Network Security
Fall 2020 - MET CS 690 OL

Instructor

Edward Matthews, DB Security, DB Concepts, Python
Part time instructor, Computer Science Department Metropolitan College Boston University

Office hours: By prior arrangement.

E-mail: ematth01@bu.edu; matthews44@gmail.com

Course Description

This course covers advanced network security issues and solutions. The course starts with consideration of why network security is necessary, network vulnerabilities and the types of attacks networks need to defend against. Discussion of basic security concepts, security services, and the role played by encryption and hash algorithms. Along with issues and approaches for key management follow. Particular focus and emphasis are then covered regarding to network security capabilities and mechanisms (Access Control on wired and wireless networks), IPsec, Firewalls, Deep Packet Inspection and network flow monitoring. A discussion of network application security (Email, Web, P2P, etc.) is presented followed by consideration of network utility (DNS, NTP, etc.) and management protocols (SNMP, RMON, etc.), management tools (Syslog, vulnerability scanning, penetration texting, etc.). Followed by a review of necessary operational security processes and activities. Discussion of remote access issues, such as dial-up servers, modems, VPN gateways and clients are included, as with the basic security concepts of cloud security.

Prerequisites

- MET CS535 or MET CS625 Data Communications and Computer Networks;
- Familiarity with the OSI and TCP/IP protocol stacks.
- Familiarity with binary numbers, prime numbers. Base conversion between binary, hexadecimal, and decimal numbering systems.
- Familiarity with computer programming concepts.

Required Course Book

Computer & Internet Security – A Hands-on Approach, Wenliang Du, 2nd Edition, Independently published, May 2019, ISBN 978-1-7330039-3-3

Introduction to Network Security – Theory and Practice, Jie Wang, Zackary Kissel**,** 2nd Edition, John Wiley and Sons, 2015, ISBN 978-1-1189-3948-2

(Students have access to this through the BU Library and can download the eCopy of the text.)

Courseware

This course uses Online Campus (Blackboard). Once the course starts all students must use the Online Campus Dashboard internal messages service.

Use Online campus:

- for reading assignments beyond textbook assigned reading,
- Submitting homework assignments,
- Submitting lab exercises,
- Taking on-line quizzes,
- Participating in discussion threads
- Taking the on-line final examination and practice final exam
- All course related email correspondence.

Fall 2020 COVID-19 Policies

Classroom Rotations: [*for courses with rooms that cannot accommodate the all students wanting to meet in-person*] Classrooms on campus have new capacities that follow guidelines issued by state and local health and government authorities related to COVID-19 and physical distancing. Before the beginning of the class, and throughout the semester, I will be reaching out to students who have indicated that they want to attend the classroom in-person. Our classroom hold [] students, and therefore we will have [two] rotations of students that come to class on campus alternate weeks. You will be asked to attend remotely on the week that you have rotated out the classroom.

Compliance: All students returning to campus will be required, through a digital agreement, to commit to a set of Health Commitments and Expectations including face coverings, symptom attestation, testing, contact tracing, quarantine, and isolation. The agreement makes clear that compliance is a condition of being a member of our on-campus community.

You have a critical role to play in minimizing transmission of COVID-19 within the University community, so the University is requiring that you make your own health and safety commitments. Additionally, if you will be attending this class in person, you will be asked to show your Healthway badge on your mobile device to the instructor in the classroom prior to starting class, and wear your face mask over your mouth and nose at all times. If you do not comply with these rules you will be asked to leave the classroom. If you refuse to leave the class, the instructor will inform the class that they will not proceed with instruction until you leave the room. If you still refuse to leave the room, the instructor will dismiss the class and will contact the academic Dean's office for follow up.

Boston University is committed to offering the best learning environment for you, but to succeed, we need your help. We all must be responsible and respectful. If you do not want to follow these guidelines, you must participate in class remotely, so that you do not put your classmates or others at undue risk. We are counting on all members of our community to be courteous and collegial, whether they are with classmates and colleagues on campus, in the classroom, or engaging with us remotely, as we work together this fall semester.

