Thesis: Structural Anomaly Detection, an Entity-Centric Fusion Framework

Abstract: Intrusions or security violations can be detected by mining system's audit records for abnormal patterns of system usage. As computer systems become more complex, attacks evolve from being opportunistic to being more stealthy, advanced, persistent and multi-staged. It is a long-standing challenge to effectively analyze audit records and detect intrusions. We present an entity-centric fusion framework that systematically mines entity behavioral patterns and builds security context for detecting structural anomalies. This proposed framework enables log process and aggregation from various levels of information granularity on entities to discover functional units, also known as communities, driven by roles that entities play or functionalities that they are built for. With multiple perspectives of interpreting entity activity, various community structures corresponding to specific system purposes can be revealed. Profiling entities through different communities involvement helps quantify their engagement of various functionalities. Collective interactions among communities outline community norms, where system structures will be derived. Unwanted or malicious activities that contradict to designated roles an entity plays will appear anomalous to community norms, as defined structural anomaly.

Committee:

- Professor Sven Dietrich, Mentor, Hunter College
- Professor Ping Ji, John Jay College
- Professor Debroy Saptarshi, Hunter College
- Professor Yong Guan, Iowa State University, Outside Member

Outside Member:

- Professor Yong Guan, Iowa State University, Outside Member