CSC 589 Class Information and Syllabus

COURSE NUMBER:	CSC 589
COURSE TITLE:	Trusted Computing and Security Models
CREDITS:	3:3
PREREQUISITES:	*Required:* CSC 250, CSC 330, and either STA 271 or STA 290. *Strongly recommended:* CSC 553, CSC 555. Or permission of the instructor.

FOR WHOM PLANNED: Elective course for upper-level undergraduate students or graduate students.

INSTRUCTOR INFORMATION:

Name:	Steve Tate
Office:	Bryan Building 320 (Petty 166 after Feb 11)
Office Hours:	Tues/Thurs 3:00 – 5:00
Phone:	336-256-1033
E-mail:	`srtate@uncg.edu`

CATALOG DESCRIPTION: Introduction to trusted computing concepts and formal security models. Stresses development of critical reasoning skills needed to assess and contribute to current research in this and other areas of security.

STUDENT LEARNING OUTCOMES: Upon successful completion of this course students will be able to

- describe concepts of trusted computing, including variations created by the Trusted Computing Group, Microsoft, and Intel;
- apply trusted computing concepts to design simple applications;
- describe foundational principles of modern cryptography;
- discuss how cryptographic models relate to real-world security;
- describe common complexity assumptions for cryptography;
- construct simple reduction-based security proofs;
- discuss current research issues in trusted computing;
- *For Graduate Students:* present a complete, non-trivial cryptographic result using technical writing standards typical of research papers.

TEACHING METHODS AND ASSIGNMENTS FOR ACHIEVING LEARNING OUTCOMES: The primary method of instruction will be 150-minute per week for lecture and discussion, with students responsible for completing assigned readings before class. Meetings will be held one evening per week, with a 20 minute break in the middle. Assignments will require students to summarize and apply covered concepts, and will include writing proofs that apply the discussed cryptographic models. *Each assignment will have a "graduate student only" problem that explores the concepts covered in more depth.* There will be opportunities for students to gain exposure outside the university by publishing their writing to a web site dedicated to trusted computing issues, although this is not required. Each student will be required to make a technical presentation of approximately 30 minutes at some point during the semester. As an introduction to research standards, writing and presentations are expected to adhere to standards of the field, and an overview of relevant guidelines will be discussed in class. Note that written material will be graded based on quality of writing as well as technical content.

EVALUATION AND GRADING: Each student activity will contribute to the final grade in the class according to the following percentages.

Assignments	55 points
Presentation	10 points
Attendance	10 points
Take-home final or project	25 points

REQUIRED TEXTS/READING/REFERENCES: The following book is required, and covers the basics of trusted computing and some applications:

- Chris Mitchell (editor). *Trusted Computing*, IEE, Herts, UK, 2005. ISBN 0-86341-535-3.

In addition, readings on formal security models and rigorous security proofs will be required, drawn primarily from the following on-line reference:

- Mihir Bellare and Phillip Rogaway. *Introduction to Modern Cryptography*, Lecture notes from a course at UCSD (2005), freely available on the Internet at http://www.cs.ucsd.edu/~mihir/cse207/classnotes.html

Some additional readings from current research literature will be covered, and will be distributed in class.

TOPICAL OUTLINE/CALENDAR: The topics in this class follow two lines: trusted computing technology/concepts and security/cryptographic models, and at the end of the course these two threads will be brought together. In addition, some time will be given to general topics to introduce students to standards used in the computer science and computer security research communities.

"Lectures" are approximately 75 minutes in length (half an evening class), and topics from the broad categories will be mixed to keep the long evening classes from being too uniform and monotonous. The following list of topics is a best-plan list, but is not ordered — specific topics will be chosen and announced at least one week prior to the lectures so that students can read the appropriate material.

Trusted Computing Topics

Topic	***Reading***
Trusted Computing: Introduction and Concepts	Mitchell Ch 1–2
Trusted Computing Technology Components	Mitchell Ch 3.1–3.3
Trusted Computing Technology Systems	Mitchell Ch 3.4–3.9
Microsoft's "Next Generation Secure Computing Base"	Mitchell Ch 4
Privacy in Trusted Computing and DAA	Mitchell Ch 5
App: Single Sign-on	Mitchell Ch 6
App: Secure delivery of conditional access applications	Mitchell Ch 7
App: Securing peer-to-peer networks using trusted computing	Mitchell Ch 10

Security Models Topics

Intro to modern crypto and security models/arguments	Bellare/Rogaway Ch 1
Pseudorandom Functions - 2 lectures	Bellare/Rogaway Ch 3
Symmetric Encryption - 2 lectures	Bellare/Rogaway Ch 4
Hash Functions	Bellare/Rogaway Ch 5
Message Authentication	Bellare/Rogaway Ch 6
Asymmetric Encryption - 2 lectures	Bellare/Rogaway Ch 8
Oblivious Transfer and Secure Function Evaluation	Handout
The Random Oracle Model	Handout

Bringing It All Together

Virtual Monotonic Counters and Applications	Handout
TPMs for instantiating random oracles	Handout
TPMs for non-interative OT and SFE	Handout

General Research Topics

Writing for research and tools (LaTeX, BibTeX, ...)	Handouts
Research/Technical Presentations	Handouts

ACADEMIC INTEGRITY POLICY: Students are expected to abide by the UNCG Academic Integrity Policy, which is online at `http://academicintegrity.uncg.edu/`

Students will be reviewing and summarizing current research throughout the course. Issues of scientific attribution and plagiarism will be discussed in class and students are expected to follow appropriate practices in this regard.

Students are required to sign the Academic Integrity Pledge on any work they do. The pledge is the statement "I have abided by the UNCG Academic Integrity Policy on this assignment."

ATTENDANCE POLICY: The topics covered in this class can involve very subtle issues, so the in-class discussions are vital to learning the material. Students are expected to attend class, but perfection is not required. Unless there is a compelling excuse, such as an extended illness, students will lose 2 points from the "attendance" portion of their grade for every day missed after the second absence.

FINAL EXAMINATION: Undergraduate students will be given a take-home final, where they are required to write some brief technical summaries as well as some proofs. *Graduate students will complete a research project in place of the final, where the project involves writing up a topic in a complete and coherent way and with some depth.*

Final exam/projects due: Thursday, May 8, 5:30 PM

ADDITIONAL REQUIREMENTS:

Laptop/Cellphone Policy: Laptops can be both a benefit and a distraction in a classroom. While many students benefit from taking notes using a laptop, or having access to outside class-related resources during class, other students cannot resist the temptation of checking e-mail, chatting, or even playing games during class time. This class has a strict "no non-class related use" rule for laptops — if you are found violating this policy, then your in-class laptop privileges will be taken away. Cellphones are a distraction for everyone, and should be turned off during class. If there is a special situation where you need to have your phone on for a particular day, please let the instructor know the situation before class.

Late Policy and Makeup Exams: Assignments are due at the beginning of class on the due date, and may be turned in up to 7 calendars days late with a 25% late penalty. *No assignment will be accepted more than 7 calendar days after the original due date!*

The final take-home exam (for undergraduates) and final project paper (for graduate students) are due at the university-scheduled final exam date and time, and will not be accepted late.

ADA STATEMENT: UNCG seeks to comply fully with the Americans with Disabilities Act (ADA). Students requesting accommodations based on a disability must be registered with the Office of Disability Services located in 215 Elliott University Center: (336) 334–5440.