

School of Interdisciplinary Informatics
University of Nebraska Omaha

CYBR/CSCI 8410 Distributed System Security
Spring 2021

Instructor	Rui Zhao
Email	ruizhao@unomaha.edu
Phone	402-554-2852
Day & Time	TBD, 01/11/2021 - 05/07/2021
Lecture Location	Online, zoom link will be provided on Canvas
Office	Peter Kiewit Institute (PKI) 282C
Office Hour	(online) by appointment

Course Description:

The course aims at understanding the issues surrounding data security, integrity, confidentiality and availability in distributed systems. Further, we will discuss various network security issues, threats that exist and strategies to mitigate them. This course will cover topics in cryptography, public key infrastructure, authentication, hashing, digital signatures, ARP protection, IP and IPSEC, IP Tables, SSL/TLS, firewalls, etc.

Course Objective

Upon completion of the course each student should:

- Understand the components of public key infrastructure
- Understand cryptographic algorithms that are used to secure client-server communication
- Understand the idea of authentication and how algorithms enable authentication over the Internet
- Understand hashing algorithms used to protect integrity of data over the Internet
- Become familiar with SSL/TLS, IP Tables and firewalls
- Understand anonymity issues in peer-to-peer systems
- Understand information dispersal algorithms for distributed storage
- Understand the ideas behind structured and unstructured peer-to-peer systems
- Understand the security issues surrounding unstructured peer-to-peer systems and small world networks

Course Materials:

Stallings, W., Cryptography and Network Security: Principles and Practice, 8th Edition, Prentice Hall.

Stalling, W., Brown, L., Computer Security: Principles and Practice, 3rd Edition, Prentice Hall.

We will also discuss a list of recent and classic research papers in security and privacy; they can be accessed on Canvas.

Email Communication:

Students are expected to check their campus e-mail account on a regular basis (at least twice in a week). Students may forward their campus e-mail to a private e-mail account, but are expected to assure the forwarding of messages is working properly so they do not miss important email communications.

Course Schedule (Tentative):

I reserve the right to amend this syllabus at any time and the course schedule only represents my best estimate. The latest version is updated on the Canvas.

Week	Date	Topic	Chapter	Lab	Paper	Project Due
1	1/11/21	Introduction to Computer/Network Security	COMP.Chap1, CYPT.Chap1			
2	1/18/21	Crypto Foundations Review 1	CYPT.Chap2,3,4,5,6			
3	1/25/21	Crypto Foundations Review 2	CYPT.Chap7,8,9,11,12,13	Lab 1		
4	2/1/21	Key Management and Distribution	CYPT.Chap15		Paper 1	Proposal
5	2/8/21	User Authentication 1	COMP.Chap3	1 Due		
6	2/15/21	User Authentication 2	CYPT.Chap16		1 Due	
7	2/22/21	Network Access Control and Cloud Security	CYPT.Chap21,22	Lab 2		
8	3/1/21	Denial-of-Service Attacks	COMP.Chap7		Paper 2	
9	3/8/21	Midterm Exam		2 Due	-	
10	3/15/21	Spring Break		-	-	
11	3/22/21	Intrusion Detection	COMP.Chap8	Lab 3	2 Due	
12	3/29/21	Firewalls and Intrusion Prevention Systems IP Security	COMP.Chap9 CYPT.Chap20		Paper 3	
13	4/5/21	Transport-Level Security Wireless Network Security	CYPT.Chap17, COMP.Chap22 CYPT.Chap18, COMP.Chap24	3 Due		
14	4/12/21	Software Security	COMP.Chap11	Lab 4	3 Due	
15	4/19/21	Operating System Security	COMP.Chap12		Paper 4	
16	4/26/21	Prep Week	-	4 Due	-	Final Report
17	5/3/21	Final Exam	-	-	4 Due	

CYPT	Cryptography and Network Security: Principles and Practice	8th edition
COMP	Computer Security: Principles and Practice	3rd edition

Grading Policy:

The final grade will be composed of:

- Lab 30%
- Paper Summary 10%
- Midterm exam (online, open book, open notes) 20%
- Final exam (online, open book, open notes) 20%
- Project 20%

