Network Security (CS 465 & CS 565) Fall 2018

October 30, 2018

Course Description

This course provides introductory but comprehensive coverage of fundamental problems, principles, and techniques in network security with emphasis on cryptographic and hands-on techniques. We will cover a comprehensive list of topics including basic networking theory & techniques, basic cryptographic techniques for implementing network security and hands-on techniques for evaluating network security like networking sniffing, denial of service attacks, TCP/IP hijacking, port scanning, remote shell code development, network packet manipulation techniques and network protocol analysis. For the hands-on parts of the course We will learn to use commonly used tools for offensive network security with an emphasis on their principles and fundamental techniques. The cryptographic techniques will focus on the mathematical aspects of the algorithms and their implementations. Time permitting we will cover some aspects of Privacy.

Goal: At the end of the course the students should have a solid understanding of both the theoretical and practical aspects of Network Security. They should be able to use common tools for testing and exploiting systems with the goal of protecting them against black hats.

Instructor Info

Dr. Tathagata Mukherjee
Class Room: OKT N324
Class Hours: TR 11:20 AM - 12:40 PM
Email: tm0130@uah.edu
Office: OKT N347
Office Hours: TWR 3:00 - 4:00 PM or By Appointment
Course Resource: Canvas

Pre-Requisites

The required courses for taking this course are CS 121 & CS 221 or CPE 221. Broadly the pre-requisites for this course ensure that the student has taken Computer Organization and Data Structures or have a good understanding of basic data types, data structures, function calls, and memory layout of programs.
Additionally a good understanding of operating systems and computer networking models is a plus. The student should be able to read and understand C programs. Being able to understand x86 assembly and write short x86 assembly programs is a major plus. The student should also have a general understanding of computer security. Having hands-on working knowledge of common vulnerabilities and exploits (such as buffer overflow and string format vulnerabilities) and various shell code development is a plus.

Please email the instructor if you are not sure whether you have the required background to take the course. Note instructor will NOT be able to waive pre-requisites.

Books

1. Text Book: The Network Security Test Lab: A Step By Step Guide
2. In addition to the textbooks, papers, documents, and notes from the literature will be distributed during the lectures
3. Paper readings will be assigned from time to time and the contents will be part of the syllabus

Assignments and Projects

Three homework assignments will be given along the lectures and they need to be done individually (or in groups of TWO) and turned in. There will be TWO hands-on projects to be implemented in programming language of your choice and demonstrated in front of the instructor. The instructor reserves the right to ask any question. There will be no midterm exam, one small surprise test (or a presentation on the term project) and a group term project. The weight distribution will be as follows:

1. Class Attendance & Participation 5 %
2. Homework assignments 20 %
3. Hands-on projects 30 %
4. Term project (Team Effort) 25 %
5. Final 20 %

The grade assignment will be as follows:

1. Over 90 %: A
2. Between 85 % and 90 %: A-
3. Between 80 % and 85 %: B+
4. Between 70 % and 79 %: B
5. Between 65 % and 69 %: B-
6. Between 60 % and 64 %: C+
7. Between 55 % and 59 %: C
8. Between 50 % and 55 %: C-
9. Less than 50: F

NOTE: I will FORCE everyone to use Latex for writing reports and homework solutions. Anyone using Latex will get a BONUS of 5 points. On Linux systems Latex can be installed by installing the Tex Live distribution. If you use any standard Linux distribution the official software repositories will have the distribution. For Mac you should download and install MacTex. For Windows there is MiKTex. You will probably use the "pdflatex" command most often for compilation of your latex code into PDF documents. You can use any standard text editor for writing Latex and use the latex commands from the terminal (command prompt). If you want you can also use Overleaf which is an online Latex editor for all your projects. It saves you the time and effort to install and get a Latex system working on your system. But being in the network Security class, I would expect that you would have the tenacity to get the Latex system installed on your system. As for Editors I prefer Sublime Text which is technically not free but you can use the evaluation version for ever. You can also use Emacs which is great but works well on Linux only.

Term Project

The term project will be set by the instructor and discussed on first day of class. It will be a group effort and end with the submission of a term project report. The format for the report will be posted by the instructor.

Tentative Schedule

1. Lectures 1,2,3,4,5,6 will cover the first part of the course. These lectures will go over the idea of ciphers, basic ciphers and modes of operation, the Diffie-Hellman Algorithm, Number and Group Theory and Attack on Diffie-Hellman Key Exchange. These lectures will tentatively be completed by the end of October.

