

ITMS 428 Database Security
Fall 2018

Maurice Dawson

Syllabus

Professor: Prof. Maurice Dawson, D.Sc., Ph.D., SMIEEE**Address:** Perlstein Hall 10 W 33rd St, Room 223, Chicago IL 60616**Telephone:** 312.567.5246**Mobile:** 571.317.1893**Fax:** 312.567.5283**Email:** mdawson2@iit.edu**Office(s):** Main Campus - Perlstein Hall 10 W 33rd St, Room 221E, Chicago IL 60616**Office Hours:** Main Campus: By Appointment & 1:00 pm - 3:00 pm TR

Course Catalog Description: Students will engage in an in-depth examination of topics in data security including security considerations in applications and systems development, encryption methods, cryptography law and security architecture and models.

Prerequisites: ITMD 421**Credit:** 3-0-3 (*lecture courses*) Semester Hours

Course Outcome: Each student will learn the fundamentals of database security as well as concepts and technologies such as encapsulation (information hiding) and using relational database security management techniques. They will be conversant with database hardening on a variety of platforms, defense against the most common threats and attacks, and the legal and regulatory environment impacting database security.

Lecture Days, Time & Place: Tuesday & Thursday 3:15pm to 4:30pm, *Rettaliata Engineering Center 242*, 10 W. 33rd Street on IIT's Main Campus, or online via IIT Online.

Schedule of Topics/Readings:

Dates	Topic	Reading Material 1	Reading Material 2	Additional Reading Material
August 20	1. Overview of Cyber Security 2. Operating System Security Fundamentals	Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company. chapter 24	Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	Anderson, R. J. (2010). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons. chapter 1
August 27	1. Access Controls - definitions and principles 2. Access Controls - threats 3. Access Controls - types of access control 4. Access Controls - access control models 5. Access Controls - monitor and management 6. NIST 800-57 Controls	Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company. chapter 24	Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	Anderson, R. J. (2010). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons. chapter 4
September 3	Labor Day - No Classes	Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company. chapter	Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST	Security and Privacy Controls for Federal Information Systems and Organizations. Available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

ITMS 428 Database Security
Fall 2018

Maurice Dawson

		24	SP)-800-53 Rev 4).	
September 10	Setting up a database environment	Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company. chapter 24	Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	1. Databases for beginners. Available at http://zcht.home.amu.edu.pl/pliki/Databases%20for%20beginners.pdf 2. How to Mitigate the Most Significant Database Vulnerabilities. Available at http://schell.com/Top_Ten_Database_Threats.pdf
September 17	Securing a database environment	Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company. chapter 24	Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	Bertino, E., & Sandhu, R. (2005). Database security-concepts, approaches, and challenges. IEEE Transactions on Dependable and secure computing, 2(1), 2-19. Available at https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-99.ps
September 24	1. Enterprise database architecture 2. Distributed systems	Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company. chapter 2	Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	Anderson, R. J. (2010). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons. chapter 6
October 1	1. Discussion on database assignment in Ethiopia with Catholic Relief Services	Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company. chapter 2	Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	Dawson provide information for CRS project assignment.
October 8	Fall Break Day - No Classes	Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company. chapter 3	Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	
October 15	Midterm	Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company. chapter 24	Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	

ITMS 428 Database Security
Fall 2018

Maurice Dawson

October 22	1. Database Encryption and Masking 2. Watermarking	Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company. chapter 24	Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	Shmueli, E., Vaisenberg, R., Elovici, Y., & Glezer, C. (2010). Database encryption: an overview of contemporary challenges and design considerations. ACM SIGMOD Record, 38(3), 29-34. Available at http://www09.sigmod.org/sigmod/record/issues/0909/p29.surveys.shmueli.pdf
October 29	1. SQL injection 2. cyber analytics for database content	Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company. chapter 4-5	Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	Halfond, W. G., Viegas, J., & Orso, A. (2006, March). A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE International Symposium on Secure Software Engineering (Vol. 1, pp. 13-15). IEEE. Available at https://www.cc.gatech.edu/fac/Alex.Orso/papers/halfond.viegas.orso.ISSS.E06.pdf
November 5	Group project and presentation start		Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	
November 12	Group project and presentation cont.		Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	
November 19	Final exam review		Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	
November 26	Thanksgiving Break - No Classes		Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4).	
December 3	Final Exam Week/Final Grading Begins on Dec 3			
December 10	No class			

ITMS 428 Database Security
Fall 2018

Maurice Dawson

December 12	No class Final Grades Due at Noon (12 p.m. CST)			
----------------	--	--	--	--

Textbook: The textbook for this course is **mandatory**.

Elmasri, R., & Navathe, S. (2010). Fundamentals of database systems. Addison-Wesley Publishing Company [instructor provided digital copy]

Ross, R. S. (2013). Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13] (No. Special Publication (NIST SP)-800-53 Rev 4). [instructor provided digital copy]

Readings/Videos: Readings for the class will be assigned from the textbook as well as in the form of online reading. Online resources and videos will be linked from or embedded in a Blackboard page. It is essential that you do all readings and/or view the videos before coming to class on the assigned date. These materials are a necessary and integral part of the class and will form the basis for any class discussions on the topic. Specific readings are assigned by topic above.

