



Fall 2010 Colloquium

Temple University

Computer and Information Sciences

Techniques for Large-scale Network-wide Attack Monitoring and Attribution

Yong Guan,

Department of Electrical and Computer Engineering
Iowa State University

Tuesday 11/2, 11am, Tech Center 111

Abstract:

The field of Digital Forensics faces many challenges and difficult problems. We have seen that digital evidence may often be available for a very short period of time and involve large volumes of data that are found locally on a single digital device or spread globally on the Internet. There is also a trend that the criminal cases where crime scenes co-exist in both cyberspace and physical worlds are increasing. In this talk, we will focus on the challenges and research problems in identifying the person(s) or organized group(s) who should be responsible for those criminal activities conducted in large-scale networked systems, such as the Internet. We will discuss the techniques we developed in the last couple of years to enable effective network-wide attack monitoring and attribution. At the end, we will discuss several other important research directions, and hope to stimulate collaborations and cross-fertilization of ideas and initiate solid research efforts in the field of digital forensics.

Bio:

Dr. Yong Guan is an Associate Professor of Electrical and Computer Engineering, and the Associate Director for Research of Information Assurance Center at Iowa State University. He received his Ph.D. degree in Computer Science from Texas A&M University in 2002, MS and BS degrees in Computer Science from Peking University in 1996 and 1990, respectively. With the support of NSF, IARPA, and ARO, his research focuses on security and privacy issues, including digital forensics, network security, and privacy-enhancing technologies for the Internet. The resulted solutions have addressed issues in attack attribution, secure network coding, key management, localization, computer forensics, anonymity, and online frauds detection. He served as the general chair of 2008 IEEE Symposium on Security and Privacy (Oakland 2008, the top conference in security), vice program chair for ICDCS 2008 (Security and Privacy Area), co-organizer for ARO Workshop on Digital Forensics in 2009, and the coordinator of Digital Forensics Working Group at NSA/DHS CAE Principals Meetings. Dr. Guan has been recognized by awards including the Best Paper Award from the IEEE National Aerospace and Electronics Conference in 1998, the 2nd place graduate winner in the international ACM student research contest in 2002, NSF Career Award in 2007, ISU Award for Early Achievement in Research in 2007, the Litton Industries Professorship in 2007, and the Outstanding Community Service Award of IEEE Technical Committee on Security and Privacy, 2008.