Syllabus

This is a single, concatenated file, suitable for printing or saving as a PDF for offline viewing. Please note that some animations or images may not work.

Description

This module is also available as a concatenated page, suitable for printing or saving as a PDF for offline viewing.

MET CS690

Network Security

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 of 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.) and concluding with 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.

Technical Notes

The table of contents expands and contracts (+/- sign) and may conceal some pages. To avoid missing content pages, you are advised to use the next/previous page icons in the top right corner of the learning modules.

This course requires you to access files such as word documents, PDFs, and/or media files. These files may open in your browser or be downloaded as files, depending on the settings of your browser.

Learning Objectives

After completing the course, the student should be able to:

- Discuss what security is, why it is necessary, security concepts, objectives and services.
- Explain the process of information security management and related information security standards
- Describe symmetric and asymmetric cryptography, secure hashing algorithms and key management including public key infrastructures.
- Discuss the different cryptographic mechanisms used to provide authentication and data integrity;
- Describe the various network physical layer media types, the vulnerabilities of each media type, typical attacks targeting each media type and available defensive mechanisms;

- Describe the various network data link layer protocols in use, the vulnerabilities of each protocol, typical attacks targeting each protocol and available defensive mechanisms;
- Based on an understanding of relevant protocols, such as ARP, ICMP, TCP/IP, IPSec, describe attacks and defenses at network and transport layers on mobile, sensor and SCADA networks.
- Describe the concept of network information flow control and how packet filtering router-firewalls enforce network information flow control.
- Understand general application layer attacks and defenses including application gateways, deep packet Inspection, intrusion detection and protection systems
- Explain various web services attacks and defenses
- Discuss security for e-mail and various defenses including Pretty Good Privacy, GNU Privacy Guard and Secure / MIME
- Describe the various forms of malicious software including viruses, worms Trojan horses, root-kits spyware, phishing and spear phishing and how to protect systems from malware.
- Discuss the security aspects of messaging applications, peer-to-peer applications, VoIP, DHCP, DNS, NTP, SNMP
- Explain the technological network management resources of: Remote System Logging and Log Management; Network Vulnerability Scanning; Security Event and Information Management; and Penetration Testing.
- Describe the importance and use of operational security guidelines and procedures
- Describe the role that accreditation and certification play in network security

After completing each module, the student should be able to:

Module 1 – Security – Why, What, Management, Terminology and Concepts

- Discuss what is the meaning of security and why security is necessary;
- Describe the different ways security is commonly presented and discussed;
- Explain the process of information security management and related information security standards;
- Describe why the terms Trust and Privacy are confusing and are not useful technical terms;
- Explain the concept of Defense in Depth and it applies to information security;
- Understand how networks have evolved over time and likely to change in the future;
- Describe security concepts, security objectives and abstract security services;
- Explain the concept of asset inventorying, asset vulnerabilities, and threats to information technology assets.

Module 2 – Cryptography – Ciphers, Symmetric and Asymmetric Encryption, Hashing, Public Key infrastructure

- Describe the different forms of symmetric cryptography;
- Discuss cryptographically secure hash algorithms;
- Explain what asymmetric encryption is, how it works and the main asymmetric algorithms;
- Describe what encryption key management is and the functions covered by key management;
- Explain what the Diffie-Helman Key Negotiation protocol is and how to protect if from Man-in-the-Middle attacks;
- Describe what Public Key Infrastructures are, how they work and why they are necessary.

Module 3 – Using cryptography to provide secure services, attacks and defenses layers 1 and 2

- Discuss the different cryptographic mechanisms used to provide authentication and data integrity;
- Describe what the Extensible Authentication Protocol (EAP) is,its structure and the various methods available;

- Explain why factors are used to authenticate humans, the basis of each type of factor, the various problems encountered with each type of factor,and how to mitigate these problems;
- Describe what single sign on (SSO) systems are and the use of XML and SAML in SSOs;
- Explain what Kerberos and Shibboleth SSO systems are and how they operate;
- Describe the various network physical layer media types are, the vulnerabilities of each media type, typical attacks targeting each media type and available defensive mechanisms;
- Describe the various network data link layer protocols in use, the vulnerabilities of each protocol, typical attacks targeting each protocol and available defensive mechanisms;

