Database Security Curriculum in InfoSec Program

S. Srinivasan
Professor of Comp. Info. Systems
University of Louisville
Louisville, KY 40292, USA
1 + 502 – 852 – 4790
srini@louisville.edu

Anup Kumar
Professor of Comp. Engg. Comp. Sci.
University of Louisville
Louisville, KY 40292, USA
1 + 502 – 852 – 0471
ak@louisville.edu

ABSTRACT
Database Security course is an important part of the InfoSec curriculum. In many institutions this is not taught as an independent course. Parts of the contents presented in this paper are usually incorporated in other courses such as Network Security. The importance of database security concepts stems from the fact that a compromise of data at rest could expose an organization to a greater security threat than otherwise. Database vulnerabilities exposed recently in several high profile incidents would be a good reason to dedicate a full course to this important topic. In this paper we present key topics such as technologies for database protection, access control, multilevel security, database vulnerabilities and defenses, privacy and legal issues, impact of policies and some well known secure database models.

Categories and Subject Descriptors
H.2.0 [General] Security, Integrity and protection
D.4.6 [Security and Protection] Access controls, Authentication
K.6.5 [Security and Protection] Physical security

Keywords
Database, multilevel security, encryption, inference, privacy, policy

1. INTRODUCTION
Information Security curriculum is receiving greater attention from many institutions, thanks to the standardization efforts by the Committee on National Security Systems (CNSS). The CNSS members come from the National Security Agency, Department of Defense, and the Department of Homeland Security, among others. The CNSS standardization efforts are based on the Presidential Decision Directive [24] issued in 1998 for training professionals to protect the nation's critical infrastructure. To achieve this goal, CNSS has developed five major standards known as the National Security Telecommunications Information Systems Security Instruction (NSTISSI). The NSTISSI standards are numbered 4011, 4012, 4013, 4014 and 4015 [8]. Additional standards under this sequence are in the offing as well. The relevance of these standards is that they include a vast number of topics that cover the entire gamut of information assurance and database security topics are included in many of these standards. First, we will briefly outline the main content of each of these standards and then move onto the main content of this paper.

Information Security Curriculum Development (InfoSecCD)
Conference '05, September 23-24, 2005, Kennesaw, GA, USA.

The 4011 standard covers the information security foundation topics such as wired and wireless communications basics, operations security, transmission security, information security from a policy perspective, cryptography, key management, legal aspects of security, contingency planning and disaster recovery, risk management, trust, auditing, and monitoring. At present, coverage of topics mentioned in this standard is considered essential by CNSS in every InfoSec curriculum. The 4012 standard is primarily aimed at training Designated Approving Authority personnel. A quick look at the following topics would show the relationship of these standards vis-à-vis database security. The primary topics of this standard include: liabilities, legal issues, security policy, sensitive data access policy, threats, vulnerabilities, incident response, life cycle management, configuration management, and contingency management. The purpose of 4013 standard is to provide a minimum set of topics necessary for certifying Systems Administrators in Information Systems Security. Some of the topics in this category include: development and maintenance of security policies and procedures, education, training and awareness of such policies, development of countermeasures for known attacks as well as development of safeguards. Also, configuration management is an important part of 4013 standard. The standard for training Information Systems Security Officers is 4014. This standard covers topics such as facilities planning, business continuity, and password management, access control policies, laws and regulations related to information security, privacy, encryption standards, intrusion detection, audit tools, and security reviews. The last standard currently in place in this series is numbered 4015. This standard is for training System Certifiers. Among the main topics here are: defining roles and responsibilities for personnel, certification of systems, identifying process

boundaries, integration, security engineering, and applications security. These five standards have been in place since 1994 and are constantly getting updated by CNSS.