Class Policies

1) Assignment, Lab Exercise and Discussion Completion & Late Work
   - Homework assignments are mandatory, must be completed and submitted in a timely manner, and are required to be submitted via Online Campus for this course. If a student will be unable to submit an assignment by its due date, the student must contact the Instructor or Facilitator **in advance** to avoid a grade of zero (0) on the submitted material.
   - Lab exercises: are mandatory, must be completed and submitted in a timely manner, and are required to be submitted via Online Campus for this course. If a student will be unable

to submit a Lab exercise by its due date, the student must contact the Instructor or Facilitator **in advance** to avoid a grade of zero (0) on the submitted material.

- Student postings to discussion topic after the listed closing dates will not be counted when calculating a student's discussion grades.

2) Academic Conduct Code – Cheating and plagiarism will not be tolerated in any Metropolitan College course. Such activities/behavior will result in no credit for the assignment or examination and may lead to disciplinary actions. Please take the time to review the Student Academic Conduct Code:

http://www.bu.edu/met/metropolitan_college_people/student/resources/conduct/code.html.

Such activities/behavior includes copying (even with modifications) of another student's work or letting your work to be copied. Your participation in interactions with the instructor and your classmates is encouraged, but the work you submit must be your own. Collaboration is not permitted.

Assignments

- All homework assignments are identified within the Online campus Class specific site.
- File names for assignment documents should be:

  CS690-HW<number>-<student last name>.doc

  An example assignment document file name is:

  CS690-HW5-Matthews.doc

  Student submissions which fail to follow this direction will have 5 points deducted!
- Student assignment submissions must be no more than 4 pages in length, be single spaced**,** use 12 point Times Roman type font and 1" margins on all sides. Student submissions which fail to follow this direction will have points deducted!
- Include the file name in the header and a page number in the footer of you assignment submission document. Student submissions which fail to follow this direction will have points deducted!
- Title cover pages are not required and should not be used;
- Assignment submission documents MUST be in Word 2016 or greater file formats that are NOT encoded in XML;
- Quoted material and citations must follow the American Psychological Association (APA) format with a reference section at the end of a student's submitted work. Please refer to the http://www.apastyle.org/ web site for guidance on following the APA style guide.
- Students are required to comply with the directions contained within the document

  APA Criteria for Course.pdf

  whenever the work of others is used as part of a student's assignment submission. Failure to do so will result in points being deducted for the assignment grade.
- Wikipedia is a useful starting point for finding information about a subject BUT NOT an acceptable direct reference source. One should only reference or quote from primary (source) documents.

Lab Exercises

- Lab exercises are identified within the Assignment description document for each course module.
- File names for lab exercise documents should be:

CS690-LAB<number>-<student last name>.doc

An example lab exercise document file name is:

CS690-LAB5-Heister.doc

Student submissions which fail to follow this direction will have 5 points deducted!

- Students should enter their lab exercise answers direct within each lab exercise document and then submit the completed document appropriately renamed as stated above;
- Lab exercise submission documents MUST be in Word 2016 or greater file formats that are NOT encoded in XML.

Discussion Threads

- Each course module includes a discussion topic that students are required to participate in. Student discussion postings will be graded as per the "Discussion Grading Rubric" under the Online Campus " Syllabus and Course Information" area.

Examinations

- Students are required to take six on-line quizzes (one per module) while the course is running. Students will be allowed 75 minutes to complete each quiz. A student may take each of these quizzes in the window that they are available via Online Campus If a student cannot complete a quiz during the week each quiz is available, the student must make prior arrangements with the instructor.
- Students are required to take a proctored final exam that will last 3 hours. This exam is open book and open notes.
- A practice final exam will be available on Online Campus which can be taken as many times as a student wishes.
- If any work is to be completed beyond the scheduled dates of this course the student must negotiate a Boston University "Contract for an Incomplete Grade" with the professor prior to the end of the class.

