CSC 5270 Computer Sysyms Security

Course Description

In this age of Internet computing, there is indeed no place or time at which security does not matter. Protecting vital data from various attacks is always an important part in data systems. This course covers basic topics in protecting information computer systems and data from various attacks. It covers crypo-algorithms, protocols and system design principles, as well as case study.

Prerequisites: CSC 4420 and CSC 5250, or the instructor's permission.

Course Learning Objectives

• Understand basic crypto algorithms
• Understand important protocols for system security
• Be able to use Crypto++ for system security

Administrative Information

Class Times: 1:30pm to 2:50pm, Mon.
Class Location: State Hall, 318
Instructor: Lihao Xu

• Office: 5057 Woodward, Room 1401.1
• Email: lihao AT wayne.edu
• Office Hours: 12:50pm to 1:20pm, 3:00pm to 3:30pm, Mon., Wed.

TA: Sumukhi Chandrashekar

• Email: fl1985@wayne.edu
• Office Hours: 3:30pm to 4:30pm Mon., Wed.
• Location: 5057 Woodward, CS Dept meeting room, Room 2214, 2nd floor

Text Book

Prof. Lihao Xu
CSC 5270

Other References


Assignments and Evaluation

- Homeworks: 4, 50% of final grade
- Project: 1, 50% of final grade

Homework Policy

The grade of this course will be based on all the homework assignments. There will be neither midterm nor final exam. There will be a final class report. The weight of homeworks in the final grade is about 40% to 50%, and the rest goes to the final project.

Collaboration in terms of discussions is generally allowed and encouraged in the homeworks. But you should write the final solutions, including programs, alone, and understand them fully. It is absolutely not allowed to copy other people's solutions and programs.

Late homeworks lose 20% of their scores per day (except in cases of illness or emergency), and will not be accepted 3 days after the due date.

Course Content

- Aug. 31: Introduction

Symmetric Key Cryptosystems

- Sep. 7: Basics
- Sep. 12: Feistel Structure
- Sep. 14: DES (1)
• Sep. 19: DES (2)
• Sep. 21: AES
• Sep. 26: Modes of Block Ciphers
• Sep. 28: Combining Block Ciphers

---

• Sep. 7: Homework 1 out
• Sep. 21: Homework 1 due and Homework 2 out

Asymmetric Key Cryptosystems

• Oct. 3: Basics of Number Theory (1)
• Oct. 5: Basics of Number Theory (2)
• Oct. 10: Principles of Public Key Cryptosystems
• Oct. 12: RSA

---

• Oct. 5: Homework 2 due and Homework 3 out

Authentication and Signature

• Oct. 17: Authentication Code
• Oct. 19: Hash Functions (1)
• Oct. 24: Hash Functions (2)
• Oct. 26: Digital Signatures
• Oct. 31: Authentication Protocols (1)
• Nov. 2: Authentication Protocols (2)

---

• Oct. 24: Homework 3 due and Homework 4 out

Systems

• Nov. 7: Kerberos
• Nov. 9: Security of Email
• Nov. 14: Web Security
• Nov. 16: Dos Attacks
Special Notes

- **Religious Holidays**:

  Because of the extraordinary variety of religious affiliations of the University student body and staff, the Academic Calendar makes no provisions for religious holidays. However, it is University policy to respect the faith and religious obligations of the individual. Students with classes or examinations that conflict with their religious observances are expected to notify their instructors well in advance so that mutually agreeable alternatives may be worked out.

- **Student Disabilities Services**:

  If you have a documented disability that requires accommodations, you will need to register with Student Disability Services for coordination of your academic accommodations. The Student Disability Services (SDS) office is located at 1600 David Adamany Undergraduate Library in the Student Academic Success Services department. SDS telephone number is 313-577-1851 or 313-577-3365 (TDD only). Once you have your accommodations in place, I will be glad to meet with you privately during my office hours to discuss your special needs. Student Disability Services' mission is to assist the university in creating an accessible community where students with disabilities have an equal opportunity to fully participate in their educational experience at Wayne State University. Students who are registered with Student Disability Services and who are eligible for alternate testing accommodations such as extended test time and/or a distraction-reduced environment should present the required test permit to the professor at least one week in advance of the exam. Federal law requires that a student registered with SDS is entitled to the reasonable accommodations specified in the studentâ€™s accommodation letter, which might include allowing the student to take the final exam on a day different than the rest of the class.

