Graduate Project Information and Possible Topics

The purpose of this handout is to give some information on project guidelines and deadlines, as well as list some possible project topics. Projects require a final written report on the chosen topic, and you are encouraged to consider including personal experimentation as well as paper reading/review. Here are the parts and milestones for the project:

Project Selection (Due Tuesday, April 12): You should look over the potential project topics below, do some initial reading to see what you find interesting and what you can get sufficient material for. Keep in mind the topic criteria below. All I need by April 12 is a project topic/title, but if you want to give me more information about what you plan on investigating I will give you feedback on that.

Progress Report (Due Thursday, April 21): By the time of the progress report your project should be pretty well investigated, meaning you've collected and read all of the reference papers, and thought through what you're going to write about in your report. You should turn in a progress report that contains *a basic introduction section to your project report (this should describe the topic you're studying at a high level and describe what you will be giving giving details on), as well as an outline of your report and a list of bibliographic references that you plan on using*.

It is very important that you use an acceptable format for your references. All references must include the following: Authors, paper title, where it appeared, date (just the year is good enough), and page numbers. For journal papers, also include volume and issue number information. Here are two sample formatted references (one conference and one journal) — please follow this format as closely as you can!

[1] J. Li, M. Sung, J. Xu, and L. Li. "Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Theoretical Foundation," *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 115–129, 2004.

[2] L. Buttyan, J. Hubaux, and S. Capkun, "A Formal Model of Rational Exchange and Its Application to the Analysis of Syverson's Protocol," *Journal of Computer Security*, Vol. 12, No. 3/4, pp. 551-588, 2004.

The progress report is graded, and counts for 25% of your overall project grade. However, the most important part of the progress report is that I will review it quickly and make comments and suggestions on the report that you can pick up from me in my office Friday, April 22 (or later). This is where I tell you if you are going in the right direction,

and give suggestions for things you should include for a good final report. *Feel free to to turn in your progress report early, and I will get feedback to you as soon as I can.*

Complete Project (Due Thursday, April 28, at the final exam): This is when the full report is due.

Topic/Depth Guidelines: This is intended to be a *research* oriented project, not a technology description. A topic which describes a product or system but without any significant underlying question is not appropriate. For instance, a report on IPsec isn't appropriate, but a report on how security protocols are analyzed using IPsec as an example would be good.

For any topic, multiple references should be used — no project should depend on a single reference source. At least two references should be "respectable references" (peer-reviewed journal or conference papers — not Joe Schmo's web page).

Keep in mind that this is a computer science class, and technical depth is important. Formulas, theorems, proofs, and analysis are certainly important and should be included as appropriate. Since this is a research topic, it's also important to think about (and write about) what questions are left unanswered by the current research that should be investigated ("open problems"). As for the length of the paper, something around 8–10 pages (11 or 12 point font, single spaced) should be enough to cover the important parts. There's no need to try to write about everything that's out there related to your topic.

Remember that the writing should be entirely your own — it is not acceptable to copy text from a paper or the web. My general advice to people is this: Investigate and read as much about the topic as you can until you really understand it, taking some light notes. Then you should know the topic well enough to put aside all your references, and do the writing *without looking* at the original material. That ensures that the writing is coming from *you* and not the reference material.

Possible Topics

The following topics are simply suggestions. If you know of some other topic you'd like to investigate for your project, talk to me about it — if it's of a sufficient level and appropriately relevant to the topics of this class, then I'll probably approve it. However, note that it should be research-oriented (in other words, it should be addressing a question, not summarizing a product or technology). If one of these topics intrigues you, but you're not sure where to start looking, just ask and I'll give you some pointers.

- Cryptographic techniques for digital rights management (DRM), such as digital watermarking, application in SDMI, etc.
- Cloud computing issues: outsourced storage and computation
- Provable security techniques (model checking, spi-calculus, etc.)

- Privacy, anonymous publishing, and anonymous communication (Tor, remailer, ...)
- Security protocols for peer-to-peer networks
- Factoring and discrete logarithm algorithms (for the mathematically adventurous!)
- Cryptanalysis
- Side-channel attacks
- Cryptography for embedded devices or sensor networks
- Contracting protocols (fair exchange, etc.)
- Alternative signature schemes (threshold signatures, undeniable signatures, group signatures, ...)
- Quantum cryptography or computing issues: key exchange or factoring
- Bitcoin and other cryptocurrencies
- Kleptography and backdoors in cryptosystems
- Privacy-preserving computations
- Recent work on Oblivious RAMs
- Secure or verifiable implementations
- Attacks on SSL/TLS
- Randomness and pseudo-random generation

The following are some of the leading security conferences, and provide excellent material (there are, of course, other good quality conferences and journals, but these are the best place to start).

- *IEEE Symposium on Security and Privacy*
- *ACM Conference on Computer and Communications Security*
- *ISOC/IEEE Symposium on Network and Distributed System Security (NDSS)*
- *USENIX Security Symposium*
- *CRYPTO: International Cryptology Conference*
- *Annual Computer Security Applications Conference (ACSAC)*