Grades will be assigned as follows:

- $96.67 \leq \{A+\};$ $93.33 \leq \{A\} < 96.67;$ $90.00 \leq \{A-\} < 93.33;$
- $86.67 \leq \{B+\} < 90.00;$ $83.33 \leq \{B\} < 86.67;$ $80.00 \leq \{B-\} < 83.33;$
- $76.67 \leq \{C+\} < 80.00;$ $73.33 \leq \{C\} < 76.67;$ $70.00 \leq \{C-\} < 73.33;$
- $66.67 \leq \{D+\} < 70.00;$ $63.33 \leq \{D\} < 66.67;$ $60.00 \leq \{D-\} < 63.33;$
- $\{F\} < 60.00.$

Homework/Lab Assignments:

Assignments are to be completed on your own unless explicitly noted by your instructor. You may discuss any component of the assignment with your classmates, but there cannot be a physical or electronic record of your conversation (no paper, files, disks, or code of any form) taken away from the conversation. While you are encouraged to discuss with each other students, **you must write your own code and answers, in whole.** You cannot directly use the code or answers that you have found on the Internet. **Copying any portion of the code or answers will result in an automatic zero for the assignments for all students involved. Two or more instances of this in the course will result in an automatic failure for the course.**

Assignments are due at **11:59PM of the specified due day.** You should turn in the PDF electronic version of your answers to the questions in each assignment. For some assignments, you also need to turn in the source code or other related files.

To turn in your assignment: Log into Canvas and submit the zipped file into the appropriate homework/lab assignment.

Late submissions: In case you cannot complete an assignment by the beginning of class on the due date, you can take another week to turn it in with the penalty of 10% for each additional day. Beyond **one week from the specified due date** the homework shall **NOT** be graded for any reason.

If you think your score is not correct, please appeal it to the instructor within 10 days from the time when it is posted. After 10 days, the score will be considered as finalized. An email will be sent through the Canvas every time when a score is posted.

Paper Summaries:

Each paper summary should be approximately between 300 and 400 words. You can write longer summaries if you really want to discuss some of your own opinions. Summaries should be written in your own words; you cannot directly copy the sentences from the paper! Ideally, each summary should be a critical analysis of a research paper from some perspectives such as threat model, assumptions, techniques, and evaluation; it should not simply be a description of the organization of that paper.

The elements of a summary must include the key points of the paper, background, motivation, related work, a critique of the paper, and analysis of the lessons to be gained from the paper. Ideally, each summary should be a critical analysis of a research paper from some perspectives such as threat model, assumptions, techniques, and evaluation; it should not simply be a description of the organization of that paper.

Summaries should be submitted to the Canvas. You will use the Blog tool on Canvas to submit summaries. You have your own individual Blog to post your Blog Entries (each summary should be in a

new blog entry, with the paper's title as the blog entry's title). All others enrolled in the course are able to and are encouraged to view and add comments to your Blog Entries.

Exams:

Exams are online, open-book, open-notes, and written. The questions asked in the exam will cover the contents from the textbook, assignments, papers, and extra materials.

There will not be any makeup exam, unless you provide convincing evidences in advance and get a preapproval from the instructor.

Project:

Students will conduct research projects over the course of the semester **individually**. The topics of the course project can come from research papers, in-class discussion, and other sources. Students are strongly encouraged to identify a good security research topic by themselves or from the discussion with the instructor. Students need to write a two-page project proposal report and a six-page final project report. The content organization of the reports should be similar to those of the conference papers summarized in the class. The originality and quality of your project determine the grade students can earn. The project progress will be regularly discussed in class.

Students with Disabilities:

Accommodations are provided for students who are registered with Disability Services and make their requests sufficiently in advance. For more information, please contact Disability Services (EAB 117, Phone: 554-2872, TTY: 554-3799) or go to the website: <http://www.unomaha.edu/disability>.

Copyright Notice:

Students must ask the instructor's permission to use the materials including but not limited to the syllabus, lecture notes, quizzes, and projects. The instructor does not grant to the students the right to publish these materials for profit in any form.