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:

- Benjie Chen and Robert Morris. "Certifying program execution with secure processors." In *Proceedings of the 9th conference on Hot Topics in Operating Systems - Volume 9*, pages 133–138, 2003.

- Taeho Kgil, Laura Falk, and Trevor Mudge. "ChipLock: support for secure microarchitectures." *SIGARCH Computer Architecture News*, 33(1):134–143, 2005.

- David Lie, Chandramohan A. Thekkath, Mark Mitchell, Patrick Lincoln, Dan Boneh, John Mitchell, and Mark Horowitz. "Architectural support for copy and tamper resistant software." *SIGARCH Computer Architecture News*, 28(5):168–177, 2000.

- David Lie, John Mitchell, Chandramohan A. Thekkath, and Mark Horowitz. "Specifying and verifying hardware for Tamper-Resistant software." In *IEEE Symposium on Security and Privacy*, page 166, 2003.

- G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, and Srinivas Devadas. Efficient memory integrity verification and encryption for secure processors. In *Proceedings of the 36th Annual IEEE/ACM International Symposium on Microarchitecture*, page 339, 2003.

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:

- A. Iliev and S.W. Smith. Protecting client privacy with trusted computing at the server. *IEEE Security and Privacy Magazine*, 3(2):20–28, 2005.

- A. Iliev and S. Smith, "Private Information Storage with Logarithmic-space Secure Hardware," Information Security Management, Education, and Privacy, Kluwer, 2004, pp. 201–216.

- Sean W. Smith and D. Safford. Practical server privacy with secure coprocessors. *IBM Systems Journal*, 40(3):683–695, 2001.

- Peter Williams, Radu Sion, and Bogdan Carbunar. Building castles out of mud: practical access pattern privacy and correctness on untrusted storage. In *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS)*, pages 139–148, 2008.

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:

- Stefan Berger, Ramón Cáceres, Kenneth A. Goldman, Ronald Perez, Reiner Sailer, and Leendert van Doorn. vTPM: virtualizing the trusted platform module. In *Proceedings of the 15th USENIX Security Symposium*, 2006.

- Juan Du, Wei Wei, Xiaohui Gu, and Ting Yu. Towards secure dataflow processing in open distributed systems. In *Proceedings of the 2009 ACM Workshop on Scalable Trusted Computing*, pages 67–72, 2009.

- M. Lorch, J. Basney, and D. Kafura. A hardware-secured credential repository for grid PKIs. In *Proceedings of the 2004 IEEE International Symposium on Cluster Computing and the Grid*, pages 640–647, 2004.

- Wenbo Mao, Fei Yan, and Chunrun Chen. Daonity: grid security with behaviour conformity from trusted computing. In *Proceedings of the ACM Workshop on Scalable Trusted Computing*, pages 43–46, 2006.

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:

- Fabrizio Baiardi, Diego Cilea, Daniele Sgandurra, and Francesco Ceccarelli. Measuring semantic integrity for remote attestation. In *Proceedings of the 2nd International Conference on Trusted Computing*, pages 81–100, 2009.

- Liqun Chen, Rainer Landfermann, Hans Löhr, Markus Rohe, Ahmad-Reza Sadeghi, and Christian Stüble. A protocol for property-based attestation. In *Proceedings of the first ACM Workshop on Scalable Trusted Computing*, pages 7–16, 2006.

- Yasuharu Katsuno, Yuji Watanabe, Sachiko Yoshihama, Takuya Mishina, and Michiharu Kudoh. Layering negotiations for flexible attestation. In *Proceedings of the First ACM Workshop on Scalable Trusted Computing*, pages 17–20, 2006.

- Ahmad-Reza Sadeghi and Christian Stüble. Property-based attestation for computing platforms: caring about properties, not mechanisms. In *Proceedings of the 2004 Workshop on New Security Paradigms*, pages 67–77, 2004.

- Frederic Stumpf, Andreas Fuchs, Stefan Katzenbeisser, and Claudia Eckert. Improving the scalability of platform attestation. In *Proceedings of the 3rd ACM Workshop on Scalable Trusted Computing*, pages 1–10, 2008.

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:

- Tal Garfinkel, Mendel Rosenblum, and Dan Boneh. Flexible OS support and applications for trusted computing. In *Proceedings of the 9th Conference on Hot Topics in Operating Systems*, pages 25–25, 2003.

- Jason F. Reid and William J. Caelli. DRM, trusted computing and operating system architecture. In *Proceedings of the 2005 Australasian Workshop on Grid Computing and E-research*, pages 127–136, 2005.

- Alan Shieh, Dan Williams, Emin Gün Sirer, and Fred B. Schneider. Nexus: a new operating system for trustworthy computing. In *Proceedings of the ACM Symposium on Operating Systems Principles*, pages 1–9, 2005.