2. INFOSEC FOUNDATION COURSES

Traditionally, the following courses are considered as a set of foundation courses: Network Security, Information Security, and Cryptography. Usually these courses are augmented by additional courses such as Operating System Security, Database Security, Secure E-commerce, and Security Management. In our curriculum at the University of Louisville we are offering the three foundation courses listed above and the Database Security course. The main purpose of this paper is to identify several topics that could be included in a Database Security course. In the last quarter of 2004 and the first quarter of 2005, several incidents of theft or loss of data from databases of large organizations have brought to light the vulnerabilities in managing database systems. Every organization depends heavily on databases, both large and small, in order to manage inventory, human resources, and business functions on a day to day basis. Therefore, in order to mitigate risk, every organization must take adequate steps to protect the data that they hold. Issues related to technology as well as policies are important for the protection of data. Such topics form the core of this Database Security course, which we will discuss in greater detail in the remaining sections.

3. INFOSEC AT U. OF LOUISVILLE

At the University of Louisville (U of L), InfoSec courses are offered in two departments. The Computer Information Systems (CIS) department in the College of Business offers an undergraduate concentration in InfoSec [36]. The Computer Science department in the college of Engineering offers graduate courses in InfoSec at the masters and doctoral levels. Database security course is offered as the second course in database, the first course being the standard database design and management course. Students taking the database security course are either juniors or seniors and are expected to have experience with one of the mainframe commercial databases such as Oracle or SQL Server 2000. The major course objectives were for students to:

- Learn the fundamental concepts in database security
- Understand how access controls work in a database
- Learn to develop and manage secure database architectures
- Be familiar with the laws governing computer privacy
- Understand the alternatives to encrypting data at rest
- Understand the security implementations and vulnerabilities in commercial database systems such as Oracle and SQL Server 2000
- Learn security audit methods
- Learn about multi-level database security

The course content was covered using material from many sources, primarily research papers. The Database Security book by Castano, et al is an out of print book as it was originally developed in 1994. The Database Security and Auditing book by Afyouni was printed in April 2005 and so was not available when the semester started. In the course we used two SQL Server Security books which were available in print and one Oracle Security book that was available in electronic form through Safari books. These books contributed to reinforcing concepts discussed by testing several attack methods. Another special feature of teaching the Database Security course was the availability of a dedicated InfoSec Lab. We will discuss the contribution of the InfoSec Lab later in this paper.

The initial emphasis in the course was on incorporating database security concepts during the design phase. The primary reason for this emphasis was on the need for integration of various components of an information system. Since database security is heavily dependent on network security, operating system security, physical security and other applications security such an integrated approach is essential for an appreciation of design decisions. The course content was arranged in such a way that both technology and policy aspects were equally emphasized. This emphasis was motivated by the fact that there are several legal requirements to be met and people's privacy must be protected. A compromised database endangers the privacy of individuals by the release of personal information such as social security number, date of birth, credit card numbers, and health history.

An important part of database security is access control. There are several types of access controls that are available for the database administrator to work with. More importantly, choosing the proper type of access control enables the allocation and revocation of privileges to individuals for various components of the database. The three types of access controls discussed related to Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role-based Access Control (RAC). A simple example of MAC would be that of using a suitable password for database access. However, practical uses of databases always require overriding a default access privilege for a specific event. In such instances one uses Discretionary Access Control. Since database privileges sometimes have the inheritance property it becomes essential to understand how the particular commercial system would handle DAC. The most important of access controls is Role-based Access Control. Discussion of this topic showed the various nuances involved in assigning access privileges in a timely manner without hindering productivity and at the same time providing security. All necessary database accesses could be associated with a specific role that an individual performs in an organization. Since roles change often and consequently access needs change as well, it is much easier to manage access control by associating privileges with roles. It is worth noting that these three types of access controls are not mutually exclusive but work in combinations that suit the organizational needs.

Another important aspect of database security is authentication. Since databases provide many views of the data, suitable privileges for the ability to drill down data requires appropriate authentication. The authentication aspect of database access supports the confidentiality in the CIA (Confidentiality-Integrity-Availability) triangle that is basic to information security. Authentication models discussed include single-factor, two-factor, and three-factor authentication and the attendant performance issues.

