COSC FACULTY CANDIDATE 2010 SEMINAR

DATE: FRIDAY, APRIL 23, 2010
WHERE: PGH 232
TIME: 11:00 AM

SPEAKER: Dr. Roberto Perdisci, Georgia Institute of Technology

Title: Detecting the Network Behavior of Malware

Abstract:

Most cyber attacks are carried out via malicious software (a.k.a. malware). It is therefore important to identify whether a machine has been compromised by malware, so that system and network administrators can take action to remediate the infection and prevent future attacks. Unfortunately, the battle against malicious software is becoming harder and harder. Today's malware developers commonly employ executable packing and other code obfuscation techniques to generate a large number of polymorphic malware variants. Existing anti-virus (AV) techniques are not able to effectively cope with obfuscated malware, thus leaving our computers vulnerable to malware infections.

In this talk I will present the results of my research on detecting the network behavior of malware. The key observation is that most malware need to generate network activities in order to perpetrate their malicious intents. In addition, while code polymorphism allows for easily creating large numbers of variants of the same malware sample, when executed these variants will behave in a similar way because they share the same intended malicious goals and activities.

I will show how we can automatically identify families of malware that share similar behavior, and how we can model their malicious network activities to enable the detection of malware-compromised machines within a monitored network. I will also empirically demonstrate that network-based detection of malware behavior can complement traditional AV tools and other system-based malware clustering and detection approaches, thus representing a valuable part of a defense-in-depth strategy to protect computer networks from malware attacks.

Bio:

Roberto Perdisci is a Post-Doctoral fellow at the College of Computing of the Georgia Institute of Technology. He currently conducts research in network security under the supervision of Prof. Wenke Lee. His research interests include computer and network security, networking, and machine learning.

Prior to joining the Post-Doctoral program, he was PhD candidate at the University of Cagliari, Italy, and Research Scholar at the Georgia Tech Information Security Center. He also worked as Principal Scientist at Damballa, Inc., a spin-off of Georgia Tech that focuses on developing and commercializing botnet-detection solutions for large enterprise and ISP networks.