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.

Course Description

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

MET CS695

Enterprise Cyber Security

This course introduces fundamental concepts, principles of cybersecurity and their use in the development of security mechanisms and policies. Topics include basic risk assessment and management; basic legal and ethics issues, various cyber attacks, defense methods and tools; security principles, models and components; different crypto protocols, techniques and tools, including symmetric and asymmetric encryption algorithms, hashing, public key infrastructure, and how they can be used; security threats and defense to hardware, operating systems, networks and applications in modern computing environments. Hands-on labs using current tools are provided and required.

Prerequisites

MET CS 535 or MET CS 625, or with in advance permission of the instructor.

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.

Course Learning Objectives

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

- Explain the fundamental concepts of the cyber security discipline.
- Describe basic risk assessment and management.
- Describe basic elements of a cryptographic system, and how crypto can be used.
- Identify strengths and weaknesses, modes, implementation issues and applications of different crypto protocols, techniques and tools including symmetric and asymmetric algorithms, encryption and hashing, PKI, etc.
- Identify potential cyber attacks, as well as cyber defense tools, methods and components to repel attacks.
- Describe appropriate measures to be taken should a system compromise occur.
- Properly use the vocabulary associated with cyber security
- Explain principles of cybersecurity and how they should be applied in the development of security mechanisms and policies
- Describe the security implications of various components in a computer system such as, hardware, OS, applications, network, and the user.
- Describe the security implications of the emerging technologies such as mobile and IoT.

Course Outline

Module 1: Introduction to Cybersecurity

- Basic concepts and terminology in cybersecurity
    - Motivation to study cybersecurity, real world examples of cyberattacks.
    - Branches of cybersecurity
    - Basic concepts: CIA, vulnerability, threat, risk, attack, compromise, control
- Legal issues and ethics,
- Risk analysis and security management

Module 2: Attacks and Defense

- Malware: virus, worms, trojan horse, rootkit, zombie, bot, botnet, ransomware,
- Bug: buffer overflow, integer overflow, TOCTTOU, covert channel
- Security model: threat model, trust model, trusted computing base
- Security principles and countermeasures

Module 3: Introduction to Crypto

- The role and property of crypto
- Terminology: Alice, Bob, Eve, encrypt, decrypt, cryptography, cryptanalysis
- Classical encryption: Caesar Cipher, ROTx, substitution cipher
- Symmetric encryption: DES, AES
- Key negotiation: DH
- Asymmetric encryption: RSA
- Hash: MD, MAC, HMAC
- Data authenticity and confidentiality

Module 4: Authentication and Authorization

- Something you know, you are, and you have: password, biometrics, token.
- Digital signature and Kerberos
- Digital certificate and PKI
- Access policy, access control matrix, access control list, capability, RBAC

Module 5: Network Security and Web Security

- Threats to network: data interception, replay attack, port scanning, DoS, DDoS, MITM
- Network defense: IPsec, VPN, Firewalls
- Browser attacks, email attacks, misleading/malicious web content

Module 6: Cyber System Security

- Hardware security: meltdown, spectre, TEE.
- Virtualization and Cloud computing security
- Mobile security and IoT security

Module 7 - Prepare for and take the final exam

- You will prepare for and take the proctored final exam.

The course will remain open two weeks after the final exam, so that you can continue discussions and ask any questions about database technology, your grades or the course. This is also a time when we enter into a dialog where we endeavor to learn from you how we can modify the course so that it better meets your needs.

Instructor

Charles Pak, Ph.D.

Computer Science Department
Metropolitan College
Boston University

Email: cpak4@bu.edu

Charles Pak earned his Ph.D. in Information Security from Nova Southeastern University, an M.S. in Network Security from Capitol Technology University, and a B.S. in Electrical Engineering from Penn State University. He has taught Information Systems (IS) courses for over 25 years as an IS practitioner and professor. He has managed U.S. Federal Government data centers for over 20 years, including personnel. He has designed, tested, implemented, and maintained many of these enterprise network sites (largest in the world) that encompasses distributed sites across the U.S. as well as the international sites. He has managed state-of-the art systems for military and federal government missions for which he was deployed.

His research topics include Cyber Security, Critical Infrastructure Protection (CIP), PKI, Cyber Counter Terrorism, and Risk Assessment & Management. He has published several research papers in Information Security. As a practitioner, he holds several industry certifications: CISM, CRISC, CISSP, ITIL, SSCP, MCSE, MCT, and CCNA.

