COLLOQUIUM

Department of Computer Science and Engineering
University of South Carolina

A Passive Approach to Wireless Device Fingerprinting

Raheem Beyah

Department of Computer Science
Georgia State University

Date: **April 22, 2011**
Time: **1100-1200**
Place: **Swearingen 3D05 (Staff Lounge)**

Abstract

Threats to computer networks have evolved rapidly over the years. Traditionally, network administrators have focused on securing the perimeter (e.g., using firewalls and network intrusion detection systems (NIDS) to keep bad actors out of the network and systems). However, the computing threat landscape constantly evolves and traditional perimeter defense mechanisms are no longer sufficient. One of the most significant threats to today's computer networks is the threat from insiders. Insider attacks are dangerous because they subvert the traditional defense mechanisms and are initiated "behind" them. Further, they are initiated by individuals who have *valid credentials to access the network and systems*. These malicious insiders or misfeasors often insert unauthorized hardware into the network to accomplish their goals, which can directly or indirectly bring harm to the network and attached systems. Given the significant threat from insiders, the security of a network cannot depend only on user authentication; rather all devices *(independent of user authorization*) that access the network must have proper authorization. In this talk, I discuss a new black-box approach to identifying a type of device by passively monitoring network traffic generated from the device. This technique is a direct result of extending the boundary of the system unit into the network. The proposed technique is applied to access point (AP) fingerprinting, where architecturally heterogeneous (e.g., chipset, firmware, driver, OS) APs are identified passively from the network. I will illustrate how the proposed technique can be used to ensure only authorized nodes are on the network (i.e., for defensive purposes), as well as to profile nodes in preparation for launching device-specific attacks (i.e., for offensive purposes).

Raheem Beyah is an Assistant Professor in the Department of Computer Science at Georgia State University where he leads the Georgia State Communications Assurance and Performance Group (CAP). He is also an Adjunct Professor in the School of Electrical and Computer Engineering at the Georgia Institute of Technology. He received his Bachelor of Science in Electrical Engineering from North Carolina A&T State University in 1998. He received his Master's and Ph.D. degrees in Electrical and Computer Engineering from the Georgia Institute of Technology in 1999 and 2003, respectively. Prior to joining Georgia State in 2005, Dr. Beyah was a research faculty member with the Georgia Institute of Technology's Communications Systems Center (CSC) for four years and remains a part of the Center. He also worked as a consultant in Andersen Consulting's (now Accenture) Network Solutions group. In 2009, Dr. Beyah served as a Guest Editor for MONET. He is an Associate Editor of several journals including the (Wiley) Wireless Communications and Mobile Computing Journal. Dr. Beyah's research interests include network security, wireless networks, network traffic characterization and performance, and security visualization. He received the National Science Foundation CAREER award in 2009 and was selected for DARPA's Computer Science Study Panel in 2010. He is a member of ACM, NSBE, ASEE, and a senior member of IEEE