A Database Security Course on a Shoestring

Binto George
Computer Science Department
Western Illinois University
1 University Circle
Macomb, IL 61455
B-George@wiu.edu

Anna Valeva
Department of Mathematics
Western Illinois University
1 University Circle
Macomb, IL 61455
AK-Valeva@wiu.edu

ABSTRACT

Database security has paramount importance in industrial, civilian and government domains. Despite its importance, our search reveals that only a small number of database security courses are being offered. In this paper, we share our experience in developing and offering an undergraduate elective course on database security with limited resources. We believe that database security should be considered in its entirety rather than being component specific. Therefore, we emphasize that students develop and implement a database security plan for a typical real world application. In addition to the key theoretical concepts, students obtain hands-on experience with two popular database systems. We encourage students to learn independently making use of the documentation and technical resources freely available on the Internet. This way, our hope is that they will be able to adapt to emerging systems and application scenarios.

Categories and Subject Descriptors

H.2.7 [**DATABASE MANAGEMENT**]: Database Administration—*security, integrity, and protection*;
K.3.2 [**COMPUTERS AND EDUCATION**]: Computer and Information Science Education—*curriculum.*

General Terms

Security.

Keywords

Undergraduate Database Security Course, Database Security, Laboratory/Active Learning, Statistical Security.

1. INTRODUCTION

Database systems are designed to provide efficient access to large volumes of data. However, many application domains require that the data access be restricted for security reasons. For example, an unauthorized access to a bank database can potentially cost millions of dollars. The federal Health Insurance Portability and Accountability Act (HIPAA) regulates the disclosure of information from a patient database, allowing access to health care providers, health plans, and health care clearinghouses, simultaneously protecting the privacy of patients. For obvious reasons, a Department of Defense (DoD) database needs to be protected from unauthorized access. Since many organizations increasingly entrust their information resources with database systems, in today's highly networked environment, the sensitive information can be at high risk unless there are security mechanisms in place to protect the data at the source itself. However, a large number of databases are incorrectly installed, configured, and maintained. This, in part, may be attributed to the lack of database security education in our computer science programs. We feel that a new undergraduate course on database security will help our students face the ever increasing challenges in this field.

Our search shows that, despite the importance, only a handful database security courses are being offered. Most of the courses we found are graduate courses and are highly theoretical. We also found a few extension program courses, which are product specific. Although a large number of database courses exist at both undergraduate and graduate levels, we feel that, one reason for not offering database security courses may be the scarcity of textbooks, reference materials, and other resources.

Realizing the importance of database security in computer science curriculum, [8] proposes adding a new module to the basic database course. Since the basic database course has already many topics to cover, we feel that the addition of new material will not completely serve the purpose. Further, we find it difficult to incorporate hands-on component to such a course. Similarly, a computer security course is too broad in scope, and rarely includes database security topics. Therefore, we decided to develop a new undergraduate level elective on database security. This paper is based on our experience of offering a database security course in Spring 2005. We have adjusted the contents and assignments in response to the feedback and course outcome. The modified version is presented here.

Since many of our students seek industrial positions after graduation, we have designed our course to meet their needs with the right blend of theory and practice. The course objective is to develop an understanding of security aspects of databases, database administration, and database supported applications. We collected information from alumni as well as potential employers before finalizing the contents.

SIGCSE'06, March 1–5, 2006, Houston, Texas, USA.
Copyright 2006 ACM 1-59593-259-3/06/0003...$5.00.

Although students were expected to gain hands-on experience with some popular databases in our course, we tried to focus on concepts rather than just syntax or product specific features. Often, students were asked to learn software packages on their own by reading the product documentation. We also offered an online feedback page for receiving anonymous student comments, which helped us know if students needed additional assistance. By encouraging students to learn and experiment on their own, we hope that they can easily apply the learned concepts to emerging application scenarios. This is particularly needed since today's work environment expects agility from employees to quickly master and develop software systems. To facilitate participation further, we asked students to research and make presentations choosing from a set of specified topics. Most importantly, since many of our educational institutions are cash strapped, we designed our course to execute with a small budget.

In the next section, we detail topics, which may be included in a database security course, with references that, we hope, will be useful for other instructors. We also discuss labs and assignments in detail. Finally, we conclude the paper with an account of lessons learned and future possibilities.