Recent Publications:

- Pak, C. (2011). Near Real-time Risk Assessment Using Hidden Markov Models. Nova Southeastern University, ProQuest Dissertations and Theses,ISBN:9781124992945.
- Pak, C. & Cannady, J. (2010). Risk Forecast Using Hidden Markov Models. Research in Information Technology (RIT), ACM, SIGITE, 7(2), 4-15.
- Pak, C. & Cannady, J. (2009). Asset Priority Risk Assessment Using Hidden Markov Models. Proceedings of the 10th ACM SIGITE, Fairfax, Virginia, 2009, 65-73.
- Pak, C. (2008). The near real time statistical asset priority driven (nrtsapd) risk assessment. Proceedings of the 9th ACM SIGITE, Cincinnati, Ohio, 2008, 105-112.

Course Developers

Yuting Zhang, Ph.D

Assistant Professor, Computer Science; Coordinator, Information Security
Metropolitan College
Boston University

PhD, Boston University MS, BS, University of Science and Technology Beijing

Email: danazh@bu.edu

Dr. Zhang's research mainly focuses on resource management in soft real-time systems, virtual machine systems, and internet end-systems, though her interest spreads to all areas of computer systems and networks. Conducted through both theoretic analysis and empirical evaluation, her research has been published in more than a dozen conference proceedings and journals. Zhang served as an assistant professor at Merrimack College, the Wentworth Institute of Technology, Allegheny College, and the University of Science and Technology Beijing. She has taught a variety of courses, including information technology, Java/C++/C programming, operating systems, computer networks, analysis of algorithms, software engineering, programming languages, and a research seminar.

Shengzhi Zhang, Ph.D.

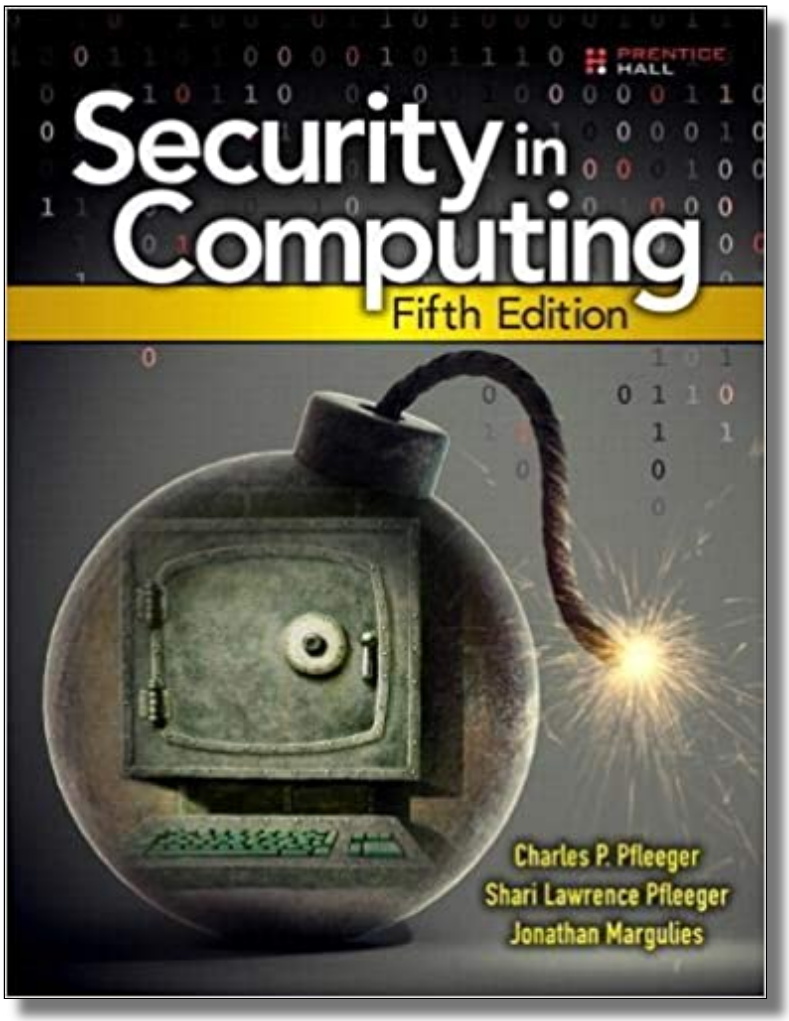
Computer Science Department
Metropolitan College
Boston University