Module 4 – Attacks and defenses at the network and transport layers

- Describe what the ARP protocol is and how it is used
- Explain ARP based attacks and how these attacks can be defended against;
- Understand and describe the concepts of connectionless networking and network address translation;
- Describe the networking protocols IPv4 and IPv6 and how these protocols are vulnerable to attacks;
- Explain what ICMP is and how ICMP can be used for attacks;
- Describe what IPsec is, IPsec's security capabilities, and deployment issues;
- Explain what Mobile IP is, how it works, and how to protect Mobile IP from attacks.
- Explain what Mobile Ad-hock networks are and how to protect them from attacks.
- Explain what Sensor and SCADA networks are and how to protect them from attacks.
- Describe the concept of network information flow control and how packet filtering router-firewalls enforce network information flow control.
- Explain what the transport protocols TCP, UDP, SCTP and OSPF are, the vulnerabilities within each of these protocols, and how to protect them from attacks.
- Describe what TLS and DTLA are, their security capabilities, and how they protect TCP and UTP communications;
- Describe what Secutre Shell is, its security capabilities, and how these capabilities protect network communications

Module 5 – General application layer attacks and defenses, network management resources

- Discuss Application Gateways and their role in network security;
- Describe how Deep Packet Inspection operates and its use in Intrusion Detection and Protection Systems;
- Explain what a Honey Port is and how it is able to detect intrusions;
- Describe what network flow monitoring is and its role in detecting intrusions;
- Explain various web services attacks and defenses;
- Discuss security for electronic mail and various defenses including Pretty Good Privacy, GNU Privacy Guard and Secure / MIME
- Describe the various forms of malicious software including viruses, worms Trojan horses, root-kits spyware, phishing and spear phishing and how to protect systems from malware.

Module 6 – Specific application layer attacks and defenses, network management resources

- After completing this module the student should be able to:
- Discuss the security impacts of Instant Messaging and Chat applications;
- Describe how Peer-to-Peer applications can cause security problems;
- Explain how Voice over Internet Protocol (VoIP) can be attacked and defended;

- Describe the security issues associated with the Dynamic Host Configuration Protocol;
- Explain security issues, attacks and defenses associated with the Domain Name System;
- Understand the security relevance of the Network Time Protocols;
- Describe the various network management protocols, how they can be attacked and defended;
- Explain the technological network management resources of: Remote System Logging and Log Management; Network Vulnerability Scanning; Security Event and Information Management; and Penetration Testing.
- Describe the importance and use of operational security guidelines and procedures;
- Explain what security event response and forensic investigations need to consider;
- Understand why operational reviews are important to network security;
- Describe the role that accreditation and certification play in network security;
- Explain why security lifecycle reviews are necessary for achieving network security;
- Describe how to achieve operational network security compliance.

Instructor

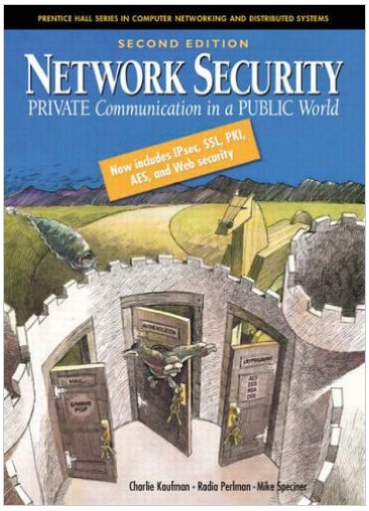
Michael Heister

Mike Heister worked in various roles in the telecommunications industry for the past 20 years. He began his career designing and building data networks for local businesses in his home town of Stillwater, Oklahoma before accepting a commission as a U.S. Army Signal officer. He spent the majority of his 5 years on active duty in Europe, with tours in both Kosovo and Iraq. Mike works as a U.S. Government contractor in both hands-on and Program Management designing and implementing strategic information security and global network infrastructure projects. He is currently a Program Manager responsible for implementation, operation, and maintenance of terrestrial data circuits in 43 countries in sub-Saharan Africa. He earned a Bachelor of Science in Computer systems from Oklahoma State University with minors in Military Science, and Economics in 1999, and completed his Master of Science in Computer Information Systems with a concentration in Security from Boston University Metropolitan College in 2014. Mike lives in Eldridge, Iowa with his wife, daughter, twin sons, and three dogs.

Computer Science Department
Metropolitan College
Boston University
+1-732-822-1670
mheister@bu.edu

Materials

Required Text



Network Security -- Private Communication in a Public World, Charlie Kaufman, Radia Perlman and Mike Speciner, 2nd Edition, Prentice-Hall, 2002, ISBN 0-13-046019-2

The e-Book version of this textbook can be purchased from Barnes and Noble at Boston University.

(Note while the publication date of this text is 2002, the content includes fundamental concepts and approaches that have stood the test of time.)

