TEXAS TECH UNIVERSITY
Edward E. Whitacre Jr.
College of Engineering™
Computer Science

What's Going On? Big Picture Awareness Oriented Security Defense in Enterprise-level Networks

Xiaoyan Sun
Prospective Faculty Candidate
Pennsylvania State University
Wednesday, March 23, 2016
3:00 p.m.
Petroleum Engineering, Room 120
(Old Petroleum Engineering Building)

Abstract

Today's enterprise network is usually under basic protection from security deployments like firewall and IDS. However, in many cases cyber security defense still fails unexpectedly, even if the security sensors have already provided relevant alerts towards ongoing attacks. In actual fact, the raised alerts are often easily ignored. One main reason for such failure is the lack of attack context, which is essential for gaining big picture awareness towards the enterprise network's actual situation. For example, given a number of security alerts, can we tell what's going on in the network? In this talk, I will describe a set of security problems that are identified in revealing the missing attack context for enterprise cyber security defense, and introduce a family of systems developed to tackle the corresponding problems. In particular, I will mainly focus on the identification of zero-day attack paths, which is one of the most fundamentally challenging security problems yet to be solved. I will present two systems, Patrol and ZePro, which can both detect the zero-day attack paths at operating system level, but employ different approaches. Lastly, I will talk about the short term and long term plans along my line of cyber security research.

Biography

Xiaoyan (Mindy) Sun is a PhD candidate in College of Information Sciences and Technology at the Pennsylvania State University. Her current research pursues enterprise-level cyber security defense based on vulnerability analysis, intrusion detection, and probabilistic uncertainty analysis, etc., with particular focus on identification of unknown attacks and revealing missing attack context. Xiaoyan is very passionate about interdisciplinary research, based on her background in cyber security, intelligent transportation systems and electrical engineering.