

Course name	Database Security	
Course ID: 40-734	Credits: 3	Program: Graduate
Prerequisites: Database Systems (The ugrad Course),		Co-requisites:
Prepared by: Rasool Jalili		

1. Aim

The course covers classical and new topics related to databases security. As one of the most important aspect of database security is access control of subjects (users/clients/agents/...) to objects (data/code/devices/...), the main part of the course focuses on Access Control models including Mandatory, Discretionary, and Role-Based. Such models are investigated from the Secrecy and Integrity aspects of security in database systems. In addition to Relational Databases as the dominant model in the industry and academia, the new non-relational database models such as Statistical, Object-Oriented, and XML-based are studied from the security perspective. Database outsourcing and Oracle security are also discussed as the final parts of the course.

2. Outline

The course is divided into 12 chapters as follows.

1. Introduction

- a. An introduction to database systems (concepts, components, query, advantages of databases vs. filing perspective).
- b. Security requirements (confidentiality, integrity, audit-ability, authentication, reliability, and availability)

2. Security Models

- a. Access control
- b. Inference and covert channels
- c. Open/close policy
- d. Discretionary/mandatory access control

3. Discretionary Access Control Models

- a. Matrix-based models
- b. Graph-based models
- c. Discretionary models specific to databases

4. Mandatory Access Control Models

- a. Secrecy-preserving models
- b. Integrity-preserving models
- c. Multi-level databases access control models
- d. Multi-level secure DBMS architecture

5. Role-based Access Control Models

- a. Role-based models
- b. Administrative role-based access control model

6. Statistical Databases Security
 - a. Conceptual techniques
 - b. Restrictive techniques
 - c. Perturbation techniques
7. Security Models for Next Generation Databases
 - a. Access control in object-oriented databases
 - b. Access control in XML-based databases
 - c. Access control in ontology-based databases
8. Privacy-Preserving Databases
 - a. Hippocratic databases
 - b. Privacy in database publishing
9. Audit Mechanisms in Relational Databases
10. Secure Database Architecture
11. Oracle Security Mechanisms (as a case study)

3. *Evaluation Criteria*

1. Assignments: 10%
2. Mid-term exam: 30%
3. Survey paper: 20%
4. Final Exam: 40%

4. *References*

1. S. Castano, M. G. Fugini, G. Martella, and P. Samarati, "Database Security," Addison-Wesley, 1996.
2. E. Bertino, R. Sandhu, "Database Security – Concepts, Approaches, and Challenges," IEEE Transaction on Dependable and Secure Computing, vol. 2, no. 1, 2005.

Additional references

1. M. Bishop, Computer Security: Art and Science, 2nd ed: Addison-Wesley, 2003.
2. J. A. Goguen and J. Meseguer, "Security Policy and Security Models," presented at IEEE Symposium on Security and Privacy, 1982.
3. D. E. Denning, "Secure Distributed Data Views: The Sea-View Formal Security Model," SRI International, Technical Report A003, 1987.
4. K. P. Smith and M. S. Winslett, "Entity Modeling in the MLS Relational Model," presented at 18th Conference on Very Large Databases, Vancouver, Canada, 1992.
5. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," IEEE Computer, vol. 29, pp. 38-47, 1996.

6. M. Nyanchama and S. L. Osborn, "The Role Graph Model and Conflict of Interest," *ACM Transaction on Information Systems Security*, vol. 2, pp. 3-33, 1999.
7. R. S. Sandhu, V. Bhamidipati, E. J. Coyne, S. Ganta, and C. E. Youman, "The ARBAC97 Model for Role-Based Administration of Roles: Preliminary Description and Outline," presented at ACM Workshop on Role-Based Access Control, 1997.
8. D. E. Denning and J. Schlörner, "Inference Controls for Statistical Databases," *IEEE Computer*, vol. 16, pp. 69-82, 1983.
9. D. Denning, "Views for Multi-level Data base Security," *IEEE Trans- Software Eng.* 1987.
10. E. Bertino and H. Weigand, "An Approach to Authorization Modeling in Object-Oriented Database Systems," *Data and Knowledge Engineering*, vol. 12, pp. 1-29, 1994.
11. A. Gabillon and E. Bruno, "Regulating Access to XML Documents," presented at 5th Annual Working Conference on Database and Application Security (DAS'01), Niagara, Ontario, Canada, 2002.
12. E. Damiani, S. D. C. d. Vimercati, S. Paraboschi, and P. Samarati, "Securing XML Documents," presented at International Conference on Extending Database Technology (EDBT 2000), Konstanz, Germany, 2000.
13. M. Kudo and S. Hada, "XML Document Security based on Provisional Authorization," *presented at ACM Conference on Computer and Communication Security (CCS 2000)*, 2000.
14. A. Masoumzadeh, M. Amini, and R. Jalili, "Context-Aware Provisional Access Control," *presented at 2nd International Conference on Information Systems Security (ICISS'06)*, Kolkata, India, 2006.
15. S. Javanmardi, M. Amini, and R. Jalili, "An Access Control Model for Protecting Semantic Web Resources," presented at 2nd International Semantic Web Policy Workshop (SWPW'06) 2006, Athens, GA, USA, 2006.
16. M. Theriault and A. Newman "Oracle Security Handbook" Osborn/McGraw-Hill 2001