Boston University Library Information

Boston University has created a set of videos to help orient you to the online resources at your disposal. An introduction to the series is below:

met_ode_library_14_sp1_00_intro video cannot be displayed here

All of the videos in the series are available on the Online Library Resources page, which is also accessible from the Campus Bookmarks section of your Online Campus Dashboard. Please feel free to make use of them.

As Boston University students, you have full access to the BU Library. From any computer, you can gain access to anything at the library that is electronically formatted. To connect to the library, use the link http://www.bu.edu/library. You may use the library's content whether you are connected through your online course or not, by confirming your status as a BU community member using your Kerberos password.

Once in the library system, you can use the links under “Resources” and “Collections” to find databases, eJournals, and eBooks, as well as search the library by subject. Some other useful links follow:

> Go to http://www.bu.edu/library/research/collections to access eBooks and eJournals directly.
>
> If you have questions about library resources, go to http://www.bu.edu/library/help/ask-a-librarian to email the library or use the live-chat feature.

To locate course eReserves, go to http://www.bu.edu/library/services/reserves.

Please note that you are not to post attachments of the required or other readings in the water cooler or other areas of the course, as it is an infringement on copyright laws and department policy. All students have access to the library system and will need to develop research skills that include how to find articles through library systems and databases.

Free Tutoring Service

Free online tutoring with SMARTHINKING is available to BU online students for the duration of their courses. The tutors do not rewrite assignments, but instead teach students how to improve their skills in the following areas: writing, math, sciences, business, ESL, and Word/Excel/PowerPoint.

You can log in directly to SMARTHINKING from Online Campus by using the link in the left-hand navigation menu of your course.

YouTube

Please Note

SMARTHINKING may be used only for current Boston University online courses and career services. Use of this service for purposes other than current coursework or career services may result in deactivation of your SMARTHINKING account.

Study Guide

Access Assignments and Labs through the "Assignments" link in the left-hand course menu. Quizzes are located under "Assessments," and discussions under "Class Discussions." Each week, students are expected to create at least one new discussion thread, and respond to threads created by other students.

Module 1 Study Guide and Deliverables

Readings:

- Module 1, Lecture 1 Slides
- Module 1, Lecture 2 Slides
- Kaufman & Perlman Textbook: Chapter 1 Sections 1.3 Terminology *through* 1.14 legal Issues
- Example Company Security Policy - Extract
- Network Overview and Review
- Symantec Internet Security Report 23 April 2018

Discussions:

- Discussion 1 postings end May 15 at 6:00 AM ET

Assignments:

- Assignment 1 due May 15 at 6:00 AM ET

Assessments:

- Quiz 1 due May 15 at 6:00 AM ET

Live Classroom:

- Friday, May 11 at 7:30 PM ET

Module 2 Study Guide and Deliverables

Readings:

- Module 2, Lecture 3 Slides
- Module 2, Lecture 4 Slides

Kaufman & Perlman Textbook:

- Chapter 2 sections 2.1 What is Cryptography *through* 2.6 Hash Algorithms
- Chapter 3 sections 3.1 Introduction *through* 3.3.1 DES Overview; 3.4 International Data Encryption Algorithm (IDEA) *through* 3.4.1 Primitive Operations; 3.5 Advanced Encryption Standard (AES); 3.6 RC4
- Chapter 4 sections 4.1 Introduction *through* 4.4.1.3 Triple Encryption with only Two Keys
- Chapter 6 sections 6.1 Introduction *through* 6.3.3 Why is RSA Secure; 6.3.6 Public-Key Cryptography Standard (PKCS); 6.4 Diffie-Hellman *through*

6.4.2 Defenses Against Man-in-the-Middle Attack; 6.4.5 Diffie-Hellman Details – Safe Primes; 6.5 Digital Signature Standard (DSS) *through* 6.7 Elliptic Cure Cryptography (ECC)

- Chapter 9 sections 9.7.2 Certificate Authorities (CAs) *through* 9.7.4.2 Multiple CA Domains
- Chapter 15 sections 15.1 Introduction *through* 15.7 X.509 and PKIX Certificates
- Chapter 26 sections 26.1 Perfect Forward Secrecy *through* 26.2 Change Keys Periodically; 26.4 Use Different Keys in the Two Directions *through* 26.24 Put Checksums at the End of Data

Discussions:

- Discussion 2 postings end May 22 at 6:00 AM ET

Assignments:

- Assignment 2 due May 22 at 6:00 AM ET

Assessments:

- Quiz 2 due May 22 at 6:00 AM ET

Live Classroom:

- Friday, May 18 at 7:30 PM ET

Module 3 Study Guide and Deliverables

Readings:

