

## MET CS 674 A1/EL – Fall 2017: DATABASE SECURITY

# SYLLABUS

*Boston University Metropolitan College*

*Boston Campus and eLive*

Schedule	Thursday 18:00-21:00 US Eastern Time
Location	Room 134 Fuller Building 808 Commonwealth Ave
Instructor	Andrew D. Wolfe, Jr, M.S.C.S. 808 Commonwealth Avenue, Rm 225 617-358-1984 781-405-9118
Email	<a href="mailto:awolfe@bu.edu">awolfe@bu.edu</a>
Office hours	2:00-4:00 pm Tuesdays at my office or by prior arrangement Zoom or other webconferencing by arrangement

### COURSE DESCRIPTION

The course provides a strong foundation in database security and auditing. This course utilizes Oracle scenarios and step-by-step examples. The following topics are covered: security, profiles, password policies, privileges and roles, Virtual Private Databases, and auditing. The course also covers advanced topics such as SQL injection, database management security issues such as securing the DBMS, enforcing access controls, and related issues.

### FORMAT

This course is presented in the “blended” or “e-Live” format. Fourteen sessions are planned over the course of the semester. Conventional students are expected to attend every lecture. E-Live students are required to attend four ‘plenary’ sessions. Each lecture, ‘plenary’ or not, will be videotaped and posted to the course site in BU Blackboard Learn within a few days of the actual lecture. The lectures will also be ‘simulcast’ via Adobe Connect for those students who can use it. You can also participate remotely, stating your questions or comments via audio, for example, using a microphone or headset on your computer. Plenary dates are as follows:

- September 11
- October 2
- November 6
- December 11
- December 19 (Projected final exam)

### OBJECTIVES

The objective we share in this course is that each student understand the application of security concepts to database technology and demonstrate the ability to work hands-on.

Specific topic objectives are:

- Understand the fundamentals of security, and how it relates to information systems

*last revision Friday, August 25, 2017*

- Identify assets in your organization and their values
- Identify risks and vulnerabilities in operating systems from a database perspective
- Learn good password policies, and techniques to secure passwords in your organization
- Learn and implement administration policies for users
- Use Oracle to create policies, profiles and roles
- Understand the various database security models and their advantages or disadvantages
- Learn how to implement a Virtual Private Database using views, roles, and application context
- Gain an overview of auditing fundamentals, and create your own auditing model
- Learn the purpose and use of data dictionaries, encryption and SQL injection
- Explore an interesting research topic of your choice related to database security

### **PREREQUISITES**

You are required to have working knowledge of a DBMS. It is assumed that you have taken CS579 or CS 669, or the requirement has been waived. *There will be an elementary database quiz at the first session.* Please contact the instructor if you use a DBMS at work, or have questions about pre-reqs.

### **COURSE TEXTS**

**There is no required textbook for MET CS 674 for Fall 2017**

#### **Optional**

***HOWTO Secure and Audit Oracle 10g and 11g***

by Ron Ben-Natan

Publisher: Auerbach Publications; 1 edition (March 10, 2009)

ISBN-10: 1420084127

ISBN-13: 978-1420084122

### **GRADING RUBRIC**

Subject mastery and evident hard work are the key things I am seeking in student performance.

#### ***Assignments - Go the Extra Mile***

The specific instructions for the standard assignments are, to some degree, *starting points* for your work. If you do only what is on the assignment, your grade will not be 100. You must demonstrate *understanding* by going above and beyond the assignment. The following will raise your grade to the top levels:

- Discussion of the meaning and use of the steps in the assignment
- Explaining how the steps in the assignment work
- Adding variations in addition to the specified steps of the assignment, for example, an example with a different set of permissions or an additional query to show unexplored aspects of the problem
- Descriptions of tradeoffs in doing the same thing in different ways

**Overall Grade**

The following is the weighting of grading criteria for this course.