2. DATABASE SECURITY TOPICS

Although a large number of topics can be included, we try to focus on a few important ones that, in our judgment, are likely to be immediately useful after graduation. We also include topics on securing the data within a database, as well as the security of database systems and operating systems as suggested in [8]. Our position is that database security should be considered in whole rather than adopting a piecemeal approach. However, we recognize that, in practice, it is often easy to overlook some aspects of database security. Therefore, we recommend that students develop a database security plan. We also include other relevant topics such as statistical database security, and security and privacy issues of data mining. Table 1 shows the schedule of topics for a typical sixteen week semester course on database security. Major labs and assignments are given in Table 2.

The course begins with an "Introduction to database security", where the objective is to highlight the importance of database security and to motivate students to learn the rest of the topics.

2.1 Introducing Database Security

One way to emphasize the importance of database security would be to reflect on the impact of not having security at all in application domains such as military, medical, financial, credit card, credit file, driving records, and insurance databases. Students may survey the incidents of database security breaches and evaluate the efforts to ensure database security by industry and government.

Since database security is a combination of database technology and computer security, basics of both will be helpful. A discussion on security properties such as confidentiality, integrity, availability and non-repudiation should be included.

Although an in-depth study of cryptography is not within the scope of this course, basics of secret key cryptography and public key cryptography will benefit students. A good reference book we found is "Data Security and Cryptography" by Dorothy Denning [5]. Digital signatures, digital certificates and Public Key Infrastructure (PKI) [21] are other topics to consider.

Week	Topic
1	Course Overview and Introduction to Database Security, Basics of Data Security and Cryptography
2	Overview of Security Models
3	Access Control Models, Covert Channels and Inference Channels
4	MySQL Security
5	Oracle Security
6	Oracle Label Security
7	Developing a Database Security Plan
8	Spring Break
9	SQL Server Security
10	Security of Statistical Databases
11	Security and privacy issues of Data Mining
12	Database Applications Security, SQL Injection, Defensive Programming
13	Database Intrusion Prevention, Audit, Fault Tolerance and Recovery
14	Hippocratic Databases, XML Security
15	Network Security, Biometrics
16	Final Examination Week

Table 1: Course Schedule

An overview of security and integrity models [4] will also be helpful at this point. This is the best time to introduce the computer security lingo such as *subjects* and *objects*. The difference between widely used access control techniques may also be highlighted.

2.2 Access Control

Discretionary Access Control (DAC) mechanisms such as capabilities, profiles, access control lists, passwords, and permission bits may be discussed. Here we also introduce the operating system security aspects (using Windows® and Linux environments), and how they impact database security in general. Although details are not required until we introduce Oracle security, overview of Role-Based Access Control (RBAC) [6, 18] may be discussed.

Unlike the above access control techniques, in Mandatory Access Control (MAC) the security is enforced by the system as dictated in the security policy, not by the owner of an object. Although there are many security models suggested for providing Mandatory security, Bell-LaPadula [2] model is probably the simplest to learn. Even when a system enforces Mandatory Access Control, information leakage through covert channels [11] and inference channels [13] may still be possible. A few examples will help students understand how the information leakage can take place through such means.

Databases enforcing MAC often assign security classification levels for objects and security clearance levels for subjects. Access control is performed by the system based on these levels. A lab may be developed, where students simulate a multilevel database on an ordinary database system. This means students will have to modify the schema to add additional fields for storing security classification levels. They also develop views for users having different clearance levels. Further, to support poly-instantiation, the primary key will have to be redefined to include security level to accommodate the possibility of the same key values existing at multiple security levels.

Another topic of interest would be to explore how the Discretionary Access Control and the Mandatory Access Control can be combined and applied in some scenarios.

2.3 Securing Real Life Databases

The candidate database systems we chose for hands-on experience were MySQL™, Oracle®, and Microsoft® SQL Server™. Because of time constraints, students were able to focus only on the first two databases, but an overview of SQL server security was also provided.

2.3.1 MySQL Security

With more than six million installations worldwide [14], the simplicity and open source architecture make MySQL, probably, the first database to study. The primary source of information would be the MySQL manual itself (available from MySQL site [14]), particularly the section on "MySQL Access Privilege System". Another source, MySQL Security Handbook [22], explains MySQL security system and provides a few practical examples.