- Module 3, Lecture 5 Slides
- Module 3, Lecture 6 Slides

Kaufman & Perlman Textbook:

- Chapter 5 sections 5.1 Introduction *through* 5.2 Nifty Things to Do with a Hash; 5.2.1 Authentication *through* 5.2.4.1 Hashing Large Messages; 5.5 MD5; 5.6 SHA-1 *through* 5.6.1 SHA-1 Message Padding; 5.7 HMAC
- Chapter 9 sections; 9.1 Password-Based Authentication *through* 9.7.1 KDCs

- Chapter 10 sections 10.1 Introduction *through* 10.10 Biometrics
- Chapter 11 sections 11.1 Login *through* 11.8 Authentication Protocol Checklist
- Chapter 13 sections 13.1 Introduction *through* 13.6 Realms
- Chapter 16 sections 16.1 What Layer *through* 16.5 Denial-of-Service/Clogging Protection; 16.12 Negotiating Crypto Parameters

Discussions:
- Discussion 3 postings end May 29 at 6:00 AM ET

Assignments:
- Assignment 3 due May 29 at 6:00 AM ET
- Lab 1 due May 29 at 6:00 AM ET

Assessments:
- Quiz 3 due May 29 at 6:00 AM ET

Live Classroom:
- Friday, May 25 at 7:30 PM ET

Module 4 Study Guide and Deliverables

Readings:
- Module 4, Lecture 7 Slides
- Module 4, Lecture 8 Slides

Kaufman & Perlman Textbook:

- Chapter 17 sections 17.1 Overview of IPsec *through* 17.6 Comparison of Encodings
- Chapter 18 sections 18.1 Proturis *through* 18.6 Phase 2 IKE: Setting up IPsec SAs
- Chapter 23 sections 23.1 Packet Filters *through* 23.7 Should Firewalls Go Away

Discussions:
- Discussion 4 postings end June 5 at 6:00 AM ET

Assignments:
- Assignment 4 due June 5 at 6:00 AM ET
- Lab 2 due June 5 at 6:00 AM ET

Assessments:	• Quiz 4 due June 5 at 6:00 AM ET
Live Classroom:	• Friday, June 1 at 7:30 PM ET

Module 5 Study Guide and Deliverables

Readings:	• Module 5, Lecture 9 Slides • Module 5, Lecture 10 Slides Kaufman & Perlman Textbook • Chapter 20 sections 20.1 Distribution Lists *through* 20.6 Authentication of the Source • Chapter 22 sections 22.1 Introduction *through* 22.9 Anomalies • Chapter 25 sections 25.1 Introduction *through* 25.6.6 Other Misuse of Cookie • A Review of Anomaly based Intrusion Detection Systems.pdf • Limitations of Network Intrusion Detection.pdf • Honeypot in Network Security- A Survey.pdf • An Overview of IP Flow-Based Intrusion Detection.pdf
Discussions:	• Discussion 5 postings end June 12 at 6:00 AM ET
Assignments:	• Assignment 5 due June 12 at 6:00 AM ET
Assessments:	• Quiz 5 due June 12 at 6:00 AM ET
Live Classroom:	• Friday, June 8 at 7:30 PM ET

Module 6 Study Guide and Deliverables

Readings:	• Module 6, Lecture 11 Slides

	• Module 6, Lecture 12 Slides • Module 6, Lecture 13 Slides • The design and implement of the centralized log gathering and analysis system.pdf • Log management comprehensive architecture in Security Operation Center.pdf • Technical Guide to Information Security Testing and Assessment.pdf
Discussions:	• Discussion 6 postings end June 19 at 6:00 AM ET
Assignments:	• Assignment 6 due June 19 at 6:00 AM ET • Lab 3 due June 19 at 6:00 AM ET
Assessments:	• Quiz 6 due June 19 at 6:00 AM ET
Live Classroom:	• Friday, June 15 at 7:30 PM ET

Final Exam Details

The Final Exam is a proctored exam available from **June 20 at 6:00 AM ET to June 23 at 11:59 PM ET**. The Computer Science department requires that all final exams be proctored.

The exam is a three-hour open-book/open-notes exam consisting of multiple choice and multiple answer questions. It will only be accessible during the final exam period. You can access it from either the Assessments section of the course or from the Final Exam module on the home page. Your proctor will enter the password to start the exam.

You will receive a technical support hotline number before the start of the exam. Please bring this number with you to the exam.

Grading Information

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.

Courseware

This course uses Online Campus (Blackboard). Once the course starts all students must use the Online Campus Dashboard internal messages service. Online campus should be used for:

- Reading assignments beyond text book 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, and
- All course related email correspondence.