Among the many topics covered in this course, one of the important ones relates to Multi-Level Secure (MLS) databases [12, 14]. Commercial databases such as Oracle or SQL Server do not handle the MLS aspects in their software. However, it is an important aspect to be aware of. For example, in an

organization not every one has the access rights to view confidential information. Database queries are designed to pull all data that satisfy the query condition. In the MLS environment, the query condition would not necessarily reflect the security level of the person making the query. Since the security level authorization of the individual running the query is known from the login time, the MLS database is supposed to show all data that is cleared for that level of user. Usually the security levels could be unclassified, confidential, secret, or top secret. Not all fields of data in a record would need to be carrying a classification. Those sensitive data that have an associated security classification should be able to serve the needs of users with the appropriate security clearance and hide the data from others. A major problem to overcome in this context is known as **polyinstantiation** [13]. This concept refers to the fact that if persons with a lower clearance level have reason to suspect the existence of a record with hidden values, then they would be able to infer. Polyinstantiation could be addressed to a large extent by allowing certain redundancies in a database.

Another common problem with MLS databases is the presence of inference channel. Inference channel leaks information about data classified at a higher level to users with lower level clearances [19]. Security policies also play an important role in protecting against inference channel leaks. A related approach to this problem is to develop classification constraints on data. These data classifications are then used at query time and then the appropriate level of the constraint is applied to the resulting data before it is presented to the user.

In this context we discussed the security architecture for databases. This was broadly classified as those systems that use a Trusted Computing Base (TCB) that is external to the DBMS and those systems that manage access to data through the DBMS [22]. In the TCB architecture, the access controls were usually handled by the operating system or the network. In the DBMS control architecture, security design involved multi-factor authentication as well as security clearance and role-based access. As part of the secure architecture topic, we studied the Bell-LaPadula Model and the Biba Model [5]. Then we took a detailed look at the Seaview Model [17]. This is the first paper that studied in detail the security needs for database systems that contained data with various levels of security clearances. The major contribution of this paper was the application-independent nature of data integrity with particular reference to entity integrity, referential integrity and polyinstantiation integrity. We studied additional secure architecture topics with particular reference to commercial database systems. These topics include input validation, credential handling and encryption.

Encryption is a major topic in itself in the security context. Usually encryption is an important tool for data in transit. However, the recent spate of incidents involving lost or stolen data [37] shows the need for protecting data at rest from falling into the wrong hands. One useful tool in this regard is encryption. We studied the impact of encrypted data with respect to performance. Usually, encryption of sensitive data at rest is a desirable feature provided the access to such data is not frequent. On the other hand, for data that is frequently used the better alternative to encryption would be to partially secure storage [31, 33] whereby the data management is handled by an independent system that works outside the operating system control. This technique protects the data from hackers as the access control is under an independent system that is not manipulated by the operating system, where most of the vulnerabilities are exploited. In this context we studied the FARSITE model that discusses the reliable storage aspects in an incompletely trusted environment such as the Internet [2]. This research, performed at Microsoft, shows how "to harness the collective resources of loosely coupled, insecure, and unreliable machines to provide logically centralized, secure, and reliable file-storage service."

