Computer Science CS 4/5/6/79995 Design of Secure Operating Systems
Section 021/020
Call Numbers 14678, 14680, 10736, 10754 respectively.

SYLLABUS

Summer 2012

Time and Place: Mondays, Tuesdays and Thursdays, 6:00 to 7:40 in room 121 MSB However, this may change...

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: Mondays, Tuesdays and Thursdays 4:00-5:30 and after class. 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: Jaeger, Trent, *Operating System Security*, Morgan & Claypool Publishers, 2008, ISBN 9781598292121 (paperbook), 9781598292138 (ebook)

Additional bibliography:

- Rueda, Sandra, Vijayakumar, Hayawardh and Jaeger, Trent, *Analysis of virtual machine system policies* in Proceedings of the 14th ACM symposium of Access control models and technologies (SACMAT 09), 2009, Stresa, Italy, pp 227-236
- Amer, Suhair Hafez and Hamilton,Jr., John A. *Understanding security architecture*, in Proceedings of the 2008 Spring simulation multiconference (SpringSim '08), 2008, Ottawa, Canada, pp 335-342
- Chaudhuri, Avik *Language-based security on Android* in Proceedings of the ACM SIGPLAN Fourth Workshop on Programming Languages and Analysis for Security (PLAS '09), 2009, Dublin, Ireland, pp 1-7
- William Enck, Machigar Ongtang and Patrick McDaniel *Understanding Android Security*, IEEE Security and Privacy, Vol 7, 2009,pp 50-57
- Anonymous (Untitled) http://www.ratliff.net/blog/2007/10/03/security-design-principles/ (A critique on selinux)
- Bishop, Matt, *Computer Security: Art and Science*, Addison-Wesley, 2003, ISBN 0201-440997, Chapter 13.

Course Goals: The goal of this course is a study of the challenges involved in the design and implementation of a secure operating system.

Prerequisite: For 5/6/79995, Graduate Standing; For 49995: C or better in CS II.

Grading: For 4/59995 students: Your grade will be based on one midterm, one final, and a 5 page term paper due at the end of the term on a preapproved relevant topic of the student's choosing. The weights are:

Midterm (Due June 29)	30%
Final (Due July 27)	30%
Term paper	40%

For 6/79995 students: Your grade will be based on one midterm, one final, and a class presentation at the end of the term on a relevant topic of the student's choosing, with instructor approval. The weights are:

Midterm (Due June 29)	30%
Final (Due July 27)	30%
Presentation	40%

The midterm and final will be take-home and done electronically; notice that the material in Graduate Student's presentations is fair game for the final also.

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

Topics: We will cover the following topics:

- Introduction to the topic of Security in Operating Systems (1 hour)
- Principles of Information Security (1 hour)
- Access Control Fundamentals (2 hours)
- Generalized Security Architectures (3 hours)
- Case study: Multics, security architecture, analysis and vulnerabilities. (3 hours)
- Case study: Analysis of security in Unix and problems with the design of its security architecture (2 hours)
- Case study: Analysis of security in Windows and problems with its security(1 hour)
- Verifiable Security Goals (3 hours)
- Case studies: Security Kernels: SCOMP design and analysis, GEMSOS design.(2 hours)
- Difficulties with securing Commercial Operating Systems (Retrofitting Security) (3 hours)
- Case study: Solaris Trusted Extensions (2 hours)
- Case study: Linux Security Modules architecture (2 hours)
- Case study: SELinux design and analysis (2 hours)
- Problems and issues in Secure Capability Systems (2 hours)
- Security issues in Virtual Machine Systems; evaluation (2 hours)
- Security issues in sandboxing designs: design and analysis of Android (2 hours)
- Space for student talks (12 hours)

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 Accessability 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 06/10/2012. 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 last withdrawal date for this course is 07/8/2012.

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. 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.(available at http://www.kent.edu/policyreg/chap3/3-01-8.cfm)

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.

For complete policy and procedure go to www.kent.edu/policyregister 3342-3-01.8, available at http://www.kent.edu/policyreg/chap3/3-01-8.cfm.