

# OU 4173/5173 Computer Security Fall 2019 Syllabus

## 1. Instructor:

Dr. Song Fang ([songf@ou.edu](mailto:songf@ou.edu))

Office hour: T&R 1:30pm to 3:00pm in DEH 232

Class meetings: T&R 3:00pm to 4:15pm in DEH 0120

## 2. Teaching Assistant:

Mr. Edwin Yang ([helloworld2edwin@ou.edu](mailto:helloworld2edwin@ou.edu))

Office hour: F 2:00 – 3:00 pm in DEH 115

## 3. Prerequisites

CS 3113

## 4. Course Description

The course is a study of fundamental concepts and principles of computer security. The course covers basic security topics, including symmetric and public key cryptography, digital signatures, cryptographic hash functions, authentication pitfalls, network security protocols, and web security.

Note: No student may earn credit for both 4173 and 5173.

## 5. Course Objectives

By the end of this course, students will be able to:

- Understand basic security terms such as plaintext, ciphertext, encryption/decryption, hash function and authentication.
- Develop an understanding of security policies (such as confidentiality, integrity and availability) as well as protocols to implement such policies in the form of message exchange.
- Explain the basic number theory required for cryptographic applications, and encrypt/decrypt and sign/verify signatures using cryptographic approaches.
- Identify typical security pitfalls in authentication protocols, and outline the protocols, i.e., AH and ESP protocols, for IP Security.

## 6. Student Learning Outcomes:

During the semester, students will have:

- One midterm
- One semester project
- Multiple in-class quizzes
- 5-6 Labs: Each lab includes a report. The labs are from the [SEED labs](#).

## 7. Recommended Textbook:

Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World, 2nd Edition*, Prentice Hall, 2002, ISBN: 0-13-0460192.

Wenliang Du. *Computer Security: A Hands-on Approach. 1st Edition*, 2017.

## 8. Tentative Schedule:

(These will be adjusted based on the actual progress in a semester.)

### T1. Basic Security Concepts (1 lecture)

- Confidentiality, integrity, availability
- Security policies, security mechanisms, assurance

### T2. Basic Cryptography (1 lecture)

- Historical background
- Transposition/Substitution, Caesar Cipher
- Introduction to Symmetric crypto primitives, Asymmetric crypto primitives, and Hash functions

### T3. Secret Key Cryptography (5 lectures)

- Data Encryption Standard (DES)
- Encrypting large messages (ECB, CBC, OFB, CFB, CTR)
- Multiple Encryption DES (EDE)

### T4. Message Digests (2 lectures)

- Applications
- Strong and weak collision resistance
- The Birthday Paradox
- MD5, SHA-1

### T5. Public Key Cryptography (4 lectures)

- Number theory: Euclidean algorithm, Euler Theorem, Fermat Theorem, Totient functions, multiplicative and additive inverse
- RSA, Selection of public and private keys
- Blockchain

### T6. Network Security (3 lecture)

- Packet Sniffing and Spoofing
- Attack on the TCP protocol
- TCP session hijacking attack

### T7. Web Security (3 lectures)

- Introduction to web security
- Cross-Site Request Forgery (CSRF), Cross-site Scripting (XSS)
- SQL Injection

#### T8. Authentication (2 lectures)

- Basic concepts of identification and authentication
- Password authentication
- Authentication protocols

### 9. Grading:

Quizzes	5%
Labs	30%
Midterm	30%
Project	35%

Grading scale: The scale for final letter grades is as follows, using standard notation for ranges: A ( $(\infty,90]$ ); B ( $(90,80]$ ); C ( $(80,70]$ ); D ( $(70,60]$ ); F ( $(60,0]$ ).

### 10. Policies on Late Assignments:

For each day an assignment is late - up to a maximum of 3 days, the grade is reduced 15%. For example, if you submit a 90%-correct assignment 2 days late, your overall assignment score will be 60%.

### 11. Policies on Absences and Scheduling Makeup Work:

There will be no makeups for homework assignments. Make-up exams will not normally be permitted. Exceptions will be made if a student presents a police report or a doctor's note that shows some emergency situation.

### 12. Student Evaluations:

The College of Engineering utilizes student ratings as one of the bases for evaluating the teaching effectiveness of each of its faculty members. The results of these forms are important data used in the process of awarding tenure, making promotions, and giving salary increases. In addition, the faculty uses these forms to improve their own teaching effectiveness. The original request for the use of these forms came from students, and it is students who eventually benefit most from their use. Please take this task seriously and respond as honestly and precisely as possible, both to the machine-scored items and to the open-ended questions.

### 13. University Policies:

In this section, include the mandatory University policies.

