

**THURSDAY  
OCTOBER 4, 2007**

**Scaife Hall Auditorium  
Room 125**

**4:30 p.m.**  
Refreshments—4:00 p.m.

## **PROF. WENKE LEE**

GEORGIE INSTITUTE OF  
TECHNOLOGY



Wenke Lee is an Associate Professor in the College of Computing at Georgia Institute of Technology. He received a Ph.D. in Computer Science from Columbia University in 1999. His research interests include systems and network security, network management, applied cryptography, and data mining. His research is currently supported by NSF, ARO, ONR, DHS, and the industry. He received a Best Paper Award at the 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD-99) in 1999, and a NSF CAREER Award in 2002.

ECE Seminar Hosts:  
Radu Marculescu,  
[radum@ece.cmu.edu](mailto:radum@ece.cmu.edu)  
Yi Luo,  
[y1827@andrew.cmu.edu](mailto:y1827@andrew.cmu.edu)  
Bruno Sinopoli,  
[brunos@andrew.cmu.edu](mailto:brunos@andrew.cmu.edu)

## **Botnet Detection and Response**

A Botnet is a network of compromised computers (or bots) commandeered by an adversary. Botnets have already become the platform of choice for launching attacks and committing frauds on the Internet. In this talk, I will first discuss the research challenges in botnet detection and response, and outline a comprehensive framework. I will then describe KarstNet, which is a component(s) of this framework. KarstNet uses DNS monitoring to identify domains associated with botnet command and control activities, and sinkholes such domains. If time permits, I will also discuss some preliminary work in P2P botnet detection.