The next major topic covered was security audit for a database. The sources used for this topic were Jajodia [15], Andrews [4], and material from the Congressional Hearing reference provided in the References section. Audit involves different components such as login, access and storage. Commercial database systems such as Oracle and SQL Server facilitate login auditing in a simple way. For example, in SQL Server the user could set the login audit level to any one of four levels. Level 0 does not log any information about the logins, level 1 logs information about successful logins only, level 2 logs information about unsuccessful logins only and level 3 logs information about all attempted logins. This aspect of setting the appropriate level is related to the security policy of the organization. An organization might feel that they need to know only those people who attempted a login and failed as the ones who successfully logged in are considered authorized users. This is not a good assumption when it comes to computer forensics where one is trying to reconstruct an event that happened in the past. Consequently, organizations must consider the impact of their policies when it comes to information security. Auditing is also mandated by certain accreditation bodies. In order to satisfy certain data security requirements, some organizations might have to secure **C2 level security** rating from the National Computer Security Center (NCSC). The NCSC certification is measured according to the Department of Defense Trusted Computer System Evaluation Criteria [4]. We concluded the course with an analysis of database protection, copyright and privacy aspects both from a policy and legal perspective. First, we discussed the Congressional hearing on "Database and Collections of Information Misappropriation Act of 2003." This hearing showed the limitations of Copyright laws and how U.S. courts have interpreted the laws that protect privacy. We then studied the future of the database protection in U.S. and the laws to help in this regard. U.S. court rulings, including that of the Supreme Court, have shown that "sweat of the brow" argument does not offer protection for databases, rather the demonstration of some form of "originality" in data collection and dissemination is essential for database ownership. A court ruling in 2001 in United Kingdom in the case of the British Horseracing Board (BHB) has once again brought into focus the sweat of the brow argument. The U.K. court upheld the BHB's claim of ownership of data pertaining to horses and jockeys [10]. It remains to be seen how the U.S. courts would consider challenges to the sweat of the brow argument when it comes to protecting large databases from competitors.

4. EVALUATION TOOLS

In this course we used several different types of evaluation tools. Students were required to write three individual research reports on topics provided in class. The topics were:

1. Buffer overflows
2. Security audit
3. Sarbanes – Oxley Act and its impact on Database Security

On the testing side, we used a closed book, closed notes, midterm and final examinations. All questions were essay type. The students had access to a dedicated InfoSec lab where they could perform several different types of hands-on testing for vulnerabilities [32]. The InfoSec Lab has 16 workstations on a LAN connected to a Windows 2000 server. First the SQL Server 2000 was installed on the server. Two stand-alone computers that were not connected to the network were also provided to the students for testing. The first assignment provided a chance for the students to install SQL Server 2000 and choose appropriate security settings for various components of the database. The students then created new SQL Server accounts on the stand-alone computers and granted suitable privileges first and then tested the DENY and REVOKE features as well. The students had to install the latest SQL Server patches on the stand-alone computers and test for vulnerabilities.

The dedicated lab environment provided an excellent facility for us to allow students to understand how a hacker would gain routine information about the database system. First the SQL Server 2000 was left unpatched and the students used the SQL Ping2 utility to gather information about the database system. This showed the port 1433 in use. Then the SQL Server 2000 was patched with version 3a and the students tried the same SQL Ping2 utility, this time finding a different type of information about the SQL Server. Next, the SQL Server was put in hide mode and the students found out this piece of information by noticing that the listening port had changed to 2433. We were able to accomplish this testing by making changes to the SQL Server every two days giving a short time between changes for testing. This was done as assignment 2. The third assignment involved testing Bulk Copy / Bulk Insert features of SQL Server. The fourth assignment involved a buffer overflow attack. A sample code was given to the students to try the buffer overflow attack on the patched server. The patched server foiled the attack. The students were then asked to test the same buffer overflow attack on the stand-alone computers where patches were not applied. The last assignment involved SQL Injection attack. The students were given a series of codes for the SQL Injection attack testing. The first part involved logging into a SQL Server database system knowing the userid of the user but not the password. The second part involved not knowing the userid or the password. The third part involved creating a new user and then exploiting the system. The fourth part involved finding the password of the sa account. The fifth part involved dropping the SQL Server from the server and shutting down the SQL Server via SQL Injection attack. The students were given the challenge in the fourth part of the SQL Injection attack testing to find out the strong password used on the server, which had all the latest patches both for the SQL Server part and the operating system part. This required more work beyond the SQL knowledge. One of the students succeeded in finding out the server password, not just the sa password, which was much easier to get using SQL Injection.