#### Academic Integrity

Cheating is strictly prohibited at the University of Oklahoma, because it devalues the degree you are working hard to get. As a member of the OU community, it is your responsibility to protect your educational investment by knowing and following the rules. A student must complete his/her tests, projects and assignments on his/her own. A student's signature on any tests, projects and assignments indicates that the student neither gave nor received unauthorized aid. Academic misconduct is defined as any act which improperly affects the evaluation of a student's academic performance or achievement. It specifically includes cheating, plagiarism, fabrication, fraud, destruction of property, and bribery or intimidation, as well as assisting others or attempting to engage in such acts. It is the responsibility of each student to be familiar with the definitions, policies and procedures concerning academic misconduct. For more information, please review the Student's Guide to Academic Integrity at [http://integrity.ou.edu/students\\_guide.html](http://integrity.ou.edu/students_guide.html).

### **Religious Observance**

It is the policy of the University to excuse the absences of students that result from religious observances and to reschedule examinations and additional required classwork that may fall on religious holidays, without penalty.

### **Reasonable Accommodation Policy**

Students requiring academic accommodation should contact the Disability Resource Center for assistance at (405) 325-3852 or TDD: (405) 325-4173. For more information please see the Disability Resource Center website <http://www.ou.edu/drc/home.html>. Any student in this course who has a disability that may prevent him or her from fully demonstrating his or her abilities should contact me personally as soon as possible so we can discuss accommodations necessary to ensure full participation and facilitate your educational opportunities.

### **Title IX Resources and Reporting Requirement**

For any concerns regarding gender-based discrimination, sexual harassment, sexual assault, dating/domestic violence, or stalking, the University offers a variety of resources. To learn more or to report an incident, please contact the Sexual Misconduct Office at 405/325-2215 (8 to 5, M-F) or [smo@ou.edu](mailto:smo@ou.edu). Incidents can also be reported confidentially to OU Advocates at 405/615-0013 (phones are answered 24 hours a day, 7 days a week). Also, please be advised that a professor/GA/TA is required to report instances of sexual harassment, sexual assault, or discrimination to the Sexual Misconduct Office. Inquiries regarding non-discrimination policies may be directed to: Bobby J. Mason, University Equal Opportunity Officer and Title IX Coordinator at 405/325-3546 or [bjm@ou.edu](mailto:bjm@ou.edu). For more information, visit <http://www.ou.edu/eoo.html>.

### **Adjustments for Pregnancy/Childbirth Related Issues**

Should you need modifications or adjustments to your course requirements because of documented pregnancy-related or childbirth-related issues, please contact your professor or the Disability Resource Center at 405/325-3852 as soon as possible. Also, see <http://www.ou.edu/eoo/faqs/pregnancy-faqs.html> for answers to commonly asked questions.

### **Final Exam Preparation Period**

Pre-finals week will be defined as the seven calendar days before the first day of finals.

### **Emergency Protocol**

During an emergency, there are official university [procedures](#) that will maximize your safety.

**Severe Weather:** If you receive an OU Alert to seek refuge or hear a tornado siren that signals severe weather *1. LOOK* for severe weather refuge location maps located inside most OU buildings near the entrances *2. SEEK* refuge inside a building. Do not leave one building to seek

shelter in another building that you deem safer. If outside, get into the nearest building. 3. *GO* to the building's severe weather refuge location. If you do not know where that is, go to the lowest level possible and seek refuge in an innermost room. Avoid outside doors and windows. 4. *GET IN, GET DOWN, COVER UP*. 5. *WAIT* for official notice to resume normal activities.

[Link to Severe Weather Refuge Areas](#) , [Severe Weather Preparedness - Video](#)

**Armed Subject/Campus Intruder:** If you receive an OU Alert to shelter-in-place due to an active shooter or armed intruder situation or you hear what you perceive to be gunshots:

1. *GET OUT*: If you believe you can get out of the area *WITHOUT* encountering the armed individual, move quickly towards the nearest building exit, move away from the building, and call 911. 2. *HIDE OUT*: If you cannot flee, move to an area that can be locked or barricaded, turn off lights, silence devices, spread out, and formulate a plan of attack if the shooter enters the room. 3. *TAKE OUT*: As a last resort fight to defend yourself.

For more information, visit <http://www.ou.edu/emergencypreparedness.html>

[Shots Fired on Campus Procedure - Video](#)

**Fire Alarm/General Emergency:** If you receive an OU Alert that there is danger inside or near the building, or the fire alarm inside the building activates: 1. *LEAVE* the building. Do not use the elevators. 2. *KNOW* at least two building exits 3. *ASSIST* those that may need help 4.

*PROCEED* to the emergency assembly area 5 *ONCE safely outside, NOTIFY first responders of anyone that may still be inside building due to mobility issues*. 6. *WAIT* for official notice before attempting to re-enter the building.

[OU Fire Safety on Campus](#)

*\*Every part of this syllabus is subject to adjustment as the semester progresses. If you are dissatisfied with the course policies, grading, and assignments, please contact the instructor. Reasonable requests for modifications may be accommodated at the instructor's discretion.*