abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

The Internet is an indispensable part of our information society, and yet its basic foundations remain vulnerable to simple attacks, and one area that remains especially susceptible to attack is routing. There have been increasing efforts in the networking community to incorporate security into current routing protocols, and secure Internet measurement is necessary to inform any routing protocol. In this talk we will show how to use theoretical tools to give a rigorous treatment of this security problem. We believe our work shows that rigorous techniques, and even tools for negative results such as reducing to one-way functions or black-box separations, can have an immediate impact on the study of security problems of real-world importance.

We describe two definitions for this problem: fault detection (FD) where the honest parties only want to know if the packets they sent were dropped or modified or not, and fault localization (FL) where the honest parties want to know in addition where exactly their packets were modified or dropped. Besides traditional per-packet definitions where we want to know the fate of every packet, we also propose *statistical* definitions that reduce the communication and storage overhead of protocols yet retain useful security properties. We will sketch constructions of schemes that satisfy our security definitions and have desirable practical properties.

Next, we show the negative results implied by our definitions. In particular, we can show the necessity of keys, cryptography, and storage in any secure FD or FL scheme. We will describe in detail the proof of our result that any secure black-box construction of a FL protocol requires cryptography to be performed at each nodes. This result uses a novel application of the black-box separation technique of Impagliazzo-Rudich and the learning algorithm of

Naor-Rothblum.

Finally, time permitting we will show a composition technique used to construct secure FL protocols out of secure FD protocols.

This is joint work with Sharon Goldberg, Boaz Barak, and Jennifer Rexford.