The University of North Carolina at Greensboro | Handout 1
CSC 495/693: Software Security | January 11, 2022
Prof. Stephen R. Tate

CSC 495/693 Class Information and Syllabus

Instructor: Stephen R. Tate (Steve)
Lectures: Tues/Thurs 3:30-4:45, in Petty 217
Office: Petty 157
Office Hours: Tues/Thurs 1:45-3:15 (or by appointment), in-person or virtual – see below
E-mail: `srtate@uncg.edu`

Note regarding Spring 2022: While the COVID-19 pandemic is ongoing, the wide availability of safe and effective vaccines provide hope that we will be able to hold a somewhat normal, in-person semester. In particular, this class is planned as a fully in-person class, and you are expected to attend lectures in the assigned classroom. If the COVID situation worsens and in-person meetings cannot be held safely, then we will revert to on-line meetings. However, this is *not* a hybrid class, and all students will have the same experience – either all in-person or all online.

Office hours are available both in-person (in my office, Petty room 157) or online via Zoom teleconferencing software – a link to the Zoom office hours room is in Canvas. Please be aware that my office is a small enclosed space, and if you are uncomfortable with that you can connect via Zoom. Also, due to my small office space, down a short but narrow side-corridor, you are asked to wait in the more open main hallway if I am meeting with someone else (in person or virtually). If I'm talking to someone online when you arrive, make sure I see you and then I will come out to the main hallway to let you know when I'm available after the online session. I can only meet with one person at a time during office hours.

For us to be able to get back to normal, everyone must do their part to protect both their own health and the health of others. More information COVID-specific class protections and policies is in the university COVID statement at the end of the syllabus.

Class Web Page: `https://www.uncg.edu/cmp/faculty/srtate/495.s22/`

Description: This course will cover common vulnerabilities in software, and how software bugs can have serious security consequences. We will consider buffer overflows, return-oriented programming, stack smashing, integer overflow, SQL injection, cross-site scripting, and other classes of vulnerabilities. We will also look at techniques for avoiding these vulnerabilities, ranging from good programming practices to the use of static analysis and other tools. The course will be experimental, with students locating, exploiting, and fixing vulnerabilities throughout the semester. Examples will include constructed examples for teaching as well as vulnerabilities in real world software with hundreds of thousands of lines of code.

Prerequisites: Grade of C or better in CSC 330 is required. Programming experience with C or C++ (such as from CSC 362 or CSC 339) is strongly recommended.

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

1. identify common types of software-based security vulnerabilities,
2. describe the consequences of common types of software-based security vulnerabilities,
3. classify common patterns of attacks and vulnerabilities,
4. use and create "proof-of-concept" exploits for vulnerabilities,
5. use tools to improve robustness of software,
6. discuss fundamental computational limitations of automated software analysis.

Textbook and Readings: There is no textbook for this course. The course will be organized around readings that are freely available on the Internet, taken largely (but not exclusively!) from the following sources:

- Software Security: Principles, Policies, and Protection by Mathias Payer (book PDF is a link on this page)
- MITRE Common Weakness Enumeration (CWE) documentation
- The Open Web Application Security Project (OWASP) documentation
- MITRE Common Attack Pattern Enumeration and Classification
- CERT secure coding standards

In addition, students will read several research papers to gain familiarity with current research standards and trends in software security. Graduate students will read additional and more advanced research papers. Readings will be posted and updated regularly in the Schedule section of the class web site.

Technology and Programming Languages: This class is all about vulnerabilities in software, and as such we will look at a *lot* of code in this class. Activities will involve working with Linux systems and with a wide variety of programming languages, including assembly language, C, C++, JavaScript, PHP, and more. Students are not expected to know all of these languages currently, but should be proficient programmers with good knowledge of assembly language (as seen in CSC 261) and Java (as seen in the CSC 130-330 sequence). All of the other languages that we will look at use the same basic concepts, structure, and syntax, and as upper-level computer science students you should be able follow examples in these languages and pick up enough of the basics to do the exercises required for the class.

This class will make heavy use of a Linux environment and Linux tools. Prior experience with Linux is helpful but not necessary. Students without prior experience are expected to learn the necessary skills on their own.

Ethics and Responsible Disclosure: Students should not, under any circumstance, test for vulnerabilities in deployed systems that they do not have permission to test in such a manner. Virtual machines and the lab facilities available to students are more than adequate for setting up test systems and allowing for experimentation. Any vulnerabilities discovered in software systems should be reported using standards of responsible disclosure. This will be discussed in class, and if there are any questions about experimentation or disclosure you should speak with the instructor.

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 are expected to be prepared and actively participate in class, having done all required readings in advance. Classes will be dynamic and somewhat unpredictable, often going through code without powerpoint slides or other notes, so students are expected to take notes. Grades are based on student work done in assignments and exams.

Assignments: For practice and to demonstrate abilities, students will be given 5-7 assignments over the course of the semester (approximately every two weeks, adjusted to exclude exam weeks). Assignments may include problems that involve analyzing existing code for security vulnerabilities (either manually or using analysis tools), writing code to explore the consequences of vulnerabilities, and patching software to remove vulnerabilities. Homeworks may also include written questions that involve discussion or analysis in a more general setting (not code-based).

Exams: There will be one mid-term exam (tentatively scheduled for Thursday, March 3) and one final exam on Tuesday, May 3, 3:30–6:30.