Course Objectives: At the conclusion of this course, each successful student will be able to:

- Recall and describe concepts of information security
- Describe and explain security architectures for protection of database resources
- Secure and harden database deployments using leading industry-standard database management systems
- Recall and describe access control approaches, including authentication, authorization, privileges and roles
- Discuss cryptography and encryption
 - ✓ Identify elements of a cryptographic system
 - ✓ Describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation
- Describe the technical details of SQL injection attacks
- Explain how to protect against SQL injection attacks
- Discuss issues and recall techniques and best practices in the protection of Big Data and data in the cloud
- Describe and discuss the processes of auditing and testing database security
- Describe and understand NoSQL and different types of NoSQL

Course Notes: Copies of the course lecture notes in the form of a PDF of the PowerPoint presentation accompanying each lecture will be provided for each student on Blackboard. This should be useful if you must miss a class. You should be aware that note taking is encouraged and should help your understanding of the material.

Course Web Site: <http://blackboard.iit.edu/>

Blackboard: The course will make intensive use of Blackboard (<http://blackboard.iit.edu/>) for communications, assignment submissions, group project coordination, providing online resources and administering examinations. All remote students will view the course lectures online via Blackboard, and online readings will be found on Blackboard.

Attendance: If you are in a live section of the class and will not be able to attend class, please notify me via email or by text message to 847.920.8442 prior to class time. Live section students who miss a class should always watch the lecture online.

Writing Assignments: There will be three additional writing assignments for this class. Below is a brief overview of final assignments.

Research Paper - Graduate Students: A research paper addressing a topic in *whatever you specify*. The paper will be fifteen to twenty pages long and will meet standards expected of a paper submitted for journal publication. Instructions for submission of the paper will be included with the assignment on Blackboard. You must fully attribute all material directly quoted and you must document all sources used in the preparation of the paper using complete, APA-style bibliographic entries. *Failure to format your bibliography entries in APA style will result in an automatic reduction of one letter grade for this assignment.* No more than twenty-five percent of material included in any paper may be direct quotes. No more than sixty percent of the resources cited may be from online. Submission of the paper for actual publication is highly encouraged. A basic outline for your paper—which should be at least three pages in length—will be due **September 24th**. The paper will be due **November 27th**. More specific instructions for the outline and the paper will be provided on Blackboard.

ITMS 428 Database Security
Fall 2018

Maurice Dawson

Examinations: The final examination will consist of an in-class essay examination measuring course outcomes as discussed above. The examination will be open-book, open note, and open-Web. Internet students may complete this exam online. (See exam statement for other options)

Academic Honesty:

Plagiarism: All work you submit in this course **must be your own**. You must fully attribute **all** material directly quoted in papers and you must document all sources used in the preparation of the paper using complete, APA-style bibliographic entries. Including directly quoted material in an assignment without attribution is always plagiarism and will always be treated as such by me. No more than thirty-three percent of material included in any paper may be direct quotes. Students have submitted plagiarized material the last six times I have taught this course and **I will not tolerate it**. If you submit plagiarized material you **WILL** receive a grade of **ZERO** for the assignment, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies. **There is no excuse for not understanding this policy** and if you do not understand it please let me know and I will be happy to discuss it with you until you do. (Should include assignment or lab collaboration statement as necessary.)

Grading: Grading criteria for ITMS 428-528 students will be as follows:

A	<i>Outstanding work reflecting substantial effort</i>	90-100%
B	<i>Excellent work reflecting good effort</i>	80-89.99%
C	<i>Satisfactory work meeting minimum expectations</i>	70-79.99%
D	<i>Substandard work not meeting expectations</i>	60-69.99%
E	<i>Unsatisfactory work</i>	0-59.99%

Grading criteria for ITMS 428-528 students will be as follows:

A	<i>Outstanding work reflecting substantial effort</i>	90-100%
B	<i>Adequate work fully meeting that expected of a graduate student</i>	80-89.99%
C	<i>Weak but marginally satisfactory work not fully meeting expectations</i>	65-79.99%
E	<i>Unsatisfactory work</i>	0-64.99%

The final grade for the class will be calculated as follows:

Assignments	28%
Labs	30%
Exams	42%

*An additional 10% will be random quizzes that will count for participation

Other Class Resources: Online readings and other class resources may be found at on Blackboard.

Our Contract: This syllabus is my contract with you as to what I will deliver and what I expect from you. If I change the syllabus, I will issue a revised version of the syllabus; the latest version will always be available on Blackboard. Revisions to readings and assignments will be communicated via Blackboard.

Disabilities: Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources and make an appointment to speak with me as soon as possible. My office hours are listed on the first page of the syllabus. The Center for Disability Resources (CDR) is located in 3424 S. State St., room 1C3-2 (on the first floor), telephone 312.567.5744 or disabilities@iit.edu.