On-line Live Sessions

There will be a weekly hour on-line session conducted by your Instructor.

During these on-line sessions the Instructor will present and clarify material from the week's readings, as well as answer students' questions. Attendance is not required at these sessions but highly recommended. All on-line sessions will be recorded and archived. The archived recordings will be accessible from the Online Campus Dashboard under the heading "Live Classroom (Question & Answer) Sessions".

Your group Facilitator may also schedule on-line sessions once the course starts.

Assignments

- All homework assignments are identified within the Online campus Study Guide.
- File names for assignment documents should be:

  CS690-HW‹number›-‹student last name›.doc

  An example assignment document file name is:

  CS690-HW5-Heister.doc
- 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.
- Include the file name in the header and a page number in the footer of your assignment submission document.
- Title cover pages are not required and should not be used;

- Assignment submission documents MUST be in MS Word 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.
- Failure to site the works of others used in your submission is considered plagiarism and violates the BU Academic Conduct Policy.
- 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-Jacobs.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;
- Students can use any word processing application they want PROVIDED their submission is directly compatible Microsoft Word. Submissions should NOT be encoded in XML.

Discussion Threads

- Each course module includes a discussion topic that students are required to participate in.
- Students are expected to participate in each module discussion activity which requires the student to make one or two primary and multiple follow- up posts to other students' primary posts. A primary post is one where the student introduces a new thread topic. A follow-up post is one which replies to another student's primary post
- Each posting should be original and add value to the discussion.
- The quality of each post is far more important than the quantity of posts.

  Facilitators will use the following table to assign a subjective grade to each student discussion post

Criteria	Subjective Grade for either Primary or Follow-up Discussion Post				
	Poor	**Fair**	**Good**	**Very Good**	**Excellent**
Participation	Very limited participation	Participation generally lacks frequency or relevance	Reasonably useful relevant participation during the discussion period	Frequently relevant and consistent participation throughout the discussion period	Continually relevant and consistent participation throughout the discussion period
Community	Mostly indifferent to discussion	Little effort to keep discussions going or provide help	Reasonable effort to respond thoughtfully, provide help, and/or keep discussions going	Often responds thoughtfully in a way frequently keeps discussions going and provides help	Continually responds thoughtfully in a way that consistently keeps discussions

					going and provides help
Content	No useful, on-topic, or interesting information, ideas or analysis	Hardly any useful, on-topic, or interesting information, ideas or analysis	Reasonably useful, on-topic, and interesting information, ideas and/or analysis	Frequently useful, on-topic, and interesting information, ideas and analysis	Exceptionally useful, on-topic, and interesting information, ideas and analysis
Reflection and Synthesis			No significant effort to clarify, summarize or synthesize topics raised in discussions	Contributes to group's effort to clarify, summarize or synthesize topics raised in discussions	Leads group's effort to clarify, summarize or synthesize topics raised in discussions

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 starting when a quiz becomes available via Online Campus. Each quiz will close at 6 AM ET on the date the next Module starts and not be reopened except for unusual circumstances as decided by the instructor. 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.

Grading Criteria

Grades will be based on:

- Homework assignments (25%)
- Quizzes (25%)
- Lab exercises (10%)
- Discussion thread 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

The instructor reserves the right to make minor adjustments to these grade ranges.

Academic Conduct Policy

Please visit Metropolitan College's website for the full text of the department's *Academic Conduct Code*.

A Definition of Plagiarism

"The academic counterpart of the bank embezzler and of the manufacturer who mislabels products is the plagiarist: the student or scholar who leads readers to believe that what they are reading is the original work of the writer when it is not. If it could be assumed that the distinction between plagiarism and honest use of sources is perfectly clear in everyone's mind, there would be no need for the explanation that follows; merely the warning with which this definition concludes would be enough. But it is apparent that sometimes people of goodwill draw the suspicion of guilt upon themselves (and, indeed, are guilty) simply because they are not aware of the illegitimacy of certain kinds of "borrowing" and of the procedures for correct identification of materials other than those gained through independent research and reflection."

"The spectrum is a wide one. At one end there is a word-for-word copying of another's writing without enclosing the copied passage in quotation marks and identifying it in a footnote, both of which are necessary. (This includes, of course, the copying of all or any part of another student's paper.) It hardly seems possible that anyone of college age or more could do that without clear intent to deceive. At the other end there is the almost casual slipping in of a particularly apt term which one has come across in reading and which so aptly expresses one's opinion that one is tempted to make it personal property."

