Dissertation Defense

WHEN: Monday, April 30, 2018, 2:30 PM
WHERE: Room F219
CANDIDATE: Yassir Hashem
MAJOR PROFESSOR: Dr. Hassan Takabi
CO-MAJOR PROFESSOR: Dr. Ram Dantu
COMMITTEE MEMBERS: Dr. Suliman Hawamdeh, Dr. Renee Bryce

TITLE

A MULTI-MODAL INSIDER THREAT DETECTION AND PREVENTION BASED ON USER'S BEHAVIOURS

Insider threat is one of the greatest concerns for information security that could cause more significant financial losses and damages than any other attack. However, implementing an efficient detection system is a very challenging task. It has long been recognized that solutions to insider threats are mainly user-centric and several psychological and psychosocial models have been proposed. A user's psychophysiological behavior measures can provide an excellent source of information for detecting user's malicious behaviors and mitigating insider threats. In this dissertation, we propose a multi-modal framework based on the user's psychophysiological measures and computer-based behaviors to distinguish between a user's behaviors during regular activities versus malicious activities. We utilize several psychophysiological measures such as electroencephalogram (EEG), electrocardiogram (ECG), and eye movement and pupil behaviors along with the computer-based behaviors such as the mouse movement dynamics, and keystrokes dynamics to build our framework for detecting malicious insiders. We conduct human subject experiments to capture the psychophysiological measures and the computer-based behaviors for a group of participants while performing several computer-based activities in different scenarios. We analyze the behavioral measures, extract useful features, and evaluate their capability in detecting insider threats. We investigate each measure separately, then we use data fusion techniques to build two modules and a comprehensive multi-modal framework. The first module combines the synchronized EEG and ECG psychophysiological measures, and the second module combines the eye movement and pupil behaviors with the computer-based behaviors to detect the malicious insiders. The multi-modal framework utilizes all the measures and behaviors in one model to achieve better detection accuracy. Our findings demonstrate that psychophysiological measures can reveal valuable knowledge about a user's malicious intent and can be used as an effective indicator in designing insider threat monitoring and detection frameworks. Our work lays out the necessary foundation to establish a new generation of insider threat detection and mitigation mechanisms that are based on a user's involuntary behaviors, such as psychophysiological measures, and learn from the real-time data to determine whether a user is malicious.