1 Introduction

This class is CSE 291, distributed systems security. The lectures will go over both secure systems design as well as cryptographic protocols, both critical elements in successfully building secure distributed systems.

2 Background

I expect that you know some basic concepts from operating systems, complexity theory, and number theory — what is an OS kernel, an RPC, what is a reduction, how to do basic big-num modulo arithmetic, etc. I'll do a quickie reminder overview of all this, but mostly I'll be building up from there; if you don't have this background, come talk to me and we can see about covering some of this in more depth.

3 Administrivia

The texts for this course are

- Practical Unix & Internet Security, and
- Applied Cryptography, 2nd Ed.

The office hours for this course are Mondays and Wednesdays 2pm to 3pm, but you should feel free to drop by at other times. If you come by outside of the official times without first making an appointment, I reserve the right to ask you to come back later if I am busy.

4 Discussion Topics

I'm flexible about the exact topics to be discussed. You should feel free to suggest an area that interests you.

The class will start with a programming contest. The contest is open to the entire CSE community, but it is security related. During the first real class, we will discuss the problem and the associated security concerns, and the discussion will lead us to many aspects of distributed systems security. The prize is still to be determined.