Email: shengzhi@bu.edu

Dr. Shengzhi Zhang earned his PhD in Computer Science and Engineering from Penn State University in 2012. His research focuses on cybersecurity, including but not limited to Internet of Things (IoT) security, automobile security, mobile security, and operating system security, among others. He has most recently worked as an assistant professor in the Department of Computer Science at the Florida Institute of Technology. Prior to academia, Dr. Zhang conducted various research projects in Cisco, IBM, and Honeywell Aerospace labs. His existing partnerships, both nationally and internationally, include researchers from Ford Motor, IBM, GE, Indiana University, Penn State, Kuwait University, and the Chinese Academy of Sciences. Dr. Zhang has published many papers and served as program committee members in top-tier security conferences and journals.

Course Materials

Required Book



Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in Computing (5th ed.). Pearson/Prentice Hall.

ISBN 9780134085043.

Physical copies of the textbook are sold at Barnes and Noble at Boston University. An e-book is available at Vitalsource.com. An e-book is available through Amazon. An e-book is available through the BU bookstore.

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.

Journals & conferences/proceedings in Information Security

- Computer Security Update
- European Conference on Information Warfare and Security
- IEEE Transactions on Dependable and Secure Computing
- Information Security Journal
- Information Security Management Principles
- Inside Cybersecurity
- International Conference on Information Warfare and Security
- International Journal of Computer Science and Information Security
- International Journal of Information Security
- Journal of Information Privacy & Security
- SC Magazine

Portals

- ACM Digital Library
- Proceedings of the IEEE

Additional links for searching

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 Collections to access eBooks and eJournals directly.

If you have questions about library resources, go to Ask a Librarian: Help & FAQs to email the library or use the live-chat feature.

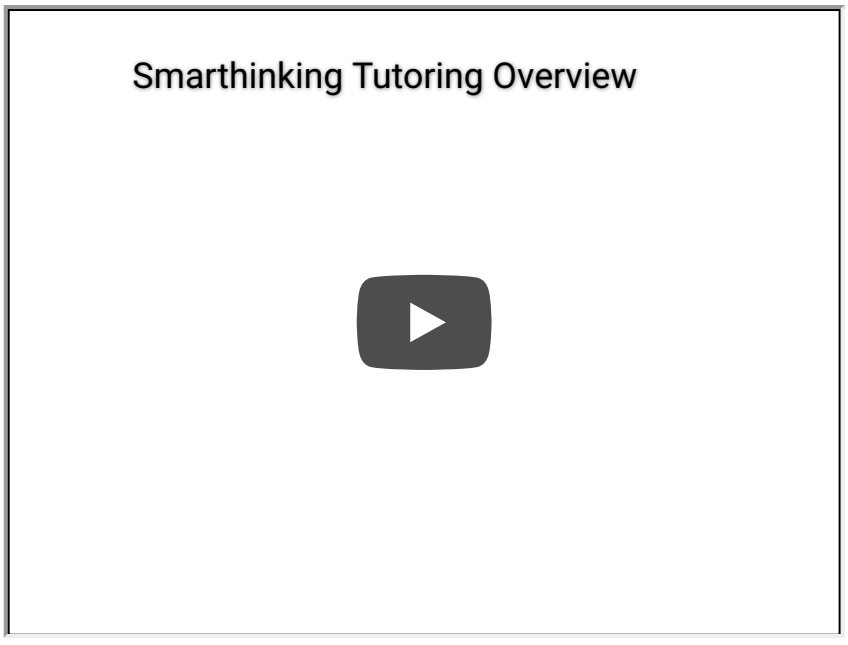
To locate course eReserves, go to Reserves.

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.



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

This course starts on a **Thursday**. The modules in this course run from **Thursday to Wednesday**.