**Grading Rubric**

Category	Weighting
Homework and Labs	20%
Quizzes	20%
Term Project	20%
Final Exam	20%
VPD Mini-Project	10%
Class and Online Participation	5%
Term Project Presentation	5%
	<b>100%</b>

**Participation Grades**

When a student participates in a class discussion I will be looking for the following qualities:

- Applicability to the topic under discussion
- Responsiveness to the points raised by others
- Demonstration of conceptual mastery
- Citation (may be informal) of pertinent materials

**VPD Mini-Project Evaluation**

The VPD lab is a substantial security project in and of itself. Because of its substantial challenges, completing each step will merit a grade of 97.

**Project Evaluation Criteria**

The term project must include a word processing document of 2000-3000 words. Powerpoint or other slide decks will *not be accepted*. Acceptable formats are Word, HTML, PDF. Collections of files, including source code, may be combined into a single ZIP-format file for submission.

The term project should explore or present original material in database security. You may choose your own project topic or choose from a selected topic. We will be discussing project topics in class, after which you will submit the topic you want to explore. Project topics are subject to instructor approval.

The following characteristics will be used to grade the term project:

- Application of basic security concepts to the specific topic
- Demonstrated understanding of technologies involved
- Proper academic formatting including table of contents, abstract,
- Describe methodology
- Comprehensiveness and depth
- Demonstrates technology
- Regulations and standards
- Helpful contrasts

- Coherent
- References in proper format

### ***Not Required in Grade***

- Exceptional native intelligence
- Substantial personal experience in topic
- Witty repartée

### ***Late or Missed Work***

In case of personal emergency or other circumstances that prevent you from fulfilling an assignment, taking a quiz or test, or attending class, please contact me before it is due.

Grade penalties for late submission may be waived if you provide this level of notice along with a reasonable and credible explanation.

***Course grade will be penalized 10 points for each assignment that has not been submitted as of the final exam.***

### **ACADEMIC INTEGRITY**

- *WRITE IT, OR CITE IT!*

Please download and review the Policy on Academic Conduct from the following page:

<http://www.bu.edu/met/for-students/met-policies-procedures-resources/academic-conduct-code/>

Neither the University, nor I, nor your classmates can tolerate plagiarism in any formal submission for this class. Please show appropriate respect for all by expressing your own mastery of the material in your own words, diagrams, programming, etc. When you include quotations, mark and attribute them clearly and in appropriate academic style. Contact your instructor with any questions.

### **SCHEDULE (*subject to revision*)**

***Bold Letter*** lectures indicate plenary sessions for which we require in-classroom attendance of e-Live students.

E-Live students are welcome to attend any session of the course in addition to the required plenary session.

### **CS 674 D1/EL Calendar for Fall 2017**

<b>Session</b>	<b>Date</b>	<b>Topics</b>
<b>01+A</b>	09-11	Introduction - Overview
02	09-18	Security Concepts, Security Architecture, Types of Attacks
03	09-25	User Creation and Administration
<b>04+B</b>	10-02	Profiles, Passwords Privileges, Roles
05	10-10	TUESDAY CLASS Flipped class: labs 1, 2
06	10-17	Application Security Models
OUT	10-24	No class. I will be giving a database security presentation overseas.
07	10-31	Further authorization

Session	Date	Topics
<b>08+C</b>	11-06	Virtual Private Databases
9	11-13	Virtual Private Databases
10	11-20	Database Auditing Models
11	11-27	Application and Data Auditing
12	12-4	Database Activity Auditing
<b>13+D</b>	12-11	Special Cases; Advanced Topics and SQL Injection
<b>14+F</b>	12-19	Final Exam (tentative)

### IMPORTANT NOTES

- We provide a virtual machine appliance for you to use during the course. This can be operated on Windows, Linux, and Macintosh OS X. The operating system internal to the virtual machine is Linux. The virtual machine is run under the free VirtualBox application, download from <http://www.virtualbox.org>.