



UMass Lowell Computer Science Colloquium Announcement

Speaker: Dr. Agnes Hui Chan
College of Computer and Information Science
Northeastern University

Date & Time: May 7, 2003 (Wed), 3:00pm-4:00pm

Place: Olsen 311. **Refreshments are served at 2:45pm**

Authentication and Key Exchange Protocols for Wireless Imbalanced Networks

Low-power wireless devices, such as Personal Device Assistants (PDAs) and cellular phones, are characterized by their limited memory capacity, low computational power, small and monochrome screens. In addition, the wireless environment is limited in bandwidth and is subject to erratic changes such as weather, terrain and external interference. These constraints have prevented a simple migration of cryptographic protocols that are widely adopted in wire-line networks to wireless networks for authentication and security. Due to the mobility of wireless devices, authentication of both the user (client) and the base station (server) becomes paramount importance. In this talk, we present our efficient mutual authentication and key exchange protocols between a low-power wireless device and a powerful base station. The aim is to reduce the computational burden on the client while maintaining similar level of security and scalability as expected by users. We will discuss both device-oriented authentication as well as password based user-oriented authentication.

Brief bio: Dr. Agnes Chan is the Associate Dean and the Graduate Director of the College of Computer and Information Science at Northeastern University. She received the A.B. degree in mathematics from Smith College and the Ph.D. degree in mathematics from Ohio State University. She joined the faculty at Northeastern University in 1976.

Her research interests include cryptography, communication security and resource constrained network problems. Under her direction, Northeastern University has been designated by NSA as a Center of Excellence in Information Assurance Education.

Colloquium Coordinator: *Jie Wang*, wang@cs.uml.edu. Website: <http://www.cs.uml.edu/~wang/colloquia/>