CS449 – Introduction to Computer Security
Department of Computer Science
University of Massachusetts Boston

Instructor:

Bo Sheng
Email: Bo.Sheng@umb.edu
Web: http://www.cs.umb.edu/~shengbo/teaching/cs449.html
Phone: (617) 287-6468
Office: Science Building, 3rd Floor, Room 167 (S-3-167)

Course Description:

The course will provide an introduction to the fundamentals of computer security, and will cover both general theoretical aspects as well as applied methods of computer security. The course will address the general concepts of confidentiality, integrity and availability of digital information, and will focus on aspects such as: risks and vulnerabilities; models and policies for access control; program security – buffer overflow attacks, malware, viruses; browser security; authentication and authorization; encryption; and an overview of applied data, operating system and network security (with emphasis on Internet security). The course will also address the aspect of privacy, which is tightly related to security and is becoming increasingly important in today’s digital society.

Rationale for CS449

Security and privacy are essential aspects of computing today, as emphasized by numerous ongoing efforts in cybersecurity education and research at the state and federal levels. Cybersecurity is widely recognized as a top priority by both industry actors and funding agencies, and there is currently a pressing need for professionals trained in computer security. CS449 will be an important addition to the CS curriculum, which currently does not include any undergraduate course focused on security.

CS449 will be listed as a Computer Science elective course, and will complement the current offering of courses in both the mandatory and elective CS batches. For instance, the program security and OS security topics covered in CS449 will complement the materials included in required courses Introduction to Software Engineering (CS410) and Introduction to Operating Systems (CS444), respectively. Furthermore, the topics on data and network security covered in CS449 will complement well the curricula of elective courses Database Management Systems (CS430) and Introduction to Internetworking (CS446).

Textbook:

Additional Reading:

Introduction to Computer Security, Matt Bishop, Addison Wesley, 2005

Grading:

Final Exam: 35%
Midterm: 25%
Homework Assignments: 4 x 10% = 40% (late submissions will not receive any points)

Prerequisites:

CS240 – Programming in C
CS310 – Advanced Data Structures and Algorithms
CS341 – Computer Architecture and Organization

Covered Topics:

• Cryptography
• Access control
• Program security
• Browser security
• OS security
• Network Security
• Database Security
• Database Privacy

Attendance Policy:

Class attendance is mandatory. In case of missed class, students are responsible to get up-to-date with course materials and announcements. More than 5 (five) unexcused absences will lead to a failing grade. Absences will be excused only in cases of illness, family grievance, or an activity sponsored by the university. In all cases a doctor's note or other official documentation will be required.

Student Conduct:

Students are required to adhere to the University Policy on Academic Standards and Cheating, to the University Statement on Plagiarism and the Documentation of Written Work, and to the Code of Student Conduct as delineated in the University Catalog and Student Handbook. The Code is available online at http://www.umb.edu/life_on_campus/policies/code/
Accommodations:

Section 504 of the Americans with Disabilities Act of 1990 offers guidelines for curriculum modifications and adaptations for students with documented disabilities. If applicable, students may obtain adaptation recommendations from the Ross Center for Disability Services, CC-UL Room 211, (617-287-7430). The student must present these recommendations and discuss them with each professor within a reasonable period, preferably by the end of Drop/Add period.

Course Outline and Tentative Schedule:

Lecture 1
Course overview.

Lecture 2
Cryptography: Terminology and classic ciphers. Block ciphers.

Lecture 3

Lecture 4
Cryptography: Key Management, Key exchange. Digital Signatures.

Lecture 5
Program security: Buffer overflow. Trojans, logic bombs, viruses, worms.

Lecture 6
Program security: Botnets, rootkits.

Lecture 7

Lecture 8
Program security: Keystroke loggers, man-in-the-middle, covert channels.

Lectures 9-10
Operating systems security: User authentication. Access control (ACLs, access control matrix, capabilities).

Lecture 11

Lecture 12
Operating systems security: Discretionary Access Control vs. Mandatory Access Control.

Lecture 13

Operating systems security: Models of security: multilevel, Bell-La Padula.

Lecture 14

Operating systems security: Memory protection. Trusted computing base.

Lecture 15

Midterm Review.

Lecture 16

Midterm Exam.

Lecture 17

Network security: overview of network protocols.

Lecture 18-19

Network security: Attacks against TCP, IP security, TLS.

Lecture 20-21

Network security: overview of wireless communication. WEP.

Lecture 22

Network security: DNS Security.

Lecture 23


Lecture 24-25

Database security: Security in Relational Databases.

Lecture 26-27

Database Privacy: Anonymity Principle and Enforcement.

Lecture 28

Final Review