BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK | Computer Science

COMPUTER SCIENCE RESEARCH SEMINAR

Towards a Timely Causality Analysis for Enterprise Security

Dr. Mu Zhang
Postdoctoral Associate
Department of Computer Science, Cornell University

Friday, March 16th at noon in room R15, Engineering Building

Abstract: The increasingly sophisticated Advanced Persistent Threat (APT) attacks have become a serious challenge for enterprise IT security. Attack causality analysis, which tracks multi-hop causal relationships between files and processes to diagnose attack provenances and consequences, is the first step towards understanding APT attacks and taking appropriate responses. Since attack causality analysis is a time-critical mission, it is essential to design causality tracking systems that extract useful attack information in a timely manner. However, prior work is limited in serving this need. Existing approaches have largely focused on pruning causal dependencies totally irrelevant to the attack, but fail to differentiate and prioritize abnormal events from numerous relevant, yet benign and complicated system operations, resulting in long investigation time and slow responses. To address this problem, we propose PrioTracker, a backward and forward causality tracker that automatically prioritizes the investigation of abnormal causal dependencies in the tracking process. Specifically, to assess the priority of a system event, we consider its rareness and topological features in the causality graph. To distinguish unusual operations from normal system events, we quantify the rareness of each event by developing a reference model which records common routine activities in corporate computer systems. We implement PrioTracker, in 20K lines of Java code, and a reference model builder in 10K lines of Java code. We evaluate our tool by deploying both systems in a real enterprise IT environment, where we collect 1TB of 2.5 billion OS events from 150 machines in one week. Experimental results show that PrioTracker can capture attack traces that are missed by existing trackers and reduce the analysis time by up to two orders of magnitude.

Bio: Mu Zhang is a Postdoctoral Associate in the Department of Computer Science at Cornell University, working with Prof. Elaine Shi. He received his Ph.D. in Computer & Information Science & Engineering from Syracuse University, advised by Prof. Heng Yin. Before joining Cornell, he spent two years as a research staff member at NEC Labs America. His research interests lie in several aspects of Computer Security and he is particularly interested in System Security, Mobile Security, Cyber-Physical Systems Security and Enterprise IT Security. His work has been published in CCS'14, CCS'15, NDSS'14, NDSS'16, NDSS'18, prestigious conferences in the area of computer security.

This event is funded by GSOCS, a subsidiary of GSO, using Student Activity Fee Funds

Refreshments will be provided!