2. Project 1 Posting: August 30 or Start of September
3. Homework 1 Posting: Mid September
4. Project 2 Posting: September end to October Beginning
5. Homework 2 Posting: October end
6. Lectures 7,8,8,10 will tentatively cover more offensive techniques like buffer overflow attacks and port scanning.
7. Homework 3 Posting: Mid November
8. Term Project Report Due: Finals Week November 29, 2018
9. **Finals Thursday November 29, 2018 11:30 AM - 2:00 PM**

Expectation from Students

Attendance is expected for this class. Unless you obtain prior consent of the instructor, missing classes will be used as basis for attendance grading. In case that it is necessary to skip a class, students are responsible to make up missed materials. Participation in in-class discussions and activities is also expected. All submitted assignments and projects must be done by the author(s). **It is a violation of the Academic Honor Code to submit other's work and the instructor of this course takes these violations very seriously and will most likely FAIL the student for the entire class in case of honor code violations. So please be careful.**

Changes to Syllabus

There might be small changes to the syllabus as we proceed. The instructor will determine, based on the student's progress, how much to cover in the time frame of the semester. Stress will be on ensuring that the students understand the concepts taught in class and are able to apply them for solving real life problems, not on speed. The changes to the syllabus will be posted on canvas and will also be discussed in class.

Disclaimer

This course will cover certain techniques to break down known systems in order to demonstrate their vulnerabilities. However it is illegal to practice these techniques on others' systems without explicit written consent as is done by white hat hackers. With great power comes great responsibility and so the students will be liable for their behavior and the resulting consequences if the tools learned in class are used unethically or unlawfully.

CS Department Policies and Procedures

This document should be handed out with the syllabus and discussed on the first day of classes

Responsibilities of Teacher

1. Provide a detailed syllabus. This syllabus should list office hours, course objectives, textbooks, references, prerequisites, and grading policy/method of assessment.

2. Come to class well prepared, on time, and make full use of the class time.

3. Provide timely and adequate feedback on grades. Return graded material promptly.

4. Conduct final exam at the time designated in the class schedule. Never post grades.

5. Not assign **new** work (i.e. not listed on syllabus) that is due in last two weeks of classes.

6. Avoid leaving the examination room without a proctor. Provide paper for exams. Make reasonable use of the assigned textbook.

7. Check students have proper prerequisites. Instructor does not waive assigned prerequisites.

8. Report all incidences of academic misconduct to the Department and VP for Student Affairs

Responsibilities of Student

1. Come to class with the proper prerequisites, well prepared, on time, and make full use of the class time.

2. Provide adequate notice of anticipated absences and take full responsibility for finding out about missed work, announcements, and assignments.

3. Submit assessment material on time and submit only your own work. (see integrity)

4. Do not allow other students to copy your work.

5. Read and understand the syllabus and follow announced policies.

Integrity

We expect CS instructors and students to conduct themselves in a professional manner. Students are subject to all the provisions in the UAH Code of Student Conduct, which is available free from the Office of Admissions and Records. Information on plagiarism and other forms of misconduct is presented in the Student Handbook Article III. Departments are obliged to report all student misconduct to the Office of Student Affairs.

Complaint Procedure

If you have difficulties or complaints related to this course, your first action should be to discuss them with your instructor. If such a discussion would be uncomfortable for you or fails to resolve your difficulties, you should ask for a meeting with the Chair of the Computer Science Department in Technology Hall N-300, info@cs.uah.edu, telephone 824-6088. If you are still unsatisfied, you should discuss the matter with Dr. Debra Moriarity, Associate Dean of the College of Science, moriard@email.uah.edu. Dr. Moriarity's office is CS 207 Materials Science Building.

Students with Disabilities

Your instructor would like to hear from anyone who has a disability that may require a modification of seating, testing, or other class procedures. Please see instructor after class or during office hours to discuss appropriate modifications. You should also contact Student Development Services in UC 113 (Ph. 824 6203) for further assistance.

Student Computer Account

Students enrolled in any CS course are entitled to an account on the departmental computer network. Use of such an account is subject to departmental and university policies. To apply for an account, and see the current policies, go to the departmental web site at http://www.cs.uah.edu/account/

Examination Policy

In response to past student complaints about problems during examinations, the Computer Science Department has developed the following guidelines for in-class examinations in all courses.

1. Come to the exam prepared to complete it without a break. If you think you will need a break, please inform the proctor before the exam if possible.

2. Do not communicate with other students. Talk only to the instructor.

3. Whenever you leave the exam room turn in your exam.

4. Use only the paper provided by the instructor for all writing.

5. If assigned a specific seat, remain in that seat.

6. Unless specifically permitted by the instructor, use no books or other reference materials. Do not bring calculators, computers, pocket-organizers, cell phones, pagers, or other electronic devices to the exam.