Computer Science CS 6/79995 ST: Design of Secure Operating Systems
Section 010
Call Numbers 21322 and 21323 respectively.
SYLLABUS
Spring 2015

Time and Place: Monday, Wednesday, 12:30-1:45 013 Cunningham 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 mail to both at once; I'll simply get it twice and think it is spam! (Substitute @ for " at ").

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

Office Hours: Monday, Wednesday, 11:00-12:00 and 3:45-5:00 PM

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
- Stallings, William and Brown, Lawrie, *Computer Security : Principles and Practice* 3d ed. Pearson Education Inc. (publishing as Prentice Hall), 2015, ISBN 978-0-13-377392-7
- 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: Graduate Standing.

Grading: 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:

Pop Quizzes and class participation	10%
Midterm (February 25)	30%
Final (10:15-12:30, May 7)	30%
Presentation	30%

The final will be comprehensive.

The midterm and final will be closed book; however, a small (like 20 sheets) amount of paper will be allowed for consultation. Notice that the material in the presentations can also be tested in the final. The presentation topic has to be chosen by March 21; failure to do so will be an automatic F in the course; note also that the drop date is March 22.

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 January 25, 2015. 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 March 22, 2015.

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. For more information, see the University policy statement 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.