- **Academic Dishonesty - Plagiarism and Cheating**:

  Academic misbehavior means any activity that tends to compromise the academic integrity of the institution or subvert the education process. All forms of academic
misbehavior are prohibited at Wayne State University, as outlined in the Student Code of Conduct (http://www.doso.wayne.edu/student-conduct-services.html). Students who commit or assist in committing dishonest acts are subject to downgrading (to a failing grade for the test, paper, or other course-related activity in question, or for the entire course) and/or additional sanctions as described in the Student Code of Conduct.

- Cheating: Intentionally using or attempting to use, or intentionally providing or attempting to provide, unauthorized materials, information or assistance in any academic exercise. Examples include: (a) copying from another student’s test paper; (b) allowing another student to copy from a test paper; (c) using unauthorized material such as a "cheat sheet" during an exam.
- Fabrication: Intentional and unauthorized falsification of any information or citation. Examples include: (a) citation of information not taken from the source indicated; (b) listing sources in a bibliography not used in a research paper.
- Plagiarism: To take and use another’s words or ideas as one’s own. Examples include: (a) failure to use appropriate referencing when using the words or ideas of other persons; (b) altering the language, paraphrasing, omitting, rearranging, or forming new combinations of words in an attempt to make the thoughts of another appear as your own.
- Other forms of academic misbehavior include, but are not limited to: (a) unauthorized use of resources, or any attempt to limit another student’s access to educational resources, or any attempt to alter equipment so as to lead to an incorrect answer for subsequent users; (b) enlisting the assistance of a substitute in the taking of examinations; (c) violating course rules as defined in the course syllabus or other written information provided to the student; (d) selling, buying or stealing all or part of an un-administered test or answers to the test; (e) changing or altering a grade on a test or other academic grade records.

- **Course Drops and Withdrawals**:

  In the first two weeks of the (full) term, students can drop this class and receive 100% tuition and course fee cancellation. After the end of the second week there is no tuition or fee cancellation. Students who wish to withdraw from the class can initiate a withdrawal request on Pipeline. You will receive a transcript notation of WP (passing), WF (failing), or WN (no graded work) at the time of withdrawal. No withdrawals can be initiated after the end of the tenth week. Students enrolled in the 10th week and beyond will receive a grade. Because withdrawing from courses may have negative academic and financial consequences, students considering course withdrawal should make sure they fully understand all the consequences before taking this step. More information on this can be found at: http://reg.wayne.edu/pdf-policies/students.pdf

- **Student services**:
  - The Academic Success Center (1600 Undergraduate Library) assists students with content in select courses and in strengthening study skills. Visit www.success.wayne.edu for schedules and information on study skills workshops, tutoring and supplemental instruction (primarily in 1000 and 2000 level courses).
• The Writing Center is located on the 2nd floor of the Undergraduate Library and provides individual tutoring consultations free of charge. Visit http://clasweb.clas.wayne.edu/writing to obtain information on tutors, appointments, and the type of help they can provide.

• **Class recordings:**

Students need prior written permission from the instructor before recording any portion of this class. If permission is granted, the audio and/or video recording is to be used only for the student’s personal instructional use. Such recordings are not intended for a wider public audience, such as postings to the internet or sharing with others. Students registered with Student Disabilities Services (SDS) who wish to record class materials must present their specific accommodation to the instructor, who will subsequently comply with the request unless there is some specific reason why s/he cannot, such as discussion of confidential or protected information.

All Rights Reserved, Lihao Xu, Fall 2016