Study Guide

Module 1 Study Guide and Deliverables	
Readings	Wang Textbook Chapter 1 1.3 Attacker Profiles 1.4 Basic Security Model 1.5 Security Resources Du Textbook Example attack The file Module 1 Example Company Security Policy - Extract.pdf The file Module 1 Network Overview and Review.pdf
Discussions	Make posts to Blackboard Discussion Board Discussion 1 Forum. Students are expected to create at least one new Discussion 1 Forum Thread and post comments to Threads created by other students.
Assignments	Complete and submit Assignment 1 via Blackboard Assignments
Assessments	Complete and submit Quiz 1 via Blackboard Assessments
Module 2 Study Guide and Deliverables	
Readings	Du Computer & Internet Security Textbook Chapter 21 Chapter 22 Chapter 21, sections 21.1 What is Cryptography THROUGH 21.7 Hash Algorithms Chapter 21 sections 21.1 Introduction THROUGH 21.3 DES Overview Chapter 23 Public Key Cryptography 23.1 Introduction THROUGH 23.6 Digital Signature using RSA 24.3 Certificate Authority THROUGH 24.4.5 Trusted Cas in the real world 24.2.1 x.509 Digital Certificates and 24.7 Types of digital certs 23.2 Diffie Hellman 24.1.2 Man in the middle attacks THROUGH 24.6 Attacks on PKI Wang Textbook Chapter 3 - Cryptography 2.7 Stream Ciphers, 2.7.1 RC4 Stream Cipher Chapter 15 15.1 Introduction THROUGH 15.3 DES and AES Algorithms 17.3 The RSA Algorithm THROUGH 17.3.4
Discussions	Make posts to Blackboard Discussion Board Discussion 2 Forum. Students are expected to create at least one new Discussion 2 Forum Thread and post

	comments to Threads created by other students.
Assignments	Complete and submit Assignment 2 via Blackboard Assignments
Assessments	Complete and submit Quiz 2 via Blackboard Assessments
Module 3 Study Guide and Deliverables	
Readings	Du Computer & Internet Security Textbook Chapter 22 22.1 Introduction THROUGH 22.2.1 Cryptographic Properties 22.3.1 MD5 22.3.2 SHA-1 THROUGH 5.6.1 SHA-1 Message Padding Wang Chapter 3 3.6 Key Distribution and Management 4.2.3 Data Authentication Algorithm The Blackboard material for this module
Discussions	Make posts to Blackboard Discussion Board Discussion 3 Forum. Students are expected to create at least one new Discussion 3 Forum Thread and post comments to Threads created by other students.
Assignments	Complete and submit Assignment 3 via Blackboard Assignments
Assessments	Complete and submit Quiz 3 via Blackboard Assessments
Lab exercises	Complete and submit Lab 1 via Blackboard Assignments
Module 4 Study Guide and Deliverables	
Readings	Du 17.2 Types of Firewalls THROUGH 17.8 Evading Firewalls Wang 5.3 IPSec 5.3.1 IPSec SAs 8.2 Packet Filters THROUGH 8.8 Setting up Firewalls The Blackboard material for this module
Discussions	Make posts to Blackboard Discussion Board Discussion 4 Forum. Students are expected to create at least one new Discussion 4 Forum Thread and post comments to Threads created by other students.
Assignments	Complete and submit Assignment 4 via Blackboard Assignments
Assessments	Complete and submit Quiz 4 via Blackboard Assessments
Lab exercises	Complete and submit Lab 2 via Blackboard Assignments
Module 5 Study Guide and Deliverables	
	Wang Chapter 7 Cloud Security