Labs/Assignments
1 Multilevel Security – Poly-instantiation
2 MySQL Grant Privilege System
3 SQL Injection
4 Oracle Security – Basic Lab
5 Database Security Plan Development
6 Backend Development for B2C Application
7 Probability Distributions, Sampling
8 Statistical Databases - Breach of Security
9 Statistical Databases - Inference Protection Techniques
10 Data Mining Security - Reading and Presentation

Table 2: Major Labs/Assignments

MySQL Access Privilege System authenticates a user based on user name, host name, and password. Further, it ensures that users perform only permitted operations based on the privileges specified in the grant tables (namely, `user`, `db`, and `host`). The format and contents of these tables, therefore, are of particular importance. Since most of the critical information including the grant tables are stored on a default database named `mysql`, the security of `mysql` database is also crucial. Students should learn to apply the "principle of least privilege" when granting privileges in order to perform the task at hand.

Each student was given a MySQL instance with `root` level access. Students were asked to create users and assign privileges while monitoring the privilege tables for changes. Students also experimented with the privilege system by manually modifying privilege tables. We created two person administrator-user teams for enabling the students to experience the system from both perspectives. Users were assigned certain tasks to perform. Some of the tasks given were specifically designed to understand the limitations of the MySQL privilege system. The role of the administrators was to grant privileges just sufficient for users to perform the task. Users could access the system in any manner they wish – in fact, users will be encouraged to expose the weaknesses in the privilege assignments. The administrators, on the other hand, controlled access based on need-to-know, at the same time trying not to be too restrictive for users to perform the required tasks. We found the users very excited to expose security weaknesses in the privilege assignment. Although administrators were a little embarrassed, they too were motivated by the exercise. For the the next lab session, students switched roles, i.e., those who were administrators became users and vice versa.

MySQL supports data security by providing functions such as ENCRYPT, DES_ENCRYPT, AES_ENCRYPT, PASSWORD, OLD_PASSWORD and ENCODE. Since these functions may not be safe under all circumstances, it would be useful to highlight the unsafe scenarios.

Students may also learn how to use SSL for security, and simultaneously make sure that the system performance is not significantly impacted. Also useful would be to study how the authentication requirements may vary when using options such as REQUIRE SSL, REQUIRE ISSUER and REQUIRE X509. Even when using SSL, the data security can depend on the type of cipher and the key lengths used. Therefore, students may learn how to specify these parameters using the REQUIRE CIPHER option.

Some privileges in MySQL, if not carefully used, can expose the system to high security risk. For example, FILE privilege may be misused to gain access to the system. Hence, a comprehensive study of unsafe privileges will be extremely useful.

Even when the privilege system is correctly set up and maintained the entire privilege system can be circumvented using a MySQL startup option like `--skip-grant-tables`. On the other hand, some startup options make the server safer. Therefore, MySQL startup options and their security consequences must be discussed.

Many web applications have MySQL database server deployed as the backend, and HTML based form acting as the front end. Since user input is used to generate SQL queries to interact with the database, if unchecked, malicious users or programs can inject unsafe SQL queries. Basic concepts of preventing SQL injection may also be discussed. Students may be asked to analyze a number of SQL queries for potential vulnerability.

Other topics, which can be included are: using MySQL network scanner to detect MySQL servers on the network with default passwords, MySQL resource control, data backup and recovery, auditing, and firewalls.

2.3.2 Planning Database Security

Since enforcing database security is extremely complex task with a large number of factors affecting the security of a database, the best way to approach the problem would be to systematically develop and implement a comprehensive database security plan. Therefore, in our course, we required that students develop a database security plan for a small Business-to-Consumer (B2C) E-Commerce application. See [19] Ch7 (available online) for detailed exposition on database security planning. Although the text is on Oracle security, the concepts can be applied to any database.

2.3.3 Oracle Security

For security reasons, the computer science department was reluctant to grant administrative privileges to students on our Oracle server. Therefore, we ended up creating a separate Oracle instance for the course. For each student, we created one administrative account with DBA privileges, and then the students were allowed to create user accounts as needed, provided they follow a naming convention to avoid conflicting names. In addition to Oracle Security Handbook [12], we found the Oracle Database Administrators Guide [15] also useful. The guide is available online from the Oracle Database Documentation Library.

First, we had an Oracle Security Basics Lab. Students were introduced to the Oracle security system through a series of tasks. The next lab was more advanced, and built up on the database security plan developed in a previous assignment. The task was to develop the backend for a small B2C E-Commerce application. Students were asked to create user accounts, roles, tables, views and triggers as required. The privileges were to be assigned by observing the "principle of least privilege", as per the security plan.