Graduate Students: In addition to the work described above, graduate students will be given approximately three research papers during the semester to read and report on with a 1-2 page written summary and critique. In addition, graduate students will complete a project based on current research in a software security topic of their own choosing, with the result typically being a 10-15 page survey paper summarizing research related to that topic.

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:

For undergraduates:

Category	
Assignments	60%
Mid-term Exam	15%
Final Exam	25%

Letter Grade Assignment				
	[87.5 , 89.5) = B+	[77.5 , 79.5) = C+	[67.5 , 69.5) = D+	[0 , 59.5) = F
[91.5 , ∞) = A	[81.5 , 87.5) = B	[71.5 , 77.5) = C	[61.5 , 67.5) = D	
[89.5 , 91.5) = A-	[79.5 , 81.5) = B-	[69.5 , 71.5) = C-	[59.5 , 61.5) = D-	

For graduate students:

Category	
Assignments	54%
Mid-term Exam	13.5%
Final Exam	22.5%
Research Project	10%

Letter Grade Assignment			
	[87.5 , 89.5) = B+	[77.5 , 79.5) = C+	[0 , 71.5) = F
[91.5 , ∞) = A	[81.5 , 87.5) = B	[71.5 , 77.5) = C	
[89.5 , 91.5) = A-	[79.5 , 81.5) = B-		

Note that Canvas uses the same letter grade assignment for undergraduate and graduate students, even though there are no passing grades below a C for graduate students. Any graduate student with a C- or below in Canvas will receive an F in the class.

Academic Integrity: Students are expected to be familiar with and abide by the UNCG Academic Integrity Policy, which is online at `https://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 websites, 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. Significant incidents will be reported to the UNCG Office of Student Rights and Responsibilities. Note that the Department of Computer Science maintains records of all academic integrity incidents, and multiple violations, even in different classes or semesters, will always result in reporting to the university and serious penalties.

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.). Given the dynamic nature of this class, 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 used 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 (the instructor will not provide notes).

Late Policy and Makeup Exams: Assignments are due at 11:59PM 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! For graduate/honors students completing the research project, it may not be submitted late.

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 may not be taken early or late due to personal travel plans.

Given the COVID-19 situation, I will be flexible and accommodating within reason, but students *must* inform me of any complications in advance of due dates.

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 use, or anything else that does not pertain to the class activities. Any distracting items may be confiscated at the discretion of the instructor. Students are required to abide by UNCG COVID policies (see below), and will be asked to leave if there is an issue.

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 `https://oars.uncg.edu`). Note that if you require testing accommodations you must make arrangements more than one week before any exam.

University COVID-19 Policy: As we return for Spring 2022, all students, faculty, and staff are required to uphold UNCG's culture of care by actively engaging in behaviors that limit the spread of COVID-19. These actions include, but are not limited to:

- Following face-covering guidelines
- Engaging in proper hand washing hygiene
- Self-monitoring for symptoms of COVID-19
- Staying home when ill
- Complying with directions from health care providers or public health officials to quarantine or isolate if ill or exposed to someone who is ill
- Completing a self-report when experiencing COVID-19 symptoms, testing positive for COVID-19, or being identified as a close contact of someone who has tested positive
- Staying informed about the University's policies and announcements via the COVID-19 website

Instructors will have seating charts for their classes. These are important for facilitating contact tracing should there be a confirmed case of COVID-19. Students must sit in their assigned seats at every class meeting. Students may move their chairs in class to facilitate group work, as long as instructors keep seating chart records. Students should not eat or drink during class time.

A limited number of disposable masks will be available in classrooms for students who have forgotten theirs. Face coverings are also available for purchase in the UNCG Campus Bookstore. Students who do not follow masking requirements will be asked to put on a face covering or leave the classroom to retrieve one and only return when they follow the basic standards of safety and care for the UNCG community. Once students have a face covering, they are permitted to re-enter a class already in progress. Repeated issues may result in conduct action. The course policies regarding attendance and academics remain in effect for partial or full absence from class due to lack of adherence with face covering and other requirements.

For instances where the Office of Accessibility Resources and Services (OARS) has granted accommodations regarding wearing face coverings, students should contact their instructors to develop appropriate alternatives to class participation and/or activities as needed.

Health and well-Being: Health and well-being impact learning and academic success. Throughout your time in the university, you may experience a range of concerns that can cause barriers to your academic success. These might include illnesses, strained relationships, anxiety, high levels of stress, alcohol or drug problems, feeling down, or loss of motivation. Student Health Services and the Counseling Center can help with these or other issues you may experience. You can learn about the free, confidential mental health services available on campus by calling 336-334-5874, visiting the website at `https://shs.uncg.edu/` or visiting the Anna M. Gove Student Health Center at 107 Gray Drive. For undergraduate or graduate students in recovery from alcohol and other drug addiction, the Spartan Recovery Program (SRP) offers recovery support services. You can learn more about recovery and recovery support services by visiting `https://shs.uncg.edu/srp` or reaching out to recovery@uncg.edu

Elasticity Statement: It is the intention of the instructor that this syllabus and course calendar will be followed as outlined, however, as the need arises there may be adjustments to the syllabus and calendar. In such cases, the instructor will notify the students in class and via e-mail with an updated syllabus and calendar within a reasonable timeframe to allow students to adjust as needed.