Readings	7.1 The Cloud Service Models THROUGH 7.6 Searchable Encryption Chapter 9 Intrusion Detection 9.1 Basic Intrusion detection THROUGH 9.6 Honeypots Du Chapter 16 16.3.1 TCP Reset Attack THROUGH 16.4.5 Creating Reverse Shell The Blackboard material for this module The file Module 5 A Review of Anomaly based Intrusion Detection Systems.pdf The file Module 5 Limitations of Network Intrusion Detection.pdf The file Module 5 Towards Next-Generation Intrusion Detection.pdf The file Module 5 Recent Advances and Future Trends in Honeypot Research.pdf The file Module 5 A Honeypot System for Efficient Capture and Analysis of Network Attack Traffic.pdf The file Module 5 Honeypot in Network Security- A Survey.pdf The file Module 5 An Overview of IP Flow-Based Intrusion Detection.pdf The file Module 5 A survey of network flow applications.pdf
Discussions	Make posts to Blackboard Discussion Board Discussion 5 Forum. Students are expected to create at least one new Discussion 5 Forum Thread and post comments to Threads created by other students.
Assignments	Complete and submit Assignment 5 via Blackboard Assignments
Assessments	Complete and submit Quiz 5 via Blackboard Assessments
Lab exercises	Complete and submit Lab 3 via Blackboard Assignments
Module 6 Study Guide and Deliverables	
Readings	Wang Chapter 6 Wireless Network Security 6.1.1 WLAN architecture THROUGH 6.7 Wireless Mesh Network security Chapter 10 Anti Malicious Software 10.1 Viruses THROUGH 10.8 DDoS DU Chapter 12 SQL Injection Attack Chapter 13 Meltdown Attack Chapter 14 Spectre Attack The Blackboard material for this module The file Module 6 Guide to Computer Security Log Management.pdf

	The file Module 6 The design and implement of the centralized log gathering and analysis system.pdf The file Module 6 Log management comprehensive architecture in Security Operation Center.pdf The file Module 6 Technical Guide to Information Security Testing and Assessment.pdf
Discussions	Make posts to Blackboard Discussion Board Discussion 6 Forum. Students are expected to create at least one new Discussion 6 Forum Thread and post comments to Threads created by other students.
Assignments	Complete and submit Assignment 6 via Blackboard Assignments
Assessments	Complete and submit Quiz 6 via Blackboard Assessment

Grading Criteria

Students will have to do homework assignments to help you master the material. You will also have to read the textbooks and to be ready to discuss the issues related to the current class topics.

Grades will be based on:

- home work assignments (25%)
- quizzes (25%)
- lab exercises (10%)
- discussion thread/class participation (10%)
- proctored final exam (30%)

Grade ranges are as follows:

- 94 <= is an A
- 90 <= and < 94 is an A-
- 87 <= and < 90 is a B+
- 84 <= and < 87 is a B
- 80 <= and < 84 is a B-
- 77 <= and < 80 is a C+
- 74 <= and < 77 is a C
- 70 <= and < 74 is a C-
- 60 <= and < 70 is an F

Course Learning Objectives

Upon successful completion of this course students will be able to:

- Describe and correctly use the terminology and concepts associated with information security.
- Understand and be able to discuss the general concepts of information security governance.
- Understand and be able to discuss the importance of balancing the use of security policies, processes, technology and operations vs. costs to minimize organizational security risks.
- Develop detailed security requirements based on business needs, threat profiles, security policy obligations and asset vulnerabilities and exposure.
- Identify what type of protection different security services provide and which technical controls (e.g., symmetric/asymmetric encryption, cryptographically secure hash algorithms, key management approaches) are necessary to provide needed security services.
- Perform risk management activities, such as: asset assessments, determine probable threats and risks that drive solution architectural alternatives, trade-off studies, modeling and design issues.
- Describe and discuss security issues within general operating systems, specific commercial operating systems and application software
- Discuss the considerations when selecting appropriate anti-malware technologies.
- Describe and discuss security issues within common used network protocols and the approaches for mitigating communications associated threats.
- Prepare service/product security architectures and designs that sufficiently comply with enterprise security requirements thereby reducing risks to acceptable cost levels.
- Plan operational security procedures, ensure that operations security activities comply with policy, along with conducting periodic security reviews and audits.
- Support product and service development, integration and procurement activities ensuring that selected components, when deployed, will comply with the organization's detailed security requirements.