Module 1 Study Guide and Deliverables

Theme:	Introduction to Cybersecurity

Topics:	• Basic concepts and terminology in cybersecurity
	  ◦ Motivation to study cybersecurity, real world examples of cyberattacks.
	  ◦ Branches of cybersecurity
	  ◦ Basic concepts: CIA, vulnerability, threat, risk, attack, compromise, control
	• Legal issues and ethics,
	• Risk analysis and security management

Readings:	• Chapter 1, Chapter 10, and Chapter 11
Assignments:	• Lab 1 due **Thursday, January 20 at 6:00 AM ET**
Assessments:	• Quiz 1 due **Thursday, January 20 at 6:00 AM ET**
Discussions:	• Discussion 1 posts due **Thursday, January 20 at 6:00 AM ET**. Any posts after the due time will not be included in the grading process.
Live Classroom:	• Lecture: **Thursday, January 13 from 7:00-8:30 PM ET** • Office hour: **Saturday, January 15 from 8:00-9:00 PM ET**

Module 2 Study Guide and Deliverables

Theme:	Attacks and Defense
Topics:	• Malware: virus, worms, trojan horse, rootkit, zombie, bot, botnet, ransomware, • Bug: buffer overflow, integer overflow, TOCTTOU, covert channel • Security model: threat model, trust model, trusted computing base • Security principles and countermeasures
Readings:	• Chapter 3
Assignments:	• Assignment 1 and Lab 2 due **Thursday, January 27 at 6:00 AM ET**
Assessments:	• Quiz 2 due **Thursday, January 27 at 6:00 AM ET**
Discussions:	• None
Live Classroom:	• Lecture: **Thursday, January 20 from 7:00-8:30 PM ET** • Office hour: **Saturday, January 22 from 8:00-9:00 PM ET**

Module 3 Study Guide and Deliverables

Theme:	Introduction to Crypto
Topics:	• The role and property of crypto • Terminology: Alice, Bob, Eve, encrypt, decrypt, cryptography, cryptanalysis • Classical encryption: Caesar Cipher, ROTx, substitution cipher • Symmetric encryption: DES, AES • Key negotiation: DH • Asymmetric encryption: RSA • Hash: MD, MAC, HMAC • Data authenticity and confidentiality
Readings:	• Chapter 2.3
Assignments:	• Lab 3 due **Thursday, February 3 at 6:00 AM ET**
Assessments:	• Quiz 3 due **Thursday, February 3 at 6:00 AM ET**
Discussions:	• None
Live Classroom:	• Lecture: **Thursday, January 27 from 7:00-8:30 PM ET** • Office hour: S**aturday, January 29 from 8:00-9:00 PM ET**

Module 4 Study Guide and Deliverables

Theme:	Authentication and Authorization
Topics:	• Something you know, you are, and you have: password, biometrics, token. • Digital signature and Kerberos • Digital certificate and PKI • Access policy, access control matrix, access control list, capability, RBAC
Readings:	• Chapter 2.1 and Chapter 2.2
Assignments:	• Assignment 2 and Lab 4 due **Thursday, February 10 at 6:00 AM ET**
Assessments:	• Quiz 4 due **Thursday, February 10 at 6:00 AM ET**
Discussions:	Discussion 2 posts due **Thursday, February 10 at 6:00 AM ET**. Any posts after the due time will not be included in the grading process.
Live Classrooms:	• Lecture: **Thursday, February 3 from 7:00-8:30 PM ET** • Office hour: **Saturday, February 5 from 8:00-9:00 PM ET**

Module 5 Study Guide and Deliverables

Theme:	Network Security and Web Security
Topics:	• Threats to network: data interception, replay attack, port scanning, DoS, DDoS, MITM • Network defense: IPsec, VPN, Firewalls • Browser attacks, email attacks, misleading/malicious web content
Readings:	• Chapter 6 and Chapter 4
Assignments:	• Lab 5 due **Thursday, February 17 at 6:00 AM ET**
Assessments:	• Quiz 5 due **Thursday, February 17 at 6:00 AM ET**
Discussions:	• Discussion 3 posts due **Thursday, February 17 at 6:00 AM ET**. Any posts after the due time will not be included in the grading process.
Live Classrooms:	• Lecture: **Thursday, February 10 from 7:00-8:30 PM ET** • Office hour: **Saturday, February 12 from 8:00-9:00 PM ET**

Module 6 Study Guide and Deliverables

Theme:	Cyber System Security
Topics:	• Hardware security: meltdown, spectre, TEE • Virtualization and Cloud computing security • Mobile security and IoT security
Readings:	• Chapter 8 and Chapter 13.1
Assignments:	• Assignment 3 due **Thursday, February 24 at 6:00 AM ET**
Assessments:	• Quiz 6 due **Thursday, February 24 at 6:00 AM ET**
Discussions:	• None
Live Classrooms:	• Lecture: **Thursday, February 17 from 7:00-8:30 PM ET** • Office hour: **Saturday, February 19 from 8:00-9:00 PM ET**

Final Exam Details

The Final Exam is a proctored exam available from **Friday, February 25 at 6:00 AM ET to Monday, February 28 at 11:59 PM ET**.

