abstract

SPECIAL LECTURE
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Mathematics has contributed immensely to the development of secure cryptosystems and protocols. Yet our networks are terribly insecure, and we are constantly threatened with the prospect of imminent doom. Furthermore, even though such warnings have been common for the last two decades, the situation has not gotten any better. On the other hand, there have not been any great disasters either. To understand this paradox, we need to consider not just the technology, but also the economics, sociology, and psychology of security. Any technology that requires care from millions of people, most very unsophisticated in technical issues, will be limited in its effectiveness by what those people are willing and able to do. This imposes strong limits on what formal mathematical methods can accomplish, and suggests that we will have to put up with the equivalent of baling wire and chewing gum, and to live on the edge of intolerable frustration.