Deep Focus: Increasing User “Depth of Field” to Improve Threat Detection

Project Goals
We believe insider threat detection methods can be improved by monitoring and analyzing features of user behavior not typically associated with malicious insider behavior. Anomalous behavioral and statistical patterns observed in such data sets may indicate new indicators or help reduce high false positive rates associated with existing indicators.

We have three specific goals for this project:
1. Detect account misappropriation by monitoring sudden and significant changes in IF system interactions by the account user.
2. Develop unique profiles of individual users based on behavior on IF systems.
3. Baseline individual user behavior and monitor for changes that indicate potentially malicious insider behavior is likely to occur.

We intend to achieve the following outcomes:
1. A measure of confidence that the person interacting with the IF system is in fact the authorized user.
2. Methods for collecting additional context of user behavior by which insider threat and anomalous detection engines can parameter with higher confidence that suspicious behavior is likely to be malicious.
3. Visualization of these methods and metrics for analyst use.

Linguistic Patterns
Characteristics of a user's speech or writing can be measured both structurally and linguistically. Using these metrics, researchers have shown the feasibility of identifying anomalous users (Taylor 2012). Others have observed measurable changes in linguistic patterns of known insiders (Taylor 2012).

Tools
- Linguistic and spoken words are extracted from source repositories and processed to identