Cryptography and Communication Security **Final Projects**
CS 6750 Fall 2009 (Pucella)

Description

Your final project for the course should be a study of 2–3 articles on a topic of your choice related to cryptography and communication security. These articles should be technical papers from security conferences, or technical reports from security researchers. The intent is to investigate topics that we did not have time to look at in class, or look at something more specifically and in more depth that we have done in class.

The final product of your project should be 10-pages paper[1] summarizing and synthesizing the articles you have studied.

I will also ask you to give a 20-minutes presentation in class about your work, followed by a 5-minutes question period. These presentations are scheduled on Thursday, December 11, and Friday, December 12, both from 18h00 to 21h00.

These projects are all individual projects.

Grading will be based on the quality and technical depth of the produced paper, as well as the quality of the presentation. I will ask to see a draft of the presentation about a week before the presentation itself, so we can ensure some quality control.

Project Topics

I would like to see your proposals of what to investigate by November 15. Please feel free to get in touch with me if you want to check whether what you have chosen makes sense, or if you have difficulty finding articles about what it is that you want to investigate. If you're really stuck, here are some suggestions:

- There has been a widely reported security flaw recently about the latest SSH protocol. Describe the SSH protocol (really, suite of protocols), especially the renegotiation protocol, and describe the flaw that has been discovered, and the way people are currently thinking of remedying it.

[1] 11pt font with reasonable margins, and single spaced

- Describe Kerberos (the protocol from MIT), the various versions, its uses, the motivations underlying the design, the attacks people have reported, the security analyses people have performed.
- Cryptosystems based on braid groups, a form of algebraic systems used in knot theory.
- The use of correspondence assertions to characterize authentication.
- The use of theorem proving for proving properties of security protocols .
- Protocols for secure online elections.
- Security protocols for IPv6.
- Security protocols for wireless networks.
- Security issues in online auctions.
- Information flow: definitions and applications.

If you need more details about any of the above, feel free to email me.

I will also post more suggestions on the web site in the next few days. In the meantime, do look for something that you have an interest in.

Time Line

November 15	Project selection
December 6	Deadline for draft of presentation
December 11, 12	Presentations
December 14	Deadline for written report