ISTeC

Colorado State University

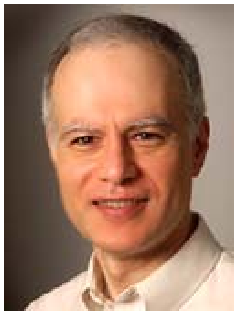
ISTeC.ColoState.edu

Knowledge to Go Places

The Information Science and Technology Center ...at Colorado State University

Colorado State University's Information Science and Technology Center (ISTeC)

presents two lectures by



Dr. Mikhail Atallah

Distinguished Professor of Computer Science,
Computer Science Department, Purdue University

ISTeC Distinguished Lecture

in conjunction with the Computer Science Department Seminar Series

"Security Issues in Collaborative Computing"

Monday, October 30, 2006
Reception: 10:30 a.m. to 11:00 a.m.
Shepardson room 114
Lecture: 11:00 a.m. to 12:00 noon
Shepardson room 118

●

Joint Electrical and Computer Engineering Department and Computer Science Department

sponsored by ISTeC

"Privacy-Preserving Trust Negotiations"

Tuesday, October 31, 2006
Lecture: 12:30 p.m. to 1:30 p.m.
University Services Building room 310B

ABSTRACTS

“Security Issues in Collaborative Computing”

Even though collaborative computing can yield substantial economic, social, and scientific benefits, a serious impediment to fully achieving that potential is a reluctance to share data, for fear of losing control over its subsequent dissemination and usage. An organization’s most valuable and useful data is often proprietary/confidential, or the law may forbid its disclosure or regulate the form of that disclosure. We survey security technologies that mitigate this problem, and discuss research directions towards enforcing the data owner’s approved purposes on the data used in collaborative computing. These include techniques for cooperatively computing answers without revealing any private data, even though the computed answers depend on all the participants' private data. They also include computational outsourcing, where computationally weak entities use computationally powerful entities to carry out intensive computing tasks without revealing to them either their inputs or the computed outputs.

“Privacy-Preserving Trust Negotiations”

In an open environment such as the Internet, the decision to collaborate with a stranger (e.g., by granting access to a resource) is often based on the characteristics (rather than the identity) of the requester, via digital credentials: Access is granted if Alice’s credentials satisfy Bob’s access policy. Both credentials and access policies can be sensitive, and the literature contains many scenarios in which it is desirable to carry out such trust negotiations in a privacy-preserving manner, i.e., so as minimize the disclosure of credentials and/or of access policies. Elegant solutions were previously proposed for achieving various degrees of privacy-preservation through minimal disclosure. In this talk, we present protocols that protect both sensitive credentials and policies. That is, Alice gets the resource only if she satisfies the policy, Bob does not learn anything about Alice’s credentials (not even whether Alice got access or not), and Alice learns neither Bob’s policy structure nor which credentials caused her to gain access. The protocols can handle the situation when each credential has its own access policy associated with it (e.g., “a top-secret clearance credential can only be used when the other party is a government employee and has a top-secret clearance”). Note that there can be a deep nesting of dependencies between credential policies, and that there can be (possibly overlapping) policy cycles of these dependencies.

SPEAKER BIOGRAPHY

Mikhail (“Mike”) Atallah (http://www.cs.purdue.edu/people/mja) obtained the Ph.D. in 1982 from the Johns Hopkins University and joined the Computer Sciences Department at Purdue University, where he currently holds the rank of Distinguished Professor. His current research interests are in information security (in particular, secure protocols, software security, and watermarking). He received a Presidential Young Investigator Award from the National Science Foundation in 1985. A Fellow of the IEEE, he has served on the editorial boards of many top journals (including SIAM Journal on Computing, JPDC, IEETC, etc), and on the Program Committees of many top conferences and workshops (including PODS, SODA, SoCG, WWW, PET, DRM, SACMAT, etc). He has been Keynote and Invited Speaker at many national and international meetings, and a speaker in the Distinguished Colloquium Series of six top Computer Science Departments. He was selected in 1999 as one of the best teachers in the history of Purdue University and included in Purdue’s Book of Great Teachers, a permanent wall display of Purdue’s best teachers past and present. He is a co-founder of Arxan Technologies Incorporated.

To arrange a meeting with the speaker, please contact MaryAnn Stroub at (970) 491- 2708 or mstroub@engr.colostate.edu

ISTeC (Information Science and Technology Center) is a university-wide organization for promoting, facilitating, and enhancing CSU’s research, education, and outreach activities pertaining to the design and innovative application of computer, communication, and information systems. For more information please see ISTeC.ColoState.edu.