Executive Summary

1990: A YEAR OF PROGRESS IN TRUSTED DATABASE SYSTEMS

John R. Campbell
National Computer Security Center
Office of Research and Development
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000
(301) 859-4488

1990 has been a year of progress in trusted database systems. It is the year when research and development has reached new level of maturity. Tougher questions, such as inference, aggregation and concurrency control are being examined, and answered. Theoretical foundations are being established. At the Third RADC Workshop on Multilevel Security, Bhavani Thurasingham of MITRE proved that the general inference problem is unsolvable and then presented a series of approaches that could be used to control inference. Knowing that the general problem is unsolvable enables us to more efficiently apply resources to research the controlling methodology.

At the same Workshop, TY Lin of California State University provided insights into aggregation by looking at aggregation through theoretical constructs. Several researchers, each of whom by their work have developed perspectives into the problem of polyinstantiation, discussed and debated this problem. The researchers who attended this Workshop, and their work, were of high quality.

The activity and productivity in trusted database systems was also seen at the 1990 IEEE Computer Society Symposium in Security and Privacy. Three of the eleven sessions discussed work being done in this area.

1990 is also the year of the trusted multilevel database prototype. At the NCSC, Oracle Corp. delivered a "B-level" prototype in April. This prototype is exploring research questions, methodologies and techniques in building multilevel trusted systems. The papers of Vetter, on TCB-Subsets and Maimone on concurrency controls (Tuscon, winter, 1990) are outputs of this work. Oracle is delivering a second prototype, based on the Gemsos Operating System, in August.

Teradata Corp. is building a trusted "B-level" database machine for the NCSC. This computer, dedicated to database management system processing, can be accessed by several host computers. It has an interesting MIMD architecture, is modular and fault tolerant. Systems can be configured from six to several hundred processors. Discussions on metadata host control were interesting.

Sybase Corp. has produced a "B-level" server. In doing this, much work on trusted subjects and covert channels was done.

In this paper, I have enclosed all trust ratings in quotes. This is done because no systems have been evaluated by the NCSC. No system has been evaluated because the "yardstick" for evaluations has not yet been built. However, it is likely that this yardstick, the first edition of the "Trusted Database Interpretations of the Trusted Computer System Evaluation Criteria", or "TDI", will be published before the Conference. This is the document that will be used to evaluate the security of database systems.

1990 is a year for users too. Users have, and will soon have still more security in off-the-shelf database systems. For example, "C2-level" security will be part of the standard database package from both Oracle and Teradata. Sybase, Trudata and others have packages.

1990 hopefully is also a good year for future plans for research and development in trusted database systems. The NCSC is sponsoring two parallel efforts to develop highly secure database systems. "Secure" here means secrecy, integrity and availability. Secrecy will be at the "B-3" and "A-1" levels. "Integrity" includes system, label and data integrity. "Data integrity" includes entity, referential and other integrity. "Availability" includes fault tolerance and distributed systems. The efforts will last from five to six years. One effort uses host-based architecture; the second uses the database machine.

To date much has been accomplished, much is being done. If this area is properly supported, it is likely that future accomplishments will be equally bright.