Computer Science CS 4/53401 Secure Programming
Call Numbers 13096 and 13105
SYLLABUS
Fall, 2014

Time and Place: Monday and Wednesday at 2:15-3:30 in room 108 Smith Hall

Instructor: Michael Rothstein, 268 MSB, phone 330-672-9065. Email address: rothstei at cs.kent.edu or mrothste at kent.edu; please do not send email to both addresses with the same topic; I'll simply get it twice and delete it as spam.

Web address: http://www.cs.kent.edu/ rothstei

Office Hours:

Monday, Wednesday 12-2; meetings permitting MW 3:30-5.

Also, you can always send email with questions and/or to set up an appointment. Usual turnaround will be a few hours during the day. Email use is to be preferred over voicemail, which will not be checked as often.

Textbook: (All of the following are available on Safari Books online).
Chess, B and West, J, *Secure Programming with Static Analysis*, Addison-Wesley, 2007, ISBN-10: 0321424778, ISBN-13: 978-0321424778.
Additional bibliography:

1. Seacord, Robert C. *Secure Coding in C and C++*, 2nd Ed. Addison-Wesley, 2013, ISBN 978-0-321-82213-0; 0-321-82213-7
2. Seacord, Robert C. *The CERT C Secure Coding Standard*, Pearson Education, 2009, ISBN-10: 0-321-56321-2; ISBN 13: 978-0-321-56321-7.
3. Howard, Michael and LeBlanc, David *Writing Secure Code*, 2nd Ed., Microsoft Press, 2003, ISBN 0-7356-1722-8.
4. Howard, Michael and LeBlanc, David *Writing Secure Code for Windows Vista*, Microsoft Press, 2007.
5. Viega, John and Messier, Matt, *Secure Programming Cookbook for C and C++*, O'Reilly & Associates, 2003, ISBN 0-596-00394-3.
6. Rice, David, *Geekonomics, The real cost of Insecure Software*, Addison-Wesley, 2008. ISBN-10 0-321-47789-8; ISBN-13: 978-0-321-47789-7
7. Klein, Tobias, *A Bug Hunter's Diary* A Guided Tour Through the Wilds of Software Security, no starch press, 2011, ISBN: 978-1-59327-385-9, 1-59327-385-1

In addition, the following websites will be helpful:

1. Wikipedia entry "List of tools for static code anlysis": http://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis.

2. The website for the cppcheck static analysis tool: http://cppcheck.sourceforge.net/ or http://sourceforge.net/projects/cppcheck/ (for the source, necesary for use on a MAC or Linux)
3. The Google checker for google coding style: http://google-styleguide.googlecode.com/svn/trunk/cpplint/ together with the document describing the style: http://google-styleguide.googlecode.com/svn/trunk/cppguide.xml
4. Splint Home page Splint is a C static analysis tool.
5. Secure Programming for Linux and Unix HOWTO
6. 2010 CWE/SANS Top 25 Most Dangerous Software Errors
7. CERT Site on Secure Programming
8. Splint Home page

There are other sites, feel free to google "Secure Programming" or "Secure Coding".

Material to be covered: The goal of this course is to learn how we can avoid the pitfalls of insecure programming and how to check for them through static analysis. That was the goal behind the choice of textbook, even though it is somewhat of an "ad book". The goals trascend the package described in the book. Even though the book tries to sell a particular static analysis tool, we will use other tools. Having said that, we will pretty much follow the book verbatim.

Prerequisites: CS 33001 (CS II) and Junior Standing.

Attendance policy By initiative of the Provost of the University, I have been charged with keeping full attendance records, at least for the first ten weeks of the semester. Though I will not compute these records into your final averages, when I assign letter grades, I will give you a slightly better grade if you have a better attendance record. Notwithstanding the above, if you are absent, there may be material created, either spontaneously or in response to questions, and covered in the classroom; often there will not be any written notes of this material, so it might be a good idea to team up with somebody who keeps good notes to make sure you have all the material covered. Some of this material may show up in an exam.

Read the text and bibliography. Only general reading assignments will be given. The tests will be take home. This means that I expect you to do some research in order to answer the questions.

The class will mostly cover material in the same order as the text book, there may be exceptions however. It is the student's responsibility to maintain an awareness of the material in the text that is currently being covered. Ask the instructor if you are unsure of the material currently being covered.

The syllabus may be changed during the semester if necesary: changes will be announced in class; they might also show up on the instructor's website.

Class disruptions Disruptions should be kept to a minimum; these include (in increasing order of seriousness):

1. Early departure (if announced and done discreetly: please sit near the door so that as few people as possible notice.)
2. Late arrival
3. Use of electronic devices or other devices which may interfere with your or other student's participation. Laptops are acceptable for taking notes, however, please sit in the last row of the room so that your screen does not distract/block other students.
4. Conversation among students.
5. Aiding and/or abetting these or any other student's disruptive behaviors.

Guidelines pertaining to class disruptions are outlined in the University Rules and Regulations, available at the University Website.

Grading: Your grade will be based on one midterm, one final, programming assignments, and a "class participation grade", based on the number of relevant questions and comments: specially good questions or catching my mistakes get extra points. The weights are:

Class Participation	10%
Midterm (Due October 15 at 10 PM)	25%
Final (Due Monday December 8 at 10 PM)	25%
Programming Assignments.	40%

The final will be comprehensive.

Test make-up policy: I will need signed documentation to verify *each* individual absence in order to provide make-ups; only university accepted reasons will be honored.

Grading scale: I will assign number grades during the session and only convert them to letter grades when I turn them in at the end of the session. No decision can be made regarding a conversion table until the very last minute due to such imponderables as test difficulty, class attendance and participation, etc. which will influence the grade. However, I guarantee the following, worst case, table:

97-100	will convert into an A
94-96	will convert into at least an A-
91-93	will convert into at least a B+
88-90	will convert into at least a B
85-87	will convert into at least a B-
82-84	will convert into at least a C+
79-81	will convert into at least a C
76-78	will convert into at least a C-
73-75	will convert into at least a D+
66-72	will convert into at least a D

Special accommodations for Students with Disabilities: University policy 3342-3-01.3 requires that students with disabilities be provided reasonable accommodations to ensure their equal access to course content. If you have a documented disability and require accommodations, please contact the instructor at the beginning of the semester to make arrangements for necessary classroom adjustments. Please note, you must first verify your eligibility for these through Student Accessibility Services (contact 330-672-3391 or visit:
http://www.kent.edu/sas for more information on registration procedures).

Registration Requirement : The official registration deadline for this course is September 07, 2014. University policy requires all students to be officially registered in each class they are attending. Students who are not officially registered for a course by published deadlines should not be attending classes and will not receive credit or a grade for the course. Each student must confirm enrollment by checking his/her class schedule (using Student Tools in FlashFast) prior to the deadline indicated. Registration errors must be corrected prior to the deadline.

The course withdrawal deadline is November 2, 2014.

On cheating, plagiarism and other unethical behavior You are encouraged to discuss class problems with other students but required to work independently of anybody else except the instructors and/or tutor, unless otherwise indicated. Midterms and the final are required to be individual work at all times. Copying other people's work, allowing your work to be copied (even inadvertently!) and plagiarizing work will not be tolerated and will be dealt with according to University regulations, as described in the University policy register on cheating

Notes:

1. By default, the penalty for cheating in this course is an "F" in the course.
2. University regulations require me to notify Student Conduct in case of violations.
3. Cooperation is just as bad as the deed itself: so, deciding which of two is the original is a non-issue: both are equally guilty.