Course Outline

Module 1

Lecture 1 Why network security is needed, The different ways security is commonly discussed, Process of information security governance, The concept of defense in depth.

Lecture 2 – Foundation concepts: security services and controls Access control concepts, Asset inventory, classification concepts, vulnerabilities, threats and risks.

Module 2

Lecture 3 – Concept of encryption, Forms of symmetric and asymmetric encryption, cryptographically secure hash algorithms,

Lecture 4 – The need for encryption key management, key distribution approaches including Diffie-Hellman key negotiation, and Public Key Infrastructures.

Module 3

Lecture 5 - Role of Cryptography in Security to provide authentication, confidentiality and data integrity, Authentication Systems: Single Sign-on and XML, Kerberos and Shibboleth Based Authentication.

Lecture 6 – Traditional networking architectures, Types of networks (LANs, MANs, WANs), Network physical layer and data link layer attacks and defensive mechanisms available (IEEE 802.1ae, 802.1x).

Module 4

Lecture 7 – The Insecurity of ARP, IP and other network layer protocols covering vulnerabilities and protocol internal security mechanism. Network layer attacks and defensive mechanisms available (IP security, packet filtering firewalls).

Lecture 8 – Transport layer protocols, vulnerabilities, attacks and defensive mechanisms available (TLS-DTLS-SSL, SSH).

Module 5 –

Lecture 9 – Multi-protocols layer attacks and defensive mechanisms (Application gateway firewalls, Deep pack inspection, network flow monitoring, Honey Pots).

Lecture 10 – Cloud Security. Web and Electronic mail vulnerabilities, attacks and defensive mechanisms (digest authentication, TLS, PGP-GPG).

Module 6

Lecture 11 – Mobile Security, Peer-to-peer, Instant Messaging, Domain Name System, Network Time vulnerabilities, attacks and defensive mechanisms (Session Boarder Controls, DNS SEC, malware scanning).

Lecture 12 – Security in management protocols**,** Network Security management tools (Syslog and log management, vulnerability scanning, Security Event and Information Management, Penetration Testing), Network Operations Security (OpSec) and OpSec compliance.

Lecture 13 – Course review.

Non-required textbooks and references good for further study

The following books are **NOT** *required for this course. However you will find each to be valuable resources to anyone involved in the Information Security area.*

Bellovin, Addison-Wesley, 1994

This book is a classic for its very detailed treatment for statefull firewalls and DMZs and is still relevant today.

Practical UNIX & Internet Security, 2nd Edition, ,Simson Garfinkel and Gene Spafford: O'Reilly, 1996

This book is a classic for its very detailed treatment of general networking security and hardening of unix typs operating systems and is still relevant today.

Hacking Expose Network Security Secrets & Solutions, 2nd Edition, Joel Scambray, Stuart McClure, and George Kurtz, McGraw-Hill, 2001

This book provides an interesting look into those involved in malware and some of the techniques used for breaching targeted systems.

Security Engineering; A Guide to Building Dependable Distributed Systems, Ross Anderson, Wiley, 2001

This book is an interesting collection of discussions on security engineering and associated challenges.

Computer Related Risks, Peter G. Neumann, Addison-Wesley, 1995

This book is one of the definitive texts on the basic concepts of what constitutes risks, especially information security risks.

Applied Cryptography, Bruce Schneier, 2nd Edition, Wiley & Sons, 1996

This book is an excellent source for details on most any encryption algorithm you are likely to encounter. Most any version, starting with the 2nd edition, will be invaluable.

Computer Security, Dieter Gollmann, 2nd ed, John Wiley, 2006

This book provides depth coverage of computer security and is highly recommended.

Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance, Stuart Jacobs, IEEE Press Series on Information and Communication Networks Security, Wiley-IEEE Press; 1 edition, ISBN-10: 0470565128, ISBN-13: 978-0470565124

The above book covers the subject area of information security from an engineering perspective