Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 17
October 23, 1997

Problem Set 7

This problem set is due on *Thursday, November 7, 1997* at the end of class. Please inform the TA by *November 30, 1997* via e-mail if you're having problems completing it.

Problem 7-1. Term Project

Find up to three other people to work with on a Term Project. The project should deal with some topic related to the class, and can range from a design project to an implementation of a scheme. However, it should be a project appropriate to your group size.

For the homework problem, please submit (only one for each team):

1. The names of the people in the team.
2. A short description of what your paper will be about.

Some past papers are available on the web at:

- `http://web.mit.edu/6.857/OldStuff/Fall95/www/term-papers.html`
- `http://web.mit.edu/6.857/OldStuff/Fall96/www/home.html`

Also here follows a short list of past papers, to help get some ideas:

- *Implementation Notes for a Platform for Internet Content Selection System*
- *SHTTP and SSL*
- *ElGamal Based Threshold Signature*
- *A Study of Secure Sockets Layer*
- *Steganography*
- *Providing Software Services on the WWW Securely*
- *Java Security*
- *Poking Holes in Athena*
- *Security Requirements for Uniform Resource Identifiers*
- *Alladin: An Authentication System Based on MD5*
- *Verification of the iKP Family of Protocols*
- *Internet Security Protocols*
- *Copyright in the Information Age: A survey of the legal and technical aspects*
- *DCE and Security*

- *PayMe! : A customer-oriented efficient micropayment scheme*
- *Designing Secure Programs in Java*

Finally, if you need more ideas, go through the class web page and follow some of the links. There are a lot of things happening in the world of security today, and many of those can be the basis for an interesting term project. If you need more help and ideas, please get in touch with the TA (during office hours for example), and he may be able to give you some, or help you formalize others.