# 10

# Open Issues in Database Security

*Ravi Sandhu (George Mason University) and John Campbell (U.S. Department of Defense)*

## 1 INTRODUCTION

*Ravi Sandhu*
George Mason University
sandhu@isse.gmu.edu
www.isse.gmu.edu/faculty/sandhu

The purpose of this group exercise was to have a brainstorming style discussion on what are the important and interesting open questions in database security. The objective was not so much to develop an exhaustive list of these questions, but rather to identify those aspects of database security that are likely to become important, interesting and hot over the next five years. The exercise began with a brief presentation from John Campbell. A position statement related to this talk is given in the next section. This was followed by open discussion moderated by Ravi Sandhu for which John Campbell prepared notes. This discussion is summarized by both of us in the subsequent section.

## 2 SECURE DATABASE SYSTEM ISSUES

*John Campbell*
U.S. Department of Defense
jrcampb@missi.ncsc.mil

### Overview

What has happened to the security of database systems in the last five years? Are they secure? Can we safely access them through the Internet? What improvements have been made? What still needs to be done?

Secure database systems have gradually been evolving to meet user needs. One vendor is offering password, query and data encryption, and digital signing and will be working on strong

P. Samarati et al. (eds.), *Database Security*

identification and authentication for distributed systems. A second is offering tools to handle aggregation. Three are increasing the assurance of trust in their systems. Two vendors have commercial products on the NCSC evaluated products list, a third vendor's product is being evaluated and resulting C2 and BI products are available for users. One vendor evaluated his product under the ITSEC for NT. However, much more needs to be done. Work is being done on secure concurrency control and multilevel transactions. High assurance, distributed and object-oriented systems need research and development. Work on aggregation, inference and downgrading needs to continue. Better legal protection for both software and data is also badly needed.

## Issues

There are many interesting and important issues, as follows.

1. *Distributed Database Systems.* Currently some users send password, queries and data, possibly thousands of miles, in the clear. The consequences of doing this on the Internet could be disastrous. What solutions exist? What problems remain? Also, how do you manage a distributed database system? What tools exist?
2. *Multimedia.* Information users are no longer content with text data. They want to use pictures, graphs, film clip and other multimedia. Can this be safely done?
3. *Parallel and Massively Parallel Systems.* Database systems are becoming larger, thus requiring more processing capabilities. Massive backups are needed. Data integrity is more important and more difficult than ever. Data Warehousing is becoming an important management decision tool. Can all this be done safely?
4. *Differing Database Architectures.* Object Oriented Systems are a promising new architecture. How do you secure them? Object vendors are tying into relational systems and relational vendors are tying into legacy and object-oriented architectures. Hybrids are being built. Can these be secured? Can differing architectures, with possibly differing security policies, safely communicate with each other?
5. *Differing vendors.* Similarly, different vendors are tying into each others products and into the file systems and packages. How do you do this safely? What can be done safely?
6. *Assurance.* How do know that your system is doing what it should be doing, and nothing more? What efforts are being made to increase the assurance of database systems?
7. *Inference and Aggregation.* These are two information problems that have to be dealt with in database applications. What is being done in these areas?
8. *Multilevel Transactions.* Users sometimes need to process multilevel data in one transaction. Are multilevel transaction capabilities a good idea? How are they implemented?
9. *Electronic Commerce.* What is being done to promote electronic commerce and to make electronic commerce safe?
10. *Secrecy versus Data Integrity.* Sometime these two concepts conflict in multilevel systems. How do you maintain referential integrity? What solutions exist? What solutions are needed?
11. *Upgrade/Downgrade.* Multilevel users need to upgrade and/or downgrade data. What capabilities exist? What is needed?
12. *Polyinstantiation.* How does your system handle polyinstantiation? What is the best solution?
13. *Concurrency Algorithms.* What concurrency algorithm(s) do you use? How do they work? Which are the best?

14. *Unrated Operating Systems.* Companies, bothered by the lack of availability of trusted operating systems are putting trusted database systems on unrated operating systems. Is this safe? How do you minimize risk?
15. *Identification and Authentication.* What is the status of current I&A solutions: Kerberos, Sesame, Fortezza?
16. *The Web.* How do you secure the web, and the web server to database server connections?
17. *Firewalls.* Of what use are firewalls? What problems do they present to distributed databases?
18. *Standards.* What standards are needed? Application programming interfaces? Secure sockets? Language standards?
19. *Research and Development Agenda.* Which of the above are the important questions? Which can/have been solved? How should our research and development be structured?

