keefe (Penn State University), Catherine McCollum (MITRE), and Ravi Mukkamala (Old Dominion University). In general, the panelist shared the opinion that much work has been done on the problem and that solutions are known with certain limitations. They differed in their views of the importance of future work in this area, since existing commercial systems do not yet incorporate much of the work. Several panelists called for the need to better understand the needs of the customer.

The second day of the conference began with a session on object-oriented security. The first paper in this session was presented by John Hale (University of Tulsa) and was titled "A Framework for High Assurance Security of Distributed Objects" (co-authors Jody Threet and Sujcet Sheno). Hale discussed the use of a process calculus tailored for concurrent objects to develop a formal model and layered architecture for secure interoperation of heterogeneous distributed objects. The second paper in this session was presented by Reind van de Riet (Free University) and was titled "An Object-Oriented Database Architecture for Providing High-Level Security in Cyberspace" (co-author Ehud Gudes). He discussed the concept of alter-egos as a representation for people in cyberspace. He also discussed an implementation based on Mokum, an object-oriented knowledge-base system, and on CORBA. The final paper in this session was presented by Frederic Cuppens (ONERA-CERT) and was titled "A Logical Approach to Model a Multilevel Object Oriented Database" (co-author Alban Gabillon). Cuppens discussed a formalization and extension of the Multiview model using a language based on first-order logic.

The next session was a group exercise lead by Pierangela Samarati (University of Milan) and Ravi Sandhu (George Mason University) on "Open Questions in Database Security." It began with a presentation by John Campbell (Department of Defense, U.S.A.) on "Secure Database System Issues." Campbell identified a number of issues requiring additional research, including secure distributed systems, multimedia systems, parallel systems, and heterogeneous systems. This was followed by a general discussion with the goal of identifying important research areas in database security. Some of the issues discussed included: (1) development of a reference model (possibly component based) and metrics to better define what a secure database system is, (2) how to deal with the fact that we must accept a non-ideal world with untrusted components mixed with trusted components, (3) how much can be done in an application-independent way and what depends on the semantics of a particular application system, and (4) recognition of the fact that the database is often just one component of a larger system, and we must consider the security of the larger system, not just the database by itself.

This session was followed by an afternoon of sightseeing in the Como area and a social dinner in a small local restaurant. The food, wine and conversation were all excellent.

The final day of the conference began with a session on multilevel databases. The first paper in this session was presented by Sushil Jajodia (George Mason University) and was titled "A Secure Locking Protocol for Multilevel Database Management Systems" (co-authors Luigi Mancini and Indrajit Ray). Jajodia discussed a secure locking protocol that produces serializable histories of transactions for single version data. The protocol requires only a trusted lock manager. The next paper was presented by Gary Grossman (ARCA Systems) and was titled "A Data Model for a Multilevel Replicated X.500 Server" (co-author Marvin Schaefer). Grossman discussed the incorporation of multiple sensitivity levels into an X.500 directory service through the use of replication. The final paper of the session was presented by Bhavani Thuraisingham (MITRE) for Janet Aisbett (University of Tasmania) and was titled "An Information Theoretic Analysis of Architectures for Multilevel Secure Databases." This paper discusses a framework for accessing the cost of security in a distributed database architecture from an information theory point of view.

The next session was on new directions in database system security. It began with a presentation by Thomas Hinke (University of Alabama, Huntsville) of a paper titled "A Framework for Inference-Directed Data Mining" (co-authors Harry Delugach and Randall Wolf). Hinke discussed a second-path inference detection approach using association cardinalities. The second paper in this section was presented by Vijay Atluri (Rutgers University) and was titled "An Extended Petri Net Model for Supporting Workflows in a Multilevel Secure Environment" (co-author Wei-Kuang Huang). This paper shows how Petri Nets can be used to detect and prevent task dependencies that violate security in workflow models.

The next session was a panel organized by Ravi Sandhu (George Mason University) on implementation experiences and prospects. The panelists were LouAnna Notargiacomo (Oracle), Dan Thomsen (Secure Computing Corporation) and Jess Worthington (Informix). During initial presentations by the panelists and subsequent discussion, the point was made that

users want more tailorable security policies than are available today in commercial systems. Traditional mandatory access control is not what everyone wants. New technologies such as the world wide web are having an impact on what users want. There appears to be a market for secure database products, but these products must support a wider variety of policies and enforcement mechanisms and they must be easy to use.

The final session of the conference was on role-based security and began with a presentation by Silvia Osborn (University of Western Ontario) titled "On the Interaction Between Role-Based Access Control and Relational Databases" (co-authors Laura Reid and Gregory Wesson). Osborn discussed issues and techniques for mappings between a role graph and the set of privileges in a relational database system. The final paper in this session was presented by T. C. Ting and was titled "Generics and Exception Handling for Supporting User-Role Based Security in Object-Oriented Systems" (co-authors S. A. Demurjian, M. Price, and M.-Y. Hu). This paper extends the authors' previous work to handle extensibility and reuse for role-based security enforcement mechanisms to facilitate the design of software systems.

Special thanks go to the organizing committee for the working conference who put together a well run and interesting conference: Elisa Bertino (General Chair), Pierangela Samarati (Program Co-Chair), Ravi Sandhu (Program Co-Chair), and Silvana Castano (Local Arrangements). The next IFIP WG 11.3 Working Conference will be held in Lake Tahoe, California, on August 11-13, 1997. For information about IFIP WG 11.3 see the world wide web page for the working group at the following address: <http://www.cs.rpi.edu/ifip/>.