The Computer Science Department requires that all final exams be administered using an online proctoring service called Examity that you will access via your course in Blackboard. In order to take the exam, you are required to have a working webcam and computer that meets Examity's system requirements. A detailed list of those requirements can be found on the How to Schedule page. Detailed instructions regarding your proctored exam will be forthcoming from the Assessment Administrator. You will be responsible for scheduling your own appointment within the defined exam window.

The Final Exam will be **open book/open notes** and is accessible during the final exam period. You can access it from the Assessments section of the course. Your proctor will enter the password to start the exam.

The following materials are allowed to use during the final exam:

- Use of the physical and/or ebook textbook.
- Use of any printed materials.
- Use of three pieces of blank scratch paper.

Final Exam Duration: **3 hours**.

Course Grading Information

It is important for each student to participate on a regular basis and complete all aspects of this course. This course is designed to include a major portion of learning by interacting (asynchronously) with the other students in the class, and the grade is therefore dependent on this activity. Course quizzes are cumulative in what they cover. This means that a quiz may include questions on material from prior modules.

Grading Structure and Distribution

The following tables depict how final grades will be calculated. Only exceptions necessary to maintain academic standards will be allowed.

Overall Grading Percentages	
Homework assignments	15
Quizzes	18
Lab exercises	25
Discussion and class participation	12
Proctored final exam	30

Grading Scale	
A	≥ 93
A-	90 ≤ and < 93
B+	85 ≤ and < 90
B	80 ≤ and < 85
B-	77 ≤ and < 80

C+	74 ≤ and < 77
C	70 ≤ and < 74
C-	65 ≤ and < 70
D	60 ≤ and < 65
F	≤ 60

Homework Assignments and Lab Exercises

- There are 3 homework assignments and 5 lab exercises. Both homework assignments and 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;
- Each assignment, including lab, quiz, discussion, etc., has a deadline. All assignments are assessed a 33% per-day late penalty, up to a maximum of 3 days. No assignments will be accepted four days after the deadline. Students with legitimate reasons who contact the professor before the deadline may apply for extension.
- All homework assignments or lab exercises are identified within the Online campus Study Guide.
- File names for assignment documents should be:

  CS695-HW<number>-<student last name>.doc

  An example assignment document file name is:

  CS695-HW5-Jacobs.doc

- File names for lab exercise documents should be:

  CS695-LAB<number>-<student last name>.doc

  An example lab exercise document file name is:

  CS695-LAB5-Jacobs.doc

- Include your name and assignment number in the header and a page number in the footer of you assignment submission document.
- Assignment submission documents MUST be in Word format with the file extension .doc, rather than .docx.
- 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.
- 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.

Quizzes

There will be six quizzes, one per every module. The purpose of quizzes is to help students practice and keep current with the course material.

Discussions

tudents will be participating in three graded discussions, one for Module 1, Module 4, and Module 5. The purpose of the discussions is to help students reflect, synthesize, do further research, and make connections between what you have learned and real world applications. Exchanging thoughts among students will help you learn from your peers. Check out the Discussion Rubric.

Final Exam

There will be a proctored Final Exam in this course. Detailed instructions regarding your proctored exam will be forthcoming from the Assessment Administrator. You will be responsible for scheduling your own appointment.

Delays

In the case of serious or emergency situations, or if, for any reason, you are unable to meet any assignment deadline, contact your instructor.

Discussion Grading Rubric

Graded discussion periods are held Day 1 of each module until 6:00 AM ET on Day 1 of the following module. You're certainly welcome to continue a discussion past the grading period, but that additional posted material will not affect your discussion grade. The discussion grading rubric below is the guide we use to evaluate your discussion contributions.

Discussion Grading Rubric					
Criteria	**51–60**	**61–70**	**71–80**	**81–90**	**91–100**
Participation	Very limited participation	Participation generally lacks frequency or relevance	Reasonably useful relevant participation during the	Frequently relevant and consistent participation	Continually relevant and consistent participation throughout the discussion period

			discussion period	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

Boston University Metropolitan College