THE DEPARTMENT OF COMPUTER SCIENCE & THE COMPUTER SCIENCE GRADUATE STUDENT ORGANIZATION (GSOCS) PRESENT

INVITED SPEAKER SERIES

Professor R. Sekar
Stony Brook University

Tuesday, April 25th at 1:15pm, Lecture Hall 10

Provenance-Based Policy Enforcement: A Unified Approach for Vulnerability Mitigation, Malware Defense and Attack Scenario Reconstruction

Abstract: The DNC hack of 2015/16 is just the latest in a string of cyberattacks of increasing sophistication and impact. Most such attacks exploit software vulnerabilities and social engineering (e.g., spear phishing) to implant malware, which underpins an attack campaign involving data theft, infection of additional users/sites, and installation of even more stealthy malware. Despite substantial investment in software security, attackers routinely sneak past existing defenses. This is because the defenses are either reactive in nature, or, they depend on isolating bad actors from the system. Reactive techniques, such as patching and signature-based scanning, are ineffective against new vulnerabilities/attacks used in sophisticated campaigns. Isolation, on the other hand, can only be partial, since users need to interact with untrusted actors (web sites, emails, or data) at times. We therefore pursue a more flexible approach, one that relies on enhanced scrutiny rather than total isolation of untrusted elements. Specifically, we use provenance-tracking to assess the degree of control exerted by untrusted actors on security-critical operations. We then use policies to define the safe bounds for these operations. While provenance indicates whether attackers have the means to carry out an attack, policies help assess their motives, i.e., whether the actions contribute towards typical attacker