"Between these poles there are degrees and degrees, but they may be roughly placed in two groups. Close to outright and blatant deceit-but more the result, perhaps, of laziness than of bad intent-is the patching together of random jottings made in the course of reading, generally without careful identification of their source, and then woven into the text, so that the result is a mosaic of other people's ideas and words, the writer's sole contribution being the cement to hold the pieces together. Indicative of more effort and, for that reason, somewhat closer to honest, though still dishonest, is the paraphrase, and abbreviated (and often skillfully prepared) restatement of someone else's analysis or conclusion, without acknowledgment that another person's text has been the basis for the recapitulation."

The paragraphs above are from H. Martin and R. Ohmann, *The Logic and Rhetoric of Exposition, Revised Edition.* Copyright 1963, Holt, Rinehart and Winston.

Academic Conduct Code

I. **Philosophy of Discipline**
The objective of Boston University in enforcing academic rules is to promote a community atmosphere in which learning can best take place. Such an atmosphere can be maintained only so long as every student believes that his or her academic competence is being judged fairly and that he or she will not be put at a disadvantage because of someone else's dishonesty. Penalties should be carefully determined so as to be no more and no less than required to maintain the desired atmosphere. In defining violations of this code, the intent is to protect the integrity of the educational process.

II. **Academic Misconduct**
Academic misconduct is conduct by which a student misrepresents his or her academic accomplishments, or impedes other students' opportunities of being judged fairly for their academic work. Knowingly allowing others to represent your work as their own is as serious an offense as submitting another's work as your own.

III. **Violations of this Code**

Violations of this code comprise attempts to be dishonest or deceptive in the performance of academic work in or out of the classroom, alterations of academic records, alterations of official data on paper or electronic resumes, or unauthorized collaboration with another student or students. Violations include, but are not limited to:

A. **Cheating on examination**. Any attempt by a student to alter his or her performance on an examination in violation of that examination's stated or commonly understood ground rules.
B. **Plagiarism.** Representing the work of another as one's own. Plagiarism includes but is not limited to the following: copying the answers of another student on an examination, copying or restating the work or ideas of another person or persons in any oral or written work (printed or electronic) without citing the appropriate source, and collaborating with someone else in an academic endeavor without acknowledging his or her contribution. Plagiarism can consist of acts of commission-appropriating the words or ideas of another-or omission failing to acknowledge/document/credit the source or creator of words or ideas (see below for a detailed definition of plagiarism). It also includes colluding with someone else in an academic endeavor without acknowledging his or her contribution, using audio or video footage that comes from another source (including work done by another student) without permission and acknowledgement of that source.
C. **Misrepresentation or falsification of data** presented for surveys, experiments, reports, etc., which includes but is not limited to: citing authors that do not exist; citing interviews that never took place, or field work that was not completed.
D. **Theft of an examination**. Stealing or otherwise discovering and/or making known to others the contents of an examination that has not yet been administered.
E. **Unauthorized communication during examinations**. Any unauthorized communication may be considered prima facie evidence of cheating.
F. **Knowingly allowing another student to represent your work as his or her own**. This includes providing a copy of your paper or laboratory report to another student without the explicit permission of the instructor(s).
G. **Forgery, alteration, or knowing misuse of graded examinations, quizzes, grade lists, or official records of documents**, including but not limited to transcripts from any institution, letters of recommendation, degree certificates, examinations, quizzes, or other work after submission.
H. **Theft or destruction of examinations or papers** after submission.
I. **Submitting the same work in more than one course** without the consent of instructors.
J. **Altering or destroying another student's work or records**, altering records of any kind, removing materials from libraries or offices without consent, or in any way interfering with the work of others so as to impede their academic performance.
K. **Violation of the rules governing teamwork**. Unless the instructor of a course otherwise specifically provides instructions to the contrary, the following rules apply to teamwork: 1. No team member shall intentionally restrict or inhibit another team member's access to team meetings, team work-in-progress, or other team activities without the express authorization of the instructor. 2. All team members shall be held responsible for the content of all teamwork submitted for evaluation as if each team member had individually submitted the entire work product of their team as their own work.
L. **Failure to sit in a specifically assigned seat during examinations.**
M. **Conduct in a professional field assignment that violates the policies and regulations of the host school or agency.**
N. **Conduct in violation of public law occurring outside the University that directly affects the academic and professional status of the student, after civil authorities have imposed sanctions.**
O. **Attempting improperly to influence the award of any credit, grade, or honor.**
P. **Intentionally making false statements to the Academic Conduct Committee or intentionally presenting false information to the Committee.**
Q. **Failure to comply with the sanctions imposed under the authority of this code.**

Important Message on Final Exams

Dear Boston University Computer Science Online Student,

As part of our ongoing efforts to maintain the high academic standard of all Boston University programs, including our online MSCIS degree program, the Computer Science Department at Boston University's Metropolitan College requires that each of the online courses includes a proctored final examination.

