CSC 495/680 — Spring 2015 — Class Information and Syllabus

Instructor: Stephen R. Tate (Steve)
Lectures: Tues/Thurs 2:00-3:15, Petty 227
Office: Petty 166
Office Hours: Tues/Thurs 10:30-12:00, or by appointment
Phone: 336-256-1033
E-mail: srtate@uncg.edu

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

Prerequisites: *Required*: CSC 330. *Recommended*: CSC 339 or other experience with C, C++, or another language that supports raw pointers.

Course 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.

Student Learning Outcomes: Upon successful completion of this course students will 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 tools to improve robustness of software,
5. perform a basic security audit of a software system, and
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:

- 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 "Readings" section of the class web site.

Technology and Programming Languages: 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, C++, and Java. None of the other languages that we will use are based on radically different concepts, 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. No prior experience with Linux is necessary, but students without prior experience are expected to learn the necessary skills on their own.

Class-Selected "Target Programs": In order to gain experience auditing software for security vulnerabilities, the class will select (through an in-class discussion the first week of the semester) 2-5 open source software projects that will be used throughout the semester. As we discuss different types of vulnerabilities, students will be assigned the task of checking for each of these types of vulnerabilities in the target software.

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. 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 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.

In-Class Exercises: Some class days will include in-class activities that can involve working through problems or completing tasks on a worksheet. Students must complete these activities during the class period in which they are distributed.

Assignments: There will be approximately four homework assignments during the semester. 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 on Thursday, March 5, during the regular class period. The final exam will be held according to the official UNCG Final Exam Schedule, which lists the time for this exam as Thursday, April 30, 3:30-6:30. The format of the final exam for this class might be unconventional: more information will be provided at least two weeks before the end of classes.

Graduate Students: In addition to the work described above, graduate students will be given approximately four 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:

Table 1: Undergraduates

Assignments and Class Exercises	45%
Mid-term Exam	25%
Final Exam	30%

Table 2: Graduate Students

Assignments and Class Exercises	40%
Mid-term Exam	20%
Final Exam	25%
Research Reports Project	15%

Topic Outline and Calendar: Since this class has not been offered before, the timing and precise list of topics may change during the semester. For the current and planned list of topics and dates, please see the "Schedule" area of the class web site.

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 appropriate UNCG office.

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, based on a collection of readings rather than a structured textbook, so it is highly unlikely that a student who regularly misses classes will be successful in the course. 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 http://ods.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.