Further, students may also be trained to perform some standard checks for security such as checking for default user accounts, default passwords, users having excessive privileges (e.g., DBA, ALTER SYSTEM, CREATE LIBRARY, CREATE ANY TRIGGER), security impact of WITH ADMIN and WITH GRANT options on privileges, EXTERNALLY authenticated users, and the existence of database links. Students may also learn how to display information on items such as triggers, views and externally authenticated users. A section on security issues of using default Oracle supplied roles will be useful.

Other topics to include are: Transparent Network Substrate (TNS) security and listener management from remote machines and setting up listener passwords, buffer overflow attacks and prevention, auditing, and undocumented Oracle features. Students may also be introduced to reading security advisories and obtaining Oracle Critical Patch Updates (CPU).

Recently, a large number of security breaches have been reported. Interestingly, however, many of these breaches were incidents of missing or stolen backup storage devices. Therefore, we feel appropriate to include a session on security and protection needs of exports, cold backups, hot backups, and disaster recovery sites.

2.3.4 Oracle Label Security

Oracle Label Security provides built-in row level access control for high security applications. Essentially, Oracle adds a new field to each row for storing the row's sensitivity labels. Row access is granted or denied by comparing the user's identity and security clearance label with the row's sensitivity labels. Earlier, in Assignment 1, students have simulated a multilevel database. Therefore, the above concepts should be easy to learn at this point.

As a source of information on Oracle Label Security Architecture, we used Oracle Label Security Administrator's Guide [16]. We covered levels, compartments, groups, session and row labels, label security algorithm, and management of label security using Oracle Internet Dictionary.

2.3.5 Microsoft SQL Server Security

As we mentioned earlier at the beginning of this section, due to time constraints, we could not provide an extensive coverage of Microsoft SQL Server. We briefly discussed SQL Server security model, authentication mechanisms, authentication modes, and good security practices for SQL servers. Students presented information they gathered on SQL server vulnerabilities, security breaches, and prevention techniques. We found a few excellent articles on SQLServerCentral.com, an online community of DBAs, developers, and SQL server users. We also found SQL Server Developer Center (http://msdn.microsoft.com/sql) useful in providing a large number of resources in this area.

2.4 Statistical Security

As for the rest of the course, this section is application oriented, giving the students the gist of the concepts they need to know and then putting them to work in the context of a real database. Thus, the first lab is a simulation based assignment designed as an introduction to probability distributions, expectation, spread, sampling methods, and sampling distributions of relevant statistics. We find that, even for students with prior coursework in probability and statistics, an assignment of this type is very beneficial. The second lab presents the task of setting up a sequence of queries, so that students can extract from a database what should have been secure information. At this point we introduce the main conceptual techniques for inference protection such as the lattice model and partitioning the database entities into populations. See [4], Ch 5 for details. The third major assignment aims at teaching inference protection techniques. Given a database, the students are asked to answer queries without disclosing sensitive information by applying restriction, perturbation, and combined techniques.

2.5 Security Issues of Data Mining

Data mining may be misused to obtain confidential information from a database. So we believe, a course on database security should include an overview of security and privacy concerns of data mining. Organizations would like to share the data for operational convenience, at the same time prevent the mining of data for information they do not want to disclose. Likewise, private individuals would like to submit their personal information for data mining without compromising their privacy while keeping the key association rules intact. Secure data mining techniques appear similar to statistical security methods, however, their computational efficiency is a major concern. We found a number of interesting papers [3, 17, 20] that can be used for reading assignments and group discussions.

2.6 Other Topics

Malicious users may bypass security mechanisms provided by an application by directly connecting to the database. Therefore, whenever possible stored procedures, and views must be used for providing data access. Database application security and defensive programming was briefly covered. Semi-structured nature of Extensible Markup Language (XML) documents make them ideal candidates for use in many applications including E-Business. Therefore, XML [7] security was also discussed.

Other topics of interest are: database intrusion detection and prevention [17], database fault tolerance and recovery, Hippocratic databases [1], network security [10], and biometrics [9].

3. RELATED COURSES

Department of Computer Science at University of Alberta has offered an independent study on database security with topics such as security models, security mechanisms, intrusion detection systems, and statistical database protection. University of Maryland University College has a graduate level course on database security with theory and applications, including frameworks for discretionary and mandatory access control, data integrity, availability and performance, secure database design, data aggregation, data inference, secure concurrency control, and secure transaction processing. University of South Carolina and George Mason University offer graduate level elective courses on Database Security. Similar courses are offered at a few other institutions, but we do not discuss them here due to space constraints. Among the undergraduate courses we found, the closest one to what we offered is taught at University of Arkansas Little Rock. It provides database security theory and background on Oracle security environment.

