CScD 437, Secure Coding Principles
Syllabus

Course Description

This course will introduce you to a variety of topics you need to be concerned with when writing code. We will examine concepts that apply to programming "in the large" as well as specifics on things like buffer overflow. The course assumes at least one year of programming in Java (if you are fluent in C++ you can probably survive the class as well, but references will be made to Java throughout the quarter). We will look at a good deal of C and C++ code, so some familiarity with those languages is desirable. We will have written assignments, coding assignments, a midterm project, and a final project. For the final project, teams will present their findings to the rest of the class in a formal presentation complete with slides, code samples, etc.

An APPROXIMATE sequence of the topics that we will cover this quarter, and their correspondence to the textbook, are listed in the table below. I will likely supplement material from the book a good deal -- any supplements will be posted to the website (of course!)

Chapter (24 DS), class notes, much supplemental material as well via website links	Topics
Notes, links	Code Security Basics, Reflections on Trusting Trust by Ken Thompson, Self-Reproducing Program Terminology
Notes, links	Regular Expressions, Threat Modeling with STRIDE, Threat Ranking with DREAD
5, 6, and 7	Buffer Overrun, Format String Problems, Integer Overflow, C Programming Language fundamental ‘flaws’
1, 10, and 11	SQL Injection, Command Injection, Failure to Handle Errors, and Security Touchpoints
2, 3, and 4	Cross Site Scripting, Cross Site Request Forgery, Magic URLs,
19, 20, and 21, notes, links	No Passwords in Code, Weak Passwords, Crypto Basics, How to Properly Work with Passwords, Failing to Protect Data, Weak random numbers, improper use of cryptography
Notes, links	Program testing to discover bugs, Fuzz Testing, American Fuzzy Lop fuzz tester,
12 and 13	Information Leakage, Race Conditions

14, 15, 16	Poor Usability, Not Updating Easily, Executing with too much privilege
22, 23, and 24	Failing to protect network traffic, improper use of PKI, trusting network name resolution
	Canonicalization issues, bonus topics time permitting

Instructor Information

Instructor	Tom Capaul, MS
Office	303 CEB
Office Hours	MWF 11:00-11:50, TTh 9-9:50 or by appointment
Email	tcapaul@ewu.edu
Phone	359-7092
Fax	359-2215
Class home page	http://penguin.ewu.edu/cscd437

Required Texts

24 Deadly Sins of Software Security, ISBN: 978-0-07-162675-0 , by Howard, LeBlanc, and Viega

Grading

Homework: (including any written homework) will count 30%.
Quizzes/Exams: 40%
Final Project: 30%

NOTE: Project presentations will be the last week of class.

Final exam will be Wednesday, December 10 from 9-12

FINAL NUMERICAL GRADE CALCULATION:

You will need at least a 95% to earn a 4.0 in this class. For each percent below 95, one tenth of a grade point will be subtracted.

NOTE: The instructor retains the right to adjust grade scale based on performance of class as a whole (which is to your benefit).

Policies

- ***Lectures***. You are expected to attend every class session. Please do not use my office hours as a substitute for attending lectures. In addition, you are expected to read the appropriate sections of the text before each class period. Classroom activities will complement, not necessarily duplicate, the text. If you are unsure as to what will be covered next, please ask at the end of the class period.
- ***Preparation.*** You are expected to read material from the chapter in the book that is being discussed in class AHEAD of time (see the syllabus for a list of topics and chapters). Examples given in class and by the authors should be confirmed by the student at home to guarantee complete understanding of the subject.
- ***Homework***. Homework assignments will be in the form of programming projects, group projects, and written assignments. Homework is due at the specified time typically to Blackboard. An assignment that is 1 day late incurs a 20% penalty. Assignments will NOT be accepted for points beyond one day late without discussion with the instructor! Note that all assignments must be turned in (in working order) before quarter's end to be eligible to earn a passing grade (2.5).
- ***Participation and Attendance***. You are not graded on participation and attendance directly, however regular attendance and participation are expected. At quarter's end, regular attendance and participation will positively influence your final grade.
- ***Professional Behavior***. All students are expected to act in accordance with the *ACM Standards for Professional Behavior*. Should you have any questions about appropriate behavior, please talk with me before submitting your work. Instances of poor ethical conduct will be dealt with SEVERELY. You may be expelled from the university, expelled from the degree program, or given a 0.0 in the class.
- ***Incompletes***. Incompletes will NOT be granted except under extreme circumstances. They will not be granted in cases where you were simply unable to keep up with the workload. Requests for an incomplete must be submitted prior to finals week and is subject to the following catalog restriction: "PASSING work/progress (2.5 or above) must be demonstrated through three weeks prior to the end of the term."
- ***Disclaimer.*** The instructor reserves the right to make changes to these policies as necessary. You will ALWAYS be informed of these changes in class.