ERIK JONSSON SCHOOL OF ENGINEERING & COMPUTER SCIENCE AT THE UNIVERSITY OF TEXAS AT DALLAS

Distinguished Lecture Series
Spring 2017

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

Dr. R. Sekar
Stony Brook University

Friday, January 20th, 2017 at 2pm
TI Auditorium, ECSS 2.102

ABSTRACT OF PRESENTATION

The DNC hack of 2015/16 is just the latest in a string of cyber attacks 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 objectives. This talk will describe our provenance policy based approach, and its successful application to (a) the mitigation of a wide range of software vulnerabilities, (b) principled malware defense across diverse OSes, including Linux, BSD, and Windows XP through Windows 10, and (c) attack scenario reconstruction, where our technique addresses the "needle-in-a-haystack" problem by achieving almost a million-fold data reduction.

R. Sekar (http://www.cs.stonybrook.edu/~sekar/) is a Professor of Computer Science and the Director of the Secure Systems Laboratory at Stony Brook University. He received his Bachelor's degree in Electrical Engineering from IIT, Madras (India), and his Ph.D. in Computer Science from Stony Brook.

After working in the industry and at Iowa State University, Sekar has been a Professor of Computer Science at Stony Brook for the past 10 years. Sekar's research interests are focused on software security, with specialization in attack detection, prevention, containment, response, and recovery; mobile and untrusted code security; malware; security policies and enforcement; anomaly detection; and vulnerability analysis. His research in these areas has been funded by several grants from AFOSR, DARPA, NSF and ONR, as well as the industry. Sekar has supervised well over 100 students, including four postdoctoral and international visiting researchers, 18 Ph.D.s, and 80+ Master's. Sekar has received SUNY Chancellor's award for Excellence in Research, SUNY Research Foundation's Research and Scholarship award, Best paper awards at USENIX Security and Annual Computer Security Applications Conferences and honorable mention for best paper at SACMAT, Catacasinos Fellowship for Computer Science at Stony Brook, and Siemens prize for best undergraduate in Electrical Engineering at IIT, Madras.

Refreshments at 1:45pm