The scope of "Database Management System" has grown in the eyes of the user to include everything from the client to the servers and everything between. Vendors, seeing new opportunities and revenues, are promoting this vision. They are purchasing or adding third parties to add expanded functionality and added security. My feeling is that database security must also grow to meet user concerns. A question that will become more and more important, as systems become more complex, is whether the system is secure. If I add a series of security components, do I have a secure system? Of what quality are these components? What are they protecting against? What is the security policy? What happens if I change the policy?

We must work more with our security neighbors and use the results of their work in our assessments. How strong is an algorithm? How strong is a protocol? Are they being used in an appropriate situation? Of what use is intrusion detection? I see database research in the future being broader, with more collaboration, and, frankly, more fun.

# 3 DISCUSSION SUMMARY

*Ravi Sandhu*
George Mason University
sandhu@isse.gmu.edu
www.isse.gmu.edu/faculty/sandhu

*John Campbell*
U.S. Department of Defense
jrcampb@missi.ncsc.mil

As stated earlier the objective of this exercise was to identify those aspects of database security that are likely to become important, interesting and hot over the next five years. John Campbell began the exercise by presenting examples of some of the open questions, listed above. This was followed by open discussion moderated by Ravi Sandhu. This summary is largely based on notes taken by John Campbell.

As it turned out the session was well placed in the schedule. Coincidentally, on the previous evening there was a discussion during the group's business meeting concerning a possible change

in name from Database Security to indicate the broader scope of this group's interest. Alternate names such as Data Security, Information Security, and Secure Information Management were suggested. There was a general consensus that Database Security may be too narrow a term for our interests as we transition into a new millennium. Throughout the Workshop, the group, as a whole, repeatedly made reference to rapid changes in systems development, architecture and security that are changing existing doctrine. All of this provided an appropriate context for our group exercise.

During his talk leading into the discussion John Campbell presented an example of a proposed system which involved web browsers and servers, networks, and distributed multimedia, multilevel database systems. Such a system would not even be conceived of five years ago. This set the stage for the open discussion.

It was generally agreed that it is becoming increasingly difficult to between the network and the operating system. What is the role of a DBMS in this context? A DBMS can play a minimal role relegated to being a relational client/server system. On the other hand vendors and researchers are pushing DBMS's to be much more than that.

At some point it make sense to ask: "is the network the DBMS", in direct analogy to the question: "is the network the operating system", that has been asked several years ago. How do we demarcate the DBMS from the network or operating system? In future architectures/systems, does it make sense to have this demarcation?

During the ensuing discussion the following major themes emerged.

1. One suggestion was to adopt a three-layer reference model consisting of infrastructures, services and applications. Within this framework it may be possible to distinguish the concerns of database security (or whatever new term we might use) from concerns of, say, network security, operating systems and application security.
2. Another suggestion was to concentrate on component-based secure database management. There would be one or more components for data integrity, secrecy, etc. These components could have differing assurance strengths and enforce differing policies. A user could select different modules according to his needs. Another participant added that we have to accept a non-ideal world of untrusted components and add trusted components as we can.
3. Yet another suggestion was to build a reference model to clarify what is a secure database, or, perhaps, what is a secure information system.
4. Some felt that they did not want to broaden the research areas of database systems, to include such things as middleware or to go below layer 7 of the ISO model. Others, however, felt that the scope should be broadened to include "data management as people are experiencing it today", that ISO layers are artificial barriers and that it is artificial to stop at a layer. In fact, we may want to define new protocols in the future. We have a dynamic situation, and must adapt to the changing situations. With either view, assumptions must be identified. If some requirement is being taken care of by a lower layer, than say it.

Some of the other issues that came up during the discussion are given below.

- We should adapt end-to-end security. But is a DBMS one component or a series of components?
- We need to know how much can be done in an application-independent manner and how much is application-dependent.
- We should be looking at how messages are stored, how users are authorized and how roles are defined.

- We need to look at new areas such as collaborative data mining, data agents and data warehousing.
- We need to determine where security belongs. Is it a separate component? Is it different agents at different layers looking for different things? Does it vary from architecture to architecture?
- Another suggestion is to look at things that are likely to be implementable by vendors. If there is no market for an item, or if the benefit is too small when compared to the cost of implementation, the vendor will not implement, and the research will not be used. On the other hand, it was pointed out that sometimes research findings are used for the first time years after the research was done. For example, relational technology took a long time to make it products but eventually the products were spectacularly successful.
- A weak link, and something that we have not been looking at, is identification and authentication (I&A). Both the technologies of I&A and the user demands for I&A should be studied.
- Another weak link is metrics: How secure is "secure"?
- We also need to know what the rest of the community is doing, for example, in directories, and specifically X.500.

The group exercise was successful in generating discussion which carried into the lunch hour and later. The group is likely to face these issues again in future meetings.