5. CONCLUSION

Overall, the students enjoyed the content of the course that involved learning many database security concepts and the ability to test many aspects of SQL Server installation, suitable settings, detect vulnerabilities, develop simple countermeasures and have the ability to use the logs to detect intrusion.

6. ACKNOWLEDGEMENTS

This research was supported in part by the NSF grant DUE-0416900 and the Kentucky Council on Postsecondary Education grant GB040955.

7. REFERENCES

[1] Abrams, M. D., Jajodia, S., Podell, H. J. 1995. *Information Security: An integrated collection of essays*, IEEE Computer Society Press, CA.

[2] Adya, A., Bolosky, W.J., Castro, M., Cermak, G., Chaiken, R., Douceur, J., Howell, J., Lorch, J.R., Theimer, M. and Wattenhofer, R.P., 2002. "FARSITE: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment," Proceedings of the 5th Symposium on Operating Systems Design and Implementation, Boston, MA, December, 1 – 14.

[3] Afyouni, H. A. 2006. *Database Security and Auditing*, Course Technology, MA.

[4] Andrews, C., Litchfield, D., Grindlay, B. 2003. *SQL Server Security Fundamentals*, McGraw-Hill/Osborne, NY.

[5] Castano, S., Fugini, M., Martella, G., Samarati, P. 1994. *Database Security*, ACM Press Books (Diane Publishing Co.), NY.

[6] Cerrudo, C. "Manipulating Microsoft SQL Server Using SQL Injection" http://database.ittoolbox.com/browse.asp?c=DBPeerPublishing&r=%2Fpub%2FSG090202%2Epdf, Accessed on 07/25/2005

[7] CERT http://www.cert.org, Accessed on 05/20/2005

[8] CNSS Stds. "National IA Education Standards," http://www.nsa.gov/ia/academia/cnsstesstandards.cfm

[9] Congressional Hearing, 2003. "Database and Collections of Information Misappropriation Act of 2003," September. http://www.copyright.gov/docs/regstat092303.html, Accessed on 04/10/2005

[10] Duke University, 2001. "The Future of Database Protection in U.S. Copyright Law" http://www.law.duke.edu/journals/dltr/articles/2001dltr0017.html, Accessed on 04/15/2005

[11] Hinke, T., 1995. "Multilevel Secure Database Management Prototypes," in Information Security: An Integrated Collection of Essays, 1st edition**,** Edited by Abrams, M.D., Jajodia, S.G., Podell, H.J., Essay 23, IEEE Computer Society Press, CA, 542-569.

[12] Jajodia, S. and Sandhu, R., 1995. "Toward a Multilevel Secure Relational Model," in Information Security: An Integrated Collection of Essays, 1st edition**,** Edited by Abrams, M.D., Jajodia, S.G., Podell, H.J., Essay 20. IEEE Computer Society Press, CA, 460-492.

[13] Jajodia, S., Sandhu, R. and Blaustein, B.T., 1995. "Solutions to the Polyinstantiation Problem" in Information Security: An Integrated Collection of Essays, 1st edition**,** Edited by Abrams, M.D., Jajodia, S.G., Podell, H.J., Essay 21. IEEE Computer Society Press, CA, 493-529.

[14] Jajodia, S. and Meadows, C. 1995. "Inference problems in multilevel secure database management systems," in Information Security: An Integrated Collection of Essays, 1st edition**,** Edited by Abrams, M.D., Jajodia, S.G., Podell, H.J., Essay 24. IEEE Computer Society Press, CA, 570-584.

[15] Jajodia, S., Gadia, S.K., and Bhargava, G., 1995. "Logical Design of Audit Information in Relational Databases" in Information Security: An Integrated Collection of Essays, 1st edition**,** Edited by Abrams, M.D., Jajodia, S.G., Podell, H.J., Essay 25. IEEE Computer Society Press, CA, 585-595.

