Project Information

As described on the class syllabus, graduate students will do a final research-oriented project in lieu of the final exam. From the syllabus:

Graduate students will not have a final exam, but each graduate student must do a research project in which they explore an area of research (and a minimum of three research papers) and write a report of approximately 10 pages summarizing research in that area.

In the past 5 years there has been a significant amount of research in trusted computing and other hardware-enhanced security techniques, and this should be the basis of your project and report. The three research papers you choose should be peer-reviewed research papers — not web pages or product documentation or anything like that. At least two papers should be specifically about trusted computing, but the third could be a general research background paper. For example, if you wanted to do a project on Private Information Retrieval, one paper could be one of the initial papers (from the early to mid 1990’s) that describes the problem and solutions that pre-date trusted computing.

The project will have various “milestones,” with the following due dates:

*Project topic selection*: Monday, November 15

*References selected and paper outline*: Monday, November 22

*Draft submitted for feedback (optional)*: Friday, December 3

*Final report due*: Friday, December 10 (7:00 PM)

You should email the final report to me by the due date — please email me a PDF (not a DOC or other format).

What follows are some possible project topics. This is by no means an exhaustive list, and you should feel free to look for other topics and to browse research literature for other topics that interest you. *(Note: The printed version of this handout gives bibliographic references that allow you to find the paper with a little bit of work — the online version of this handout has links to these papers when possible, although for some links you need to be on the UNCG campus so that you can use the library’s subscription to these publications.)*
Other hardware-enhanced security architectures

Trusted computing technology, as defined by the Trusted Computing Group, is not the only way to enhance security through hardware additions or modifications. Surveying some alternative approaches, highlighting strengths and weaknesses of different approaches, could be an interesting project. Some of the papers you might consider are the following:


Private Information Retrieval

Consider a data provider that allows you to make queries against the data it holds, but the user would like to make queries in a private manner so that the server cannot tell exactly what data has been retrieved. For example, you could have a medical database that patients could query, but patient queries have full privacy. At first this seems to be impossible (or at least very difficult), but trusted hardware provides some interesting possibilities. Some of the work in this area is in the following papers:


Handout 6: Project Information


**Grid or cloud computing or virtualization**

Using computing resources across the Internet is a hot topic these days, whether it is to increase the computing power available by aggregating computing resources together (grid computing) or simply making use of hardware managed remotely (cloud computing). There are clearly some interesting security and privacy issues when your computing resources are not under your control, and trusted computing technology can be used to increase security and privacy in such a situation. Some papers along these lines are the following:


**Attestation issues**

Attestation, or proving that a system is running particular software or has particular properties, is a very important feature of trusted computing. As we discussed in class, using secure boot and a static root of trust leads to a highly complex system. Chipset and processor support for a dynamic root of trust is one solution, but there are other interpretations (sometimes built on a dynamic root of trust) of attestation that are interesting to consider. The following papers are examples of work in this area:


**Operating system support/issues**

What sort of support from the operating system is required for trusted computing applications? That is the question explored in the following research papers:

