# Panel: Database Security: Browsers, Encryption, Certificates and More

Chair: John Campbell, National Security Agency

Panelist:

Tim Ehrsam, Oracle Corporation
Carl Landwehr, Naval Research Laboratory
Tom Parenty, Sybase, Inc.

## I. Problem Statement

This has been an exciting year in the use and development of information systems. A user, using a laptop computer attached to a cellular phone, can access and gather information from databases from around the world. Web browsers and search engines make the task even easier. And the pot of gold is growing: some data warehouses are becoming terabyte in size and mining tools provided by the vendor or third parties enable users to establish correlations between elements which the user never realized existed.

Transactions, including credit card and other financial transactions, can easily be accomplished using web/database technology. Can they be done safely?

The new database systems are not just relational engines. They contain multimedia, text, contextual and temporal capabilities and include object architectures. Do these new systems retain the security of the former relational systems? If not, what is lost?

Can all the user's multifaceted activities take place securely? Do JUST the users who are approved and who have need-to-know obtain this data and write into or append to these databases? Can I perform a secure transaction using a browser, operating systems, network software, routers, clients, servers, encryption technology and database management systems, all of which could be from different vendors? Am I sure that my data has retained its privacy and integrity and is available when I need it? What will a firewall or an applet do for (or to) my data security? And what can't they do?

Strong identification seems to be a requirement for many of these systems. What is strong identification? How do I get it?

Single sign on also seems to be a requirement of many users. What is it? Why do users want it? How can they get it?

Certificates and certificate authorities appear to be an "in' thing. What are they? How are they built, maintained and destroyed?

How do I maintain data integrity, and user nonrepudiation?

How do I gain confidence that an information system is doing exactly what it should be doing, and nothing more? Controlled development environments? Use software engineering in building the system? Formal methods? Testing? If so, how do I test my system? Stress tests? Penetration testing?

What are some new approaches to multiple single-level or multilevel security?

And how do I put all these concepts together into a user-friendly, efficient system?

## A Few Additional Questions:

1. Our information system has to be evaluated for security as a whole, as the attack is likely to be at the weakest point in the system. I recently attended a session on Java security, and the security work seems to be coming along nicely. However, the participants kept pointing to the rest of the system; the applet can not be secure if the operating system on which it is running is not secure. The database system cannot be secure unless the operating system, or network on which it is running is secure. Similarly, the interconnections between browser and database have to be carefully looked at; different modules may be made by different vendors. Are they compatible security-wise?

2. Users still require multilevel solutions. Some data is more important to them than other data. They do not want the world to see all of their data and traditional discretionary security is not sufficient. Are the solutions there?

3. Are we really looking at assurance in our data systems: does the system do exactly what we want it to do, and nothing more? And will this system continue to behave in this manner in the future?

4. The requirements being placed on identification, authentication, and access control will become very much more demanding. An example of this was recently described in a government systems trade paper where the complexity of controls on a health care system was noted, because so many people had to see data from the database, but their needs were very different as to what they should see, and as to whether and what they could write into the database. The problems and complexities with the health model were noted, several years previously, by database workshops, sponsored both by the International Federation of Information Processing and by Rome Laboratories.

A second example is the data warehouse, where very large amounts of different data increase aggregation and inference problems and large numbers of people and different communities increase the I&A and access control problems.

Also, more data will be obtained from federated systems, systems where the data is owned or controlled by more than one entity. Each entity may want to protect its own data and may want to impose its own conditions as to whom the data may be released or updated. These conditions may conflict with each other. Thus again the demands on I&A and access control will be greater and researchers have been looking at this problem.

Finally, different parts of these systems may be enforcing different, and possibly conflicting, security policies. The same group may want to enforce different policies under different conditions, for example, wartime versus peacetime conditions, or before and after the announcement of a major product. Will we be able to satisfy these demands?

## II. Some Answers:

1. Some companies are working on strong I&A. For example, Hughes has developed a solution employing Fortezza (TM), using standard interfaces, for client/server database systems.

2. Some database vendors realize that these problems and are trying to assist their users in solving these security problems. For example, Oracle has issued an "Advanced Network Options" package which contains encryption, identification and authentication, and hashing tools for the user and a Security Server for certificates. Sybase has worked on transaction servers and Guardian.

3. Finally some researchers are exploring and developing alternative architectures to provide safe and effective information systems.

This panel consists of leading experts in this field. They will share their insights with you. They will discuss what they see as the most pressing database security problems and will present solutions to some of these problems. They will leave you with a better understanding of the state of security in today's database information systems.

Tom Parenty, Director, Data & Communication Security, Sybase, Inc. has been active in the cryptography and computer security field for over a decade, starting with his tenure at the National Security Agency (NSA) in the eighties. While at the NSA, he worked on the security of global nuclear command and control networks as well as advised the Director of the NSA on internal NSA computer security issues.

In addition to directing all security development activities at Sybase, Mr. Parently is active in the encryption public policy arena and has testified in Congress on this issue. He holds a Bachelor's degree in Philosophy and a Master's degree in Computer Science. Mr. Parenty also founded and ran the largest Chinese martial arts school in the San Francisco east bay area.

Abstract: Tim Ehrsam

Database management systems have traditionally been used to store, manage and secure critical information. Today, the amount of digital information as well as the number of users accessing that information is rapidly expanding.

Databases are now replacing the file system as the repository for data and information because they can store pedabytes of information of any kind (e.g., text, spatial, video) in a more manageable, secure, and cost effective manner than file systems. This is the concept behind Network Computing, an industry-standard architecture where information is stored and managed on the network, while information consumers access that information via simple, low-cost network computers.

As the global economy moves toward Network Computing, industry and government require encryption technologies that protect sensitive information as it travels through the networked society. Additionally, the identity of consumers must be positively established in order to facilitate electronic commerce. Although there are a growing number of products that support strong authentication (e.g., biometric, token, Kerberos, FORTEZZA), the challenge for Network Computing is to integrate the growing number of encryption and authentication technologies into a multi-tier architecture (e.g., client, web application server, data server) to support single sign-on. The discussion will focus on the issues and challenges of integrating and supporting a variety of security technologies in a multi-tier, Network Computing architecture.

Tim Ehrsam
Senior Manager, Security Products
Oracle Corporation

Mr. Ehrsam has over fourteen years of experience in the design, development, and marketing of trusted operating systems, database management systems, and networking

technologies. His experience in trusted systems development includes operating systems and database engineering at U.S. TCSEC evaluation classes C2 through A1, and European ITSEC E3. He has authored numerous papers and articles published in worldwide conference and trade publications. At Oracle Corporation since 1990, Mr. Ehrsam is Senior Manager for Security Products in Oracle's Worldwide Government, Healthcare, and Higher Education Division.

Mr. Ehrsam earned a Bachelor of Arts in economics from Dartmouth College, a Bachelor of Science in computer science from West Chester University, and a Master of Science in computer science from the George Washington University.