The University of North Carolina at Greensboro — Handout 6
CSC 589: Trusted Computing and Security Models — March 26, 2008
Prof. Stephen R. Tate

Graduate Project Information

In this class, graduate students are required to complete a research-oriented project. Specific suggestions and ideas for topics are given in Blackboard, and this documents describes expectations and due dates. The final turned-in project will be a paper with significant technical depth, and I would estimate that the length of the reports will be around 12 pages (single spaced, 11 or 12 point font, with reasonable margins). Projects can be at various levels or styles, described below.

Good: You can satisfy the requirements for this class by reading existing research papers and presenting the results in a report, in your own words. In addition to text describing the results, this means that proofs should be re-written and justifications made in your own words and style. To earn a grade better than a "B" from this type of project, it must be very well done, and it must present something new rather than just be a restatement of published results. For example, a project could take different solutions to the same (or very similar) problem and do a more careful comparison and analysis of the benefits and drawbacks of each method than is available in the published papers.

Better: The next level up would be a paper which takes existing and known results but which have incomplete presentations in the published literature. There are an unfortunately high number of papers in cryptography in which techniques are developed but the proofs are either given in incomplete form (usually indicated in the paper by having a "proof sketch" for a theorem rather than a "proof"), or are missing entirely with a statement that the complete proof will appear in the "full paper" (which may or may not ever be published). Writing up one of these results with complete proofs would be a very nice project — your paper needs to still be your own writing (this is not just "filling in the holes" of someone else's paper!).

Best: The best possible project is something that presents new results along with a fairly complete presentation of justifications and proofs. Since this class is a mix of discussion of a new technology (trusted computing) and cryptographic algorithm design and analysis, one approach to this is to ask questions like "how does the presence of a trusted platform module affect possibilities for protocols for problem X?" I don't expect ground-breaking results here, but I want to see some creativity and innovation on techniques as well as rigorous justifications.

Important dates:

- *April 10* - General project selection and identification of sources. E-mail to me your topic selection, a brief (few sentences) description of what you'll cover in your report, and a list of papers you're using as references.
- *April 24* - Progress report due. Significant progress is expected by this date, including an overall outline and a several-page overview of topics covered (like the "Introduction" section to a paper).
- *May 8, 5:30 PM* - Final report due