
IEEE COMSOC Distinguished Lecture: An overview of IT Security Forensics

by Manu Malek, Stevens Institute of Technology

Date: February 20, 2007 (Tuesday)
Time: 6:00 pm (refreshment starts at 5:45 pm)
Place: 202 ECEC, NJIT

About the Speaker

Manu Malek is Industry Professor of Computer Science and Director, Certificate in CyberSecurity Program, at Stevens Institute of Technology. Prior to joining Stevens, he was Distinguished Member of Technical Staff at Lucent Technologies Bell Laboratories. He has more than 20 years of experience in teaching, practicing, and research in communication networks design, optimization, operations, and management. He has held various academic positions in the US and overseas, as well as technical management positions with Bellcore (now Telcordia Technologies) and AT&T Bell Laboratories.

He is the author, co-author, or editor of seven books, co-holder of two patents, and the author or co-author of more than fifty published technical papers and numerous technical reports in the areas of network design, computer communications, and network operations and management.

Dr. Malek is a fellow of the IEEE, an IEEE Communications Society Distinguished Lecturer, and the founder and Editor-in-Chief of *Journal of Network and Systems Management*. He earned his Ph.D. in EE/CS from University of California, Berkeley.

About the Talk

Organizations increasingly rely on computing and intelligent networking infrastructures as keystones to their operations. Although the use of this technology provides many advantages, the Internet poses a unique set of vulnerabilities. Security attacks, such as virus, worm and other malware attacks, are examples of threats encountered daily by various institutions.

Against this backdrop, it is clear that security is one of the most important IT concerns today. Security forensics is a discipline to identify the attackers and document their activity with sufficient reliability to justify appropriate technical, business, and legal responses. The discipline involves identification, preservation and analysis of evidence of security attacks. Forensic activity takes place in a complex, legal and social context which must be understood to fully appreciate its power and value.

This talk will provide an overview of security forensics and address some of the methodologies involved. Some simple tools will also be demonstrated as examples.

**Sponsors: IEEE Communications Society North Jersey Chapter
IEEE NJIT Student Chapter
NJIT Department of Electrical and Computer Engineering**