4. CONCLUSIONS

Our new undergraduate elective course on database security covers basic concepts and provides practical experience on two popular databases. We emphasized that students develop a database security plan that, we hope, will encourage them to view the problem of ensuring database security as a task that needs to be carefully planned in whole rather than something that can be addressed in parts.

The initial offering of the course had “Data Structures” as the only pre-requisite, because we wanted to keep the course open to a larger audience. Students, in general, were found be more motivated to follow through on course work than other courses we have taught. We received excellent numerical score as well as comments from students in the departmental student evaluations. We had a good mixture of students. All were computer science majors, and forty seven percent were honors students. Sixty seven percent of the class completed the course with an overall score of 80% or higher with all honors students falling into this category. However, it was felt that a few students lacked basics to fully grasp the material. Therefore, having a basic database technology course as the pre-requisite will help cover more of the suggested topics in depth.

In closing, we hope that our experience shared herein will help other instructors develop and offer a similar course on database security with limited resources.

5. REFERENCES

[1] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic Databases. In *Proc. of the Very Large Data Bases (VLDB) Conference*, Hong Kong, China, August 2002.

[2] D. Bell and L. LaPadula. Secure Computer Systems: Mathematical Foundations. Technical Report ESD-TR-73-278, MITRE Corporation, 1973.

[3] C. Clifton and D. Marks. Security and Privacy Implications of Data Mining. In *Workshop on Data Mining and Knowledge Discovery*, Montreal, Canada, February 1996.

[4] S. Castano, M. G. Fugini, G. Martella, and P. Samarati. *Database Security.* Addison-Wesley & ACM Press, 1995.

[5] D. E. Denning. *Cryptography and Data Security.* Addison-Wesley, 1982.

[6] D. Ferraiolo and R. Kuhn. Role-Based Access Controls. In *Proc. 15th NIST-NCSC National Computer Security Conference*, Baltimore, MD, October 1992.

[7] B. Dournaee. *XML Security.* RSA Press, Berkeley, CA, USA, 2002.

[8] M. Guimaraes, H. Mattord, and R. Austin. Incorporating Security Components into Database Courses. In *Proc. of the InfoSecCD Conference'04*, Kennesaw, GA, September 2004.

[9] A. Jain, L. Hong, and S. Pankanti. Biometric Identification. *Commun. ACM*, 43(2), 2000.

[10] C. Kaufman, R. Perlman, and M. Speciner. *Network Security: Private Communication in a Public World, Second Edition.* Prentice-Hall, 2002.

[11] B. W. Lampson. A Note on the Confinement Problem. *Commun. ACM*, 16(10), October 1973.

[12] M. Theriault and A. Newman. *Oracle Security Handbook : Implement a Sound Security Plan in Your Oracle Environment.* Osborne McGraw-Hill, 2001.

[13] M. Morgenstern. Security and Inference in Multi-Level Database and Knowledge-Base Systems. In *ACM SIGMOD Conf. on the Management of Data*, San Francisco, CA, May 1987.

[14] http://www.mysql.com.

[15] *Oracle Database Administrator's Guide.* Oracle Corporation, 2001.

[16] *Oracle Label Security Administrator's Guide.* Oracle Corporation, 2003.

[17] R. Agrawal and R. Srikant. Privacy-preserving Data Mining. In *Proc. of the ACM SIGMOD Conference on Management of Data*, Dallas, TX, May 2000.

[18] R. Sandhu and Q. Munawer. How to do Discretionary Access Control Using Roles. In *RBAC '98: Proceedings of the third ACM workshop on Role-based access control*, Fairfax, VA, 1998.

[19] M. Theriault and W. Heney. *Oracle Security.* O'Reilly & Associates, Inc., 1998.

[20] V. Verykios, E. Bertino, I. Fovino, L. Provenza, Y. Saygin and Y. Theodoridis. State-of-the-art in Privacy Preserving Data Mining. *SIGMOD Record*, 33(1), 2004.

[21] W. Ford and M. S. Baum. *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption.* Prentice Hall, 2000.

[22] Wrox Author Team. *MySQL Security Handbook.* Wrox Press, 2003.