By requiring proctored finals, we are ensuring the excellence and fairness of our program. The final exam is administered online, and the access will be available at the exam sites.

Specific information regarding final-exam scheduling will be provided approximately two weeks into the course. This early notification is being given so that you will have enough time to plan for where you will take the final exam.

I know that you recognize the value of your Boston University degree and that you will support the efforts of the University to maintain the highest standards in our online degree program.

Thank you very much for your support with this important issue.

Regards,

Professor Lou Chitkushev, Ph.D.
Associate Dean for Academic Affairs
Boston University Metropolitan College

Who’s Who: Roles and Responsibilities

You will meet many BU people in this course and program. Some of these people you will meet online, and some you will communicate with by email and telephone. There are many people behind the scenes, too, including instructional designers, faculty who assist with course preparation, and video and animation specialists.

People in Your Online Course in Addition to Your Fellow Students

Your Facilitator. Our classes are divided into small groups, and each group has its own facilitator. We carefully select and train our facilitators for their expertise in the subject matter and their excellence in teaching. Your facilitator is responsible for stimulating discussions in pedagogically useful areas, for answering your questions, and for grading homework assignments, discussions, term projects, and any manually graded quiz or final-exam questions. If you ask your facilitator a question by email, you should get a response within 24 hours, and usually faster. If you need a question answered urgently, post your question to one of the urgent help topics, where everyone can see it and answer it.

Your Professor. The professor for your course has primary responsibility for the course. If you have any questions that your facilitator doesn't answer quickly and to your satisfaction, then send your professor an email in the course, with a cc to your facilitator so that your facilitator is aware of your question and your professor's response.

Your Senior Faculty and Student Support Administrator, Jennifer Sullivan. Jen is here to ensure you have a positive online experience. You will receive emails and announcements from Jen throughout the semester. Jen represents Boston University's university services and works for the Office of Distance Education. She prepares students for milestones such as course launch, final exams, and course evaluations. She is a resource to both students and faculty. For example, Jen can direct your university questions and concerns to the appropriate party. She also handles general questions regarding Online Campus functionality for students, faculty, and facilitators, but she does not provide tech support. She is enrolled in all classes and can be contacted within

the course through Online Campus email as it is running. You can also contact her by external email at jensul@bu.edu or call toll free at 1-888-524-2200.

People Not in Your Online Course

Although you will not normally encounter the following people in your online course, they are central to the program. You may receive emails or phone calls from them, and you should feel free to contact them.

Your Computer Science Department Online Program Coordinator, Peter Mirza. Peter administers the academic aspects of the program, including admissions and registration. You can ask him questions about the program, registration, course offerings, graduation, or any other program-related topic. He can be reached at metcsol@bu.edu or (617) 353-2566.

Your Computer Science Department Program Manager, Kim Richards. Kim is responsible for administering most aspects of the Computer Science Department. You can reach Kim at kimrich@bu.edu or (617) 353-2566.

Andrew Gorlin, Academic Advisor. Reviews requests for transfer credits and waivers. Advises students on which courses to take to meet their career goals .You can reach Andrew at asgorlin@bu.edu, or (617)-353-2566.

Professor Anatoly Temkin, Computer Science Department Chairman. You can reach Professor Temkin at temkin@bu.edu or at 617-353-2566.

Professor Lou T. Chitkushev, Associate Dean for Academic Affairs, Metropolitan College. Dr. Chitkushev is responsible for the academic programs of Metropolitan College. Contact Professor Chitkushev with any issues that you feel have not been addressed adequately. The customary issue-escalation sequence after your course facilitator and course faculty is Professor Temkin, and then Professor Chitkushev.

Professor Tanya Zlateva, Metropolitan College Dean Dr. Zlateva is responsible for the quality of all the academic programs at Boston University Metropolitan College.

Disability Services

In accordance with University policy, every effort will be made to accommodate unique and special needs of students with respect to speech, hearing, vision, or other disabilities. Any student who feels he or she may need an accommodation for a documented disability should contact the Office of Disability Services at (617) 353-3658 or at access@bu.edu for review and approval of accommodation requests.

Netiquette

The Office of Distance Education has produced a netiquette guide to help you understand the potential impact of your communication style.

Before posting to any discussion forum, sending email, or participating in any course or public area, please consider the following:

Ask Yourself…

- How would I say this in a face-to-face classroom or if writing for a newspaper, public blog, or wiki?
- How would I feel if I were the reader?
- How might my comment impact others?
- Am I being respectful?
- Is this the appropriate area or forum to post what I have to say?

