CS449
Introduction to Computer Security
Fall 2020

Gabriel Ghinita
University of Massachusetts at Boston
Contact Information

- **Instructor:** Dr. Gabriel Ghinita
  - **Email:** Gabriel.Ghinita AT umb DOT edu (preferred contact)
  - **Web:** [http://www.cs.umb.edu/~gghinita](http://www.cs.umb.edu/~gghinita)
Course Info

- **Lecture Hours**
  - Mon and Wed, 7:00-8:15pm
  - ONLINE

- **Office Hours**
  - Mon & Wed 5:30-7:00pm (online)

- **Class URL**
Textbook & Recommended Readings

- **Textbook**
  

- **Other recommended texts**
  
  *Introduction to Computer Security*, Matt Bishop
Prerequisites

- Data Structures and Algorithms
  - CS310

- Must have strong programming skills: Java and C
  - Helps to know Linux scripting and system tools

- Programming in C
  - CS240 – understand pointers!
  - Must be able to code in Unix-like systems

- Knowledge of OS, Computer Architecture, Databases, Networks
Grading

- Final exam (40%) – open book
- Midterm (30%) – open book (Wed Nov 4th)

- 5 homework assignments
  - 6% each
  - Assignments are individual – submit your own work only!
  - No plagiarism please – see student code of conduct

- Lecture attendance is mandatory
Course Materials

- **Class URL**
  - Username: CS449 (in CAPS)
  - Password: WLtsS@U#449!
  - *We LOVE to study Security @ UMB#449!*

- **Blackboard**
  - Discussion forums

- Make sure you create Unix course accounts
Course Rules & Conventions

- Security starts with good organization/administration!

- Course-related emails (for instructor and for TA)
  - Subject line **MUST BEGIN** with *[CS449]*

- Homework submission in digital form
  - Follow **EXACTLY** instructions
  - File names and directory structure **EXACTLY** as requested
  - File permissions must be correctly set: g+w, o-r
  - Ensure your files belong to correct grader group!
University Policies

- **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 Overview

- Cryptography
- Program Security
- Operating System Security
- Network Security
- Database Security
Causes of Security Incidents

- Unsecure software, or improperly configured
  - Unsafe programming languages, complex programs
  - Security considered rather as add-on, not by-design
- Awareness and education
  - Few courses in computer security
  - Programming text books do not emphasize security
- Usability and Economic factors
  - Security sometimes makes things harder to use
  - Consumers do not care about security
  - Security is difficult, expensive, few security audits
- Human users
  - Often the “weakest link”, due to lack of security education
What is This Course About?

- **Learn to think about security:**
  - Threats, defenses, policies
  - Software, human and environment factors

- **Think as an attacker:**
  - Learn to identify threats

- **Think as a security designer:**
  - Learn how to prevent attacks and/or limit their consequences
  - Understand and apply security principles
  - Learn tools that can defend against specific attacks, no silver-bullet solution
Security Goals

- Confidentiality (secrecy, privacy)
  - only those who are authorized to know can know

- Integrity
  - modifications only by authorized parties in authorized ways

- Availability
  - those authorized to access must be able to get access
Terminology

- Vulnerabilities (weaknesses)
- Threats (potential scenario of attack)
- Attacks
- Controls (security measures)
Security Principles

- **Principle of weakest link**
  - A system is as secure as its weakest link

- **Principle of adequate protection**
  - Maximize utility while limiting risk to an acceptable level within reasonable cost

- **Principle of effectiveness**
  - Controls must be efficient, easy to use

- **Kerkoff’s principle**
  - System design should be known, security relies on secret parameters (e.g., key)
  - Do NOT rely on “security-by-obscurity”
Ethical Use of Security Information

- We discuss vulnerabilities and attacks
  - Most vulnerabilities have been fixed
  - Some attacks may still cause harm
  - **DO NOT ENACT** in real life

- Purpose of this class
  - Learn to prevent malicious attacks
  - Use knowledge for good purposes