[16] Lewis, M. 2004. "*SQL Server Security Distilled*," 2nd edition, Apress, CA.

[17] Lunt, T., Denning, D. E., Schell, R. R., Heckman, M. and Shockley, W. R. 1990. "*The Seaview Security Model*," IEEE Transactions on Software Engineering, 16 (#6), June, 593 – 607.

[18] Mao, W. 2004. "*Modern Cryptography*," Prentice-Hall, NJ.

[19] Meadows, C. and Jajodia, S., 1995. "Integrity in Multilevel Secure Database Management Systems," in Information Security: An Integrated Collection of Essays, 1st edition**,** Edited by Abrams, M.D., Jajodia, S.G., Podell, H.J., Essay 22. IEEE Computer Society Press, CA, 530-541.

[20] Nevins, S.C., 2003. "Database security breaches on the rise" http://www.snwonline.com/evaluate/database_ security_03-31-03.asp?article_id=224, Accessed on 04/15/2005.

[21] Nessus http://www.nessus.org. Accessed on 05/19/2005.

[22] Notargiacomo, L. "Architectures for MLS Database Management Systems" in Information Security: An Integrated Collection of Essays, 1st edition**,** Edited by Abrams, M.D., Jajodia, S.G., Podell, H.J., Essay 19. IEEE Computer Society Press, CA.

[23] O'Reilly Publishers. Developing a Database Security Plan http://www.oreilly.com/catalog/orasec/chapter/ch07.html Accessed on 03/10/2005.

[24] PDD63, 1998. http://www.fas.org/irp/offdocs/pdd/pdd63.htm, Accessed on 05/22/2005.

[25] Pernul, Gunther, 1994. "Database Security" chapter in '*Advances in Computers*,' Edited by M.C.Yovits, vol. 38, Academic Press, NY.

[26] Rob, P. and Coronel, C. 2004. "*Design, Implementation and Management*," 6th Edn., Course Technology, MA.

[27] Sandhu, R. and Samarati, P., 1994. "Access Control: Principles and Practice," IEEE Communications Magazine, vol. 32, September, 40-48.

[28] Sandhu, R., Coyne, E.J., Feinstein, H. L. and Youman, C.E., 1996. "Role-based Access Control Models," IEEE Computer, vol. 29, February, 38-47.

[29] SANS http://www.sans.org, Accessed on 05/19/2005.

[30] Solworth, J. A. 2004. "Integrating Discretionary and Mandatory Access Controls" http://parsys.cs.uic.edu/~solworth/integratingMacDac.pdf. Accessed on 04/15/2005.

[31] Son, S. H., Chaney, C., and Thomlinson, N. P., "Partial Security Policies to Support Timeliness in Secure Real-time Databases," 1998. Proceedings of the IEEE Symposium on Security and Privacy, May 3-6, 136 – 147.

[32] Srinivasan, S. 2005. "Design and Development of an Information Security Laboratory," Proceedings of the 9th Annual Colloquium on Information System Security Education, Atlanta, GA, June 6-9.

[33] Strunk, J.D., Goodson, G.R., Scheinholtz, M.L., Soules, C.A.N. and Ganger, G.R., 2003. "Self-Securing Storage: Protecting Data in Compromised Systems," Foundations of Intrusion Tolerant Systems, 195 – 209.

[34] Theriault, M. and Heney, W. 1998. "*Oracle Security*," O'Reilly Publishers, IN.

[35] Tomson, B., 2004. "SQL Server 2000 Security Best Practices" http://wp.bitpipe.com/resource/org_1078177630_947/SQLserver2000.pdf. Accessed on 03/20/2005.

[36] UofL InfoSec, 2005. "InfoSec Program website," http://www.louisville.edu/infosec

[37] Wall Street Journal, 2005. "ChoicePoint struggles to gauge how much information fell into wrong hands," May 3, Page 1.