Computer Science CS 4/53401 Secure Programming
Call Numbers 13643 and 13653
SYLLABUS
Fall, 2013

Time and Place: Monday and Wednesday at 12:30-1:45 in room 228 MCS aka MSB;

Instructor: Michael Rothstein, 268 MSB, phone 330-672-9065. Email address: rothstei at cs.kent.edu (The address mrothste at kent.edu will not work too well because I do not check it as often; for a quicker response, the first address is recommended.)

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

Office Hours:

Monday, Wednesday 2:00-3:30 (often extended to 5:00 PM)

Also, you can always send email to cs.kent.edu 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).
Seacord, Robert C. *Secure Coding in C and C++*, 2nd ed, Addison Wesley, 2013. ISBN 978-0-321-82213-0; 0-321-82213-7.

Additional bibliography:

1. Seacord, Robert C. *The CERT(R) C Secure Coding Standard*, Addison Wesley, 2009, ISBN-10: 0-321-56321-2; ISBN 13: 978-0-321-56321-7.
2. Howard, Michael and LeBlanc, David *Writing Secure Code*, 2nd Ed., Microsoft Press, 2003, ISBN 0-7356-1722-8.
3. Howard, Michael and LeBlanc, David *Writing Secure Code for Windows Vista*, Microsoft Press, 2007.
4. Viega, John and Messier, Matt, *Secure Programming Cookbook for C and C++*, O'Reilly & Associates, 2003, ISBN 0-596-00394-3.
5. 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
6. 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. Dan Wheeler's web-site includes many resources including a Secure Programming for Linux and Unix HOWTO
6. 2010 CWE/SANS Top 25 Most Dangerous Software Errors
7. CERT Site on Secure Programming

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. After covering an introduction, we will start by studying some of the particulars of using cppcheck, and will continue with the topics outlined in the book.

Prerequisites: C in CS 23001 (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.

Tentative Material Schedule (Subject to change without notice)

Week	Dates	Material
1	Aug 25, 27	Introductory material: why secure coding? Static Analysis
2	Sep 3	(Sep 1 is Labour Day) Installing and using cppcheck
3	Sep 8, 10	Strings, manipulation errors, vlunerabilities and exploits
4	Sep 15, 17	Mitigation strategies; string handling functions, Runtime protection strategies, some vulnerabilities.
5	Sep 22, 24	Subverting Pointers. Memory management and MM problems
6	Sep 29, Oct 2	(cont) MM problems; mitigation. Integer mismanagement
7	Oct 7, 9	Continue Integer problems, vulnerabilities, mitigation
8	Oct 14, 16	Formatted Output problems, mitigation.
9	Oct 21, 23	Concurrency problems.
10	Oct 28, 30	File I/O problems.
11	Nov 4, 6	More on File I/O, some recommended practices
12	Nov 13	(Nov 11 is Veteran's Day) Continue recommended Practices
13	Nov 18, 20	Remaining time reserved for slack, selected topics, review
14	Nov 25	Nov 27 starts the Thanksgiving Recess
15	Dec 2, 4	
	Dec 9 to 13	Finals Week

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 such a way 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 Wednesday October 16 at 10 PM)	20%
Final (Due Friday Dec 13 at 12:30 PM)	30%
Programming Assignments	40%

Please note that the final will be comprehensive and is due in the early afternoon of the Friday of Finals week..

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. Since tests are take-home and handled over email, the reason for a make-up must be strong.

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

I usually slide this scale downwards by at least 2-3 points.

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 8, 2013. 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 3 2013.

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 instructor and/or tutor, unless otherwise indicated. Midterms 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 Policies and Procedures, a condensed version of which is attached. 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.

ADMINISTRATIVE POLICY AND PROCEDURES REGARDING STUDENT CHEATING AND PLAGIARISM

Condensed Version

For complete policy and procedure go to www.kent.edu/policyregister 3342-3-01.8. (search the kent.edu website).

Cheating and plagiarism constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted and will be applied.

The university affirms that acts of cheating and plagiarism by students constitute a subversion of the goals of the institution, have no place in the university and are serious offenses to academic goals and objectives, as well as to the rights of fellow students.

"Cheat" means to intentionally misrepresent the source, nature, or other conditions of academic work so as to accrue undeserved credit, or to cooperate with someone else in such misrepresentation. **Cheating includes, but is not limited to**:

1. Obtaining or retaining partial or whole copies of examinations, tests or quizzes before these are distributed for student use;
2. Using notes, textbooks or other information in examinations, tests and quizzes, except as expressly permitted;
3. Obtaining confidential information about examinations, tests or quizzes other than that released by the instructor;
4. Securing, giving or exchanging information during examinations;
5. Presenting data or other material gathered by another person or group as one's own;
6. Falsifying experimental data or information;
7. Having another person take one's place for any academic performance without the specific knowledge and permission of the instructor;
8. Cooperating with another to do one or more of the above;
9. Using a substantial portion of a piece of work previously submitted for another course or program to meet the requirements of the present course or program without notifying the instructor to whom the work is presented; and
10. Presenting falsified information in order to postpone or avoid examinations, tests, quizzes, or other academic work.

"Plagiarize" means to take and present as one's own a material portion of the ideas or words of another or to present as one's own an idea or work derived from an existing source without full and proper credit to the source of the ideas, words, or works. As defined, plagiarize includes, but is not limited to:

a. The copying of words, sentences and paragraphs directly from the work of another without proper credit;

b. The copying of illustrations, figures, photographs, drawings, models, or other visual and nonverbal materials, including recordings of another without proper credit; and

c. The presentation of work prepared by another in final or draft form as one's own without citing the source, such as the use of purchased research papers.

Academic Sanctions

The following academic sanctions are provided by this rule for offenses of cheating or plagiarism. Kent campus instructors shall notify the department chairperson and the student conduct office each time a sanction is imposed. Regional campus instructors shall notify the regional campus dean and the student conduct officer each time a sanction is imposed. Regional campus student conduct officer shall notify the Kent student conduct office each time a sanction is imposed by a regional campus Instructor. **The following academic sanctions are provided by this rule for offenses of cheating or plagiarism. In those cases the instructor may**:

1. Refuse to accept the work for credit; or

2. Assign a grade of "F" or zero for the project, test, paper, examination or other work in which the cheating or plagiarism took place; or

3. Assign a grade of "F" for the course in which the cheating or plagiarism took place; and/or;

4. Recommend to the department chair or regional campus dean that further action specified in the rule be taken. The department chairperson or regional campus dean shall determine whether or not to forward to the academic dean or to the vice president for the extended university a recommendation for further sanction under this rule.