CSC 581 Class Information and Syllabus

Instructor: Stephen R. Tate (Steve)
Lectures: Tues/Thurs 3:30-4:45, Petty 224
Office: Petty 166
Office Hours: Tues/Thurs 10:00-12:00, or by appointment
Phone: 336-256-1033
E-mail: `srtate@uncg.edu`

Class Web Page: `http://www.uncg.edu/cmp/faculty/srtate/581/`

Catalog Description: Core concepts in computer security, including the security goals of confidentiality, integrity, and availability; authentication; access control; secure software development; use of cryptography; and basic network security.

Prerequisites: Grade of C or better in CSC 261 and CSC 330, or permission of instructor.

Longer Description: This class provides an introduction to computer security concepts, techniques for protecting information and computer systems, and practice using a "security mindset." The course includes coverage of authentication, access control models, operating system security, cryptography, network security, and software security. Topics are covered at an introductory level, with subsequent courses available for more in-depth exploration of cryptography and network security. Student work will include a mix of written (analytical) work and hands-on security exercises.

Student Learning Outcomes: Upon successful completion of this course students should be able to

1. Describe the basic goals of computer security;
2. Identify appropriate technologies related to different computer security goals;
3. Describe high-level properties of basic cryptographic mechanisms, including symmetric and public-key encryption, pseudorandom number generators, cryptographic hash functions, and digital signatures;
4. Explain secure design principles such as isolation and least privilege, and their relation to modern system tools and technologies;
5. Identify common vulnerabilities in software;
6. Describe secure software development principles and practices;
7. Diagram a basic networked system, identifying security-sensitive aspects and appropriate protection techniques;
8. (Graduate Students) Explain and critique research in computer security.

Textbook and Readings: The required textbook is

> Michael T. Goodrich and Roberto Tamassia. *Introduction to Computer Security*, Pearson, 2011. ISBN-13 978-0-321-51294-9.

Additional readings will be assigned throughout the semester, ranging from current news stories to technical articles to research papers. All of the additional readings will either be freely available or copies will be provided for students.

Labs and Optional Text: Hands-on exercises will come from the SEED labs developed by Wenliang Du at Syracuse University (possibly slightly modified). While these labs are very well documented on the SEED lab web site, students looking for more information can consider purchasing Prof. Du's book:

> Wenliang Du. *Computer Security: A Hands-on Approach*, CreateSpace Independent Publishing, 2017. ISBN-13: 978-1548367947.

Topics: Since Fall 2018 is the first semester this class is being offered, the schedule is not completely determined. The topics to be covered are shown below, where each topic is a single class meeting unless otherwise specified. For an updated week-by-week schedule, please see the class web site.

> Class Overview
> Overview of computer security and basic goals (Sections 1.1 and 1.4)
> High level view of cryptography (Section 1.3)
> Physical security (Sections 2.1-2.5)
> Access Control Models (Sections 1.2, 9.1, and 9.2)
> Operating System Security - Basics (Sections 3.1-3.3)
> Operating System Security - Advanced: sandboxes, chroot, and containers (readings)
> More isolation: crypto devices, SGX, TrustZone (readings)
> Software security and vulnerabilities (Section 3.4 and readings) [2 classes]
> Malware (Chapter 4) [2 classes]
> Network security I (Chapter 5) [2 classes]
> Network security II (Chapter 6) [2 classes]
> Web security (Chapter 7) [2 classes]
> Cryptography (Sections 8.1-8.4) [2 classes]
> Database and email security (Sections 10.1-10.2)
> Social networks - security models and privacy (Section 10.5 and readings)
> Case study: Voting machines (readings)

Teaching Methods and Assignments: This class will meet for two 75-minute periods per week, and class meetings will consist of a combination of lecture/presentation, discussion, and in-class exercises. Students must to come to class prepared, having done all required readings, and are expected to participate in in-class activities. Grades are based on student work done in assignments and exams.

Assignments: For practice and to demonstrate abilities, students will be given 5-6 assignments over the course of the semester (approximately every two weeks, adjusted to exclude exam weeks). Assignments

will include some written problems and some hands-on security exercises. Hands-on exercises will utilize either a shared Linux server or virtual machines that can be downloaded for use on students' own computers.

