



**The George Washington University
Department of Computer Science
Colloquium**

**February 26, 2008, 4:30pm
Room 736 Academic Center**

**Robert Sherwood
University of Maryland**

Securing and Understanding the Internet

ABSTRACT

Despite its increasing importance in our lives, the Internet remains insecure and its global properties unknown. Spam, phishing, and Denial of Service (DoS) attacks have become common, while global properties as basic as the router-connectivity graph continue to elude researchers. Further, these two problems are inter-related: curtailing abuse exposes gaps in knowledge of the Internet's underlying structure, and studying the underlying structure exposes new techniques to curtail abuse. The author's research leverages this insight by working on both securing and understanding the Internet. In this talk, the author first discusses his work in securing the Internet by describing Opt-Ack, a DoS attack on the network using optimistic acknowledgements. With this attack, malicious TCP receivers "optimistically" acknowledge packets they did not receive and cause unwitting TCP senders to flood the network. Using Opt-Ack, the resulting traffic flood is hundreds to millions of times the attacker's true bandwidth. The author demonstrates randomly skipped segments, an efficient and incrementally deployable solution to the Opt-Ack attack. Second, the author describes his work in understanding the Internet with DisCarte, a constraint-solving system that infers the Internet router-connectivity graph. DisCarte uses disjunctive logic programming to cross-validate topology information from TTL-limited traceroute probes and the often ignored IP Record Route option against observed network engineering practices. Compared to previous techniques, router-connectivity graphs produced by DisCarte are more accurate and contain more features.

BIOGRAPHY

Robert Sherwood is completing his Ph.D. in Computer Science from the University of Maryland. His work is in networking and security, and is advised by Bobby Bhattacharjee and Neil Spring. He has worked on many aspects of network security including anonymous communications, fair file sharing, Denial-of-Service prevention, and reputation-based trust. He obtained his B.S. from the University of Maryland and is a member of the Association for Computing Machinery (ACM).