The Information Science & Technology Center

ISTeC.ColoState.edu

Colorado State University's
Information Science and Technology Center (ISTeC)
presents <u>two</u> lectures by

Dr. Radia Perlman

Sun Fellow, Sun Microsystems

ISTeC Distinguished Lecture

"Myths, Missteps, and Folklore of Network Protocol Design"

Tuesday, March 25, 2008
Reception: 8:30 – 9:00 a.m.
Lecture: 9:00 – 10:00 a.m.
Location: Lory Student Center Room 216

•

Computer Science BMAC Distinguished Lecture

"Data: Making It Be There When You Want It and Go Away When You Want It Gone"

Monday, March 24, 2008
Lecture: 11:00 – 12:00 a.m.
Location: Lory Student Center Room 222

ABSTRACT

“Myths, Missteps, and Folklore of Network Protocol Design”

Network protocol design is not a nice, clean science, where what gets deployed is the best possible design. Instead, designs are influenced by issues such as politics, general confusion, and backward compatibility. Statements get made, and repeated, until it never occurs to anyone to question whether they're true. Mistakes get made, and rather than backing up and fixing them, kludges are introduced to make things sort of work. This talk discusses how some of the odder things we live with (e.g., bridges) came about, and interesting bad protocol designs that have been standardized and/or deployed. It also discusses **“**obvious**”** protocol design issues that somehow get overlooked, such as designing for future evolution, and ability to change parameters, node by node, without disrupting a network. The talk is intended to be provocative, making people question the things they have always taken for granted. It is also a plea to teach the subject in a way that empowers students to think critically about protocol designs, rather than simply memorizing the current standards in order to implement them.

“Data: Making It Be There When You Want It and Go Away When You Want It Gone”

In order not to lose data, copies should be kept in lots of locations. That makes it difficult to really delete the data, since the backup copies can be stolen or copied. The obvious solution is to encrypt the data, and then discard the keys of data that is to be destroyed. However, reliably keeping, then reliably destroying all copies of deleted keys has the same problem. This talk describes a system that supports three types of assured delete: expiration time known at file creation, on-demand deletion of individual files, and custom keys for classes of data. This system is easy and inexpensive to manage and involves only trivial performance overhead over a traditional encrypted file system.

SPEAKER BIOGRAPHY

Radia Perlman (http://research.sun.com/people/mybio.php?uid=28941) is a SUN Fellow at SUN Microsystems, working on network and security protocols. She invented many of the basic algorithms that make today's network infrastructure robust and scalable. She is famous for her invention of the spanning tree protocol which is fundamental to the operation of network bridges. It allows network bridges to connect networks without loops. She also made large contributions to many other areas of network design and standardization such as link state protocols. In routing, her contributions include making link state protocols robust and scalable, simplifying the IP multicast model, and routing with policies. Her doctoral thesis at MIT addressed the issue of routing in the presence of malicious network failures and forms the basis for most of the work in the area. She has made contributions in diverse areas such as network security, credentials download, strong password protocols, analysis and redesign of IPsec's IKE protocols, PKI models, efficient certificate revocation, and distributed authorization. Her current research interests include assured delete, making large networks robust against Byzantine failures, and replacing bridges / switches with technology that is upwardly compatible, but more robust, flexible, and scalable.

She is author of **“**Interconnections: Bridges, Routers, Switches, and Internetworking Protocols,**”** and coauthor of **“**Network Security: Private Communication in a Public World,**”** which are widely used both as textbooks in universities and for engineers to learn the field. She holds over 80 patents, a Ph.D. in computer science from MIT, and an honorary doctorate from KTH, the Royal Institute of Technology, Sweden. She was named the SVIPLA (Silicon Valley Intellectual Property Law Association) Inventor of the year. Dr. Perlman was awarded the USENIX Lifetime Achievement Award in 2007. She is a recipient of the Woman of Vision Award from the Anita Borg Institute. She has been named twice as one of the 20 most influential people in the industry by the Data Communications magazine (the only person to be named so).

To arrange a meeting with the speaker, please contact Dr. Indrajit Ray at (970) 491-7097 or indrajit.ray@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.