CSC5270 Syllabus

1. CSC 5270 Computer Systems Security

2. 3 Credits
   Class Times: 1:00pm to 2:15pm, Mon., Wed.
   Class Location: State Hall, 318

3. Instructor: Lihao Xu

4. Text book

   Other References


5. Specific course information
   a. brief description of the content:
      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 crypto-algorithms, protocols and system design principles, as well as case study.

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

   c. Elective

6. Course Learning Objectives
Upon successful completion of this course, the students will be able to:

a. Understand basic crypto algorithms
b. Understand important protocols for system security
c. Be able to use Crypto++ for system security

7. Brief list of topics to be covered

Course Content

Aug. 30: Introduction

**Symmetric Key Cryptosystems**

Sep. 6: Basics

Sep. 11: Feistel Structure

Sep. 13: DES (1)

Sep. 15: DES (2)

Sep. 20: AES

Sep. 22: Modes of Block Ciphers

Sep. 27: Combining Block Ciphers

Sep. 6: Homework 1 out

Sep. 20: Homework 1 due and Homework 2 out

**Asymmetric Key Cryptosystems**

Oct. 2: Basics of Number Theory (1)

Oct. 4: Basics of Number Theory (2)

Oct. 9: Principles of Public Key Cryptosystems

Oct. 11: RSA

Oct. 4: Homework 2 due and Homework 3 out
Oct. 16: Authentication Code

Oct. 18: Hash Functions (1)

Oct. 23: Hash Functions (2)

Oct. 25: Digital Signatures

Oct. 30: Authentication Protocols (1)

Nov. 1: Authentication Protocols (2)

Oct. 23: Homework 3 due and Homework 4 out

**Systems**

Nov. 6: Kerberos

Nov. 8: Security of Email

Nov. 13: Web Security

Nov. 15: Dos Attacks

Nov. 8: Homework 4 due

**Final Class Report**

Nov. 6: Report Proposal due

Nov. 15 to Dec. 17: Reading and Writing Time

Dec. 17: Final Class Report due.