Writing

When you are writing, please follow these rules:

- **Stay polite and positive in your communications**. You can and should disagree and participate in discussions with vigor; however, when able, be constructive with your comments.
- **Proofread your comments before you post them.** Remember that your comments are permanent.
- **Pay attention to your tone.** Without the benefit of facial expressions and body language your intended tone or the meaning of the message can be misconstrued.
- **Be thoughtful and remember that classmates' experience levels may vary.** You may want to include background information that is not obvious to all readers.
- **Stay on message.** When adding to existing messages, try to maintain the theme of the comments previously posted. If you want to change the topic, simply start another thread rather than disrupt the current conversation.
- **When appropriate, cite sources.** When referencing the work or opinions of others, make sure to use correct citations.

Reading

When you are reading your peers' communication, consider the following:

- **Respect people's privacy.** Don't assume that information shared with you is public; your peers may not want personal information shared. Please check with them before sharing their information.
- **Be forgiving of other students' and instructors' mistakes.** There are many reasons for typos and misinterpretations. Be gracious and forgive other's mistakes or privately point them out politely.
- **If a comment upsets or offends you, reread it and/or take some time before responding.**

> #### Important Note
>
> Don't hesitate to let your instructor or your faculty and student support administrator know if you feel others are inappropriately commenting in any forum.

All Boston University students are required to follow academic and behavioral conduct codes. Failure to comply with these conduct codes may result in disciplinary action.

Registration Information and Important Dates

> View the drop dates for your course.
>
> Withdraw or drop your course.
>
> - If you are dropping down to zero credits for a semester, please contact your college or academic department.

- **Nonparticipation in your online course does not constitute a withdrawal from the class.**
- If you are unable to drop yourself on student link please contact your college or academic department.

Technical Support

Experiencing issues with BU websites or Blackboard?

It may be a system-wide problem. Check the BU Information Services & Technology (IS&T) news page for announcements.

Boston University technical support is available via email (ithelp@bu.edu), the support form, and phone (888-243-4596). Please note that the IT Help Center has multiple locations. All locations can be reached through the previously mentioned methods. For IT Help Center hours of operation please visit their contact page. For other times, you may still submit a support request via email, phone, or the support form, but your question won't receive a response until the following day. If you aren't calling, it is highly recommended that you submit your support request via the technical-support form as this provides the IS&T Help Center with the best information in order to resolve your issue as quickly as possible.

Examples of issues you might want to request support for include the following:

- Problems viewing or listening to sound or video files
- Problems accessing internal messages
- Problems viewing or posting comments
- Problems attaching or uploading files for assignments or discussions
- Problems accessing or submitting an assessment

To ensure the fastest possible response, please fill out the online form using the link below:

IT Help Center Support
888-243-4596 or 617-353-4357 or Web
Check your open tickets using BU's ticketing system.

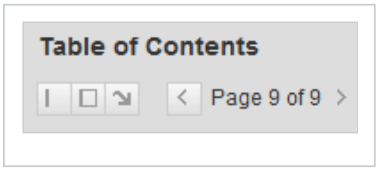
Navigating Courses

For best results when navigating courses, it is recommended that you use the Mozilla Firefox browser.

The Table of Contents may contain folders. These folders open and close (+ and − signs) and may conceal some pages. To avoid missing content pages, you are advised to use the next- and previous-page buttons (and icons) in the top-right corner of the learning content.

Please also familiarize yourself with the navigation tools, as shown below; these allow you to show and hide both the Course Menu and the Table of Contents on the left. This will be helpful for freeing up screen space when moving through the weekly lecture materials.

Navigation tools for the Table of Contents are shown in the image below:



Clicking on the space between the Course Menu and the Table of Contents allows you to show or hide the Course Menu on the left:

Web Resources/Browser Plug-Ins

To view certain media elements in this course, you will need to have several browser plug-in applications installed on your computer. See the Course Resources page in the syllabus of each individual course for other specific software requirements.

- Check your computer's compatibility by reviewing Blackboard's System Requirements
- Check your browser settings with Blackboard's Connection Test
- Download most recent version of Adobe Flash Player
- Download most recent version of Adobe Acrobat Reader

How to Clear Your Browser Cache

The IT Help Center recommends that you periodically clear your browser cache to ensure that you are viewing the most current content, particularly after course or system updates.

This page is also found within the "How to…" section of the online documentation, which contains a list of some of the most common tasks in Blackboard Learn.

Boston University Metropolitan College