Exams: There will be one mid-term exam and one final exam, which will assess student's mastery of learning outcomes 1-7 in an exam setting. Problems will be similar to written homework problems, but will be somewhat simplified from the homework assignments, due to time limitations of testing.

Graduate Students: Graduate students will be given a handout on security research practices and standards, and sample research papers to read and critique during the first 2/3 of the semester. For the final 1/3 of the semester, graduate students will select a topic from the research literature according their interests, locate appropriate references, and write a thorough research summary and critique. This addresses the graduate student learning outcome 8.

Evaluation and Grading: Each student work product will be graded, and the student's final grade will be determined by assigning each category of work a weighted score according to the following distribution:

Undergraduates	
Assignments	50%
Mid-term Exam	20%
Final Exam	30%

Graduate Students	
Assignments	45%
Mid-term Exam	15%
Final Exam	25%
Research Readings/Project	15%

Academic Integrity: Students are expected to be familiar with and abide by the UNCG Academic Integrity Policy, which is online at `http://academicintegrity.uncg.edu/`

Assignments in this class are for individual work, unless explicitly stated otherwise. General concepts and material covered in the class may be discussed with other students or in study groups, but specific assigned problems should not be discussed and all submitted work should be entirely your own. If you use external references (including web sites, books, etc.) in preparing your solutions, you should clearly mark the part(s) of your solution influenced by these references and provide clear citations to the source of information you are using. Sharing your own work is a serious violation of academic integrity, and if homework is copied then *both* the person who actually did the work and the person who copied it will be punished. Any incidents of academic dishonesty will be handled strictly, resulting in either a zero on the assignment or an F in the class, depending on the severity of the incident, and incidents will be reported to the UNCG Office of Student Rights and Responsibilities.

Attendance Policy: Attendance will not be taken in class, and is voluntary; however, all students are responsible for everything done or said in class (this can include changes in assignments, due dates, etc.). Note that this is a very dynamic class, with regular in-class activities, so it is highly unlikely that a student who regularly misses classes will be successful in the course. If attendance becomes a problem, then in-class exercises may be collected and included as part of the assignment portion of the grade.

The university allows for a limited number of excused absences for religious observances. Students who plan to take such an absence should notify the instructor at least two weeks in advance so that accommodations can be made (see the late work policy below). It is the student's responsibility to obtain notes from another student if they miss class.

Late Policy and Makeup Exams: Assignments are due at the beginning of class on the due date, and may be turned in up to 7 calendar days late with a 25% late penalty. Students with planned absences, whether for university events, religious observance, or other reason, are expected to make arrangements with the instructor to turn in assignments or take exams before the scheduled date of the assignment or test. No assignment will be accepted more than 7 calendar days after the original due date!

Exam/test dates will be announced at least two weeks in advance, and may be made up only if it was missed due to an extreme emergency and arrangements are made before the exam date. Exams (including the final) may not be taken early or late due to personal travel plans.

In-class Behavior: When you are in class you should be focused on the class, and you should act in a professional and mature manner. During class there should be no eating, drinking, e-cigarettes, cellphone use, non-class related laptop, or anything else that does not pertain to the class activities. Any distracting items may be confiscated at the discretion of the instructor.

ADA Statement: UNCG seeks to comply fully with the Americans with Disabilities Act (ADA). Students requesting accommodations based on a disability must be registered with the Office of Accessibility Resources and Services located in 215 Elliott University Center: (336) 334-5440 (or on the web at `http://oars.uncg.edu`).

University Closings: If university facilities are closed due to flu outbreak or other emergencies, it does not mean that classes are canceled. In such an event, please check the class web page and Blackboard site for information about if and how the class will proceed.

Commercial note-taking services: Selling class notes for commercial gain or purchasing such class notes in this or any other course at UNCG is a violation of the University's Copyright Policy and of the Student Code of Conduct. Sharing notes for studying purposes, or borrowing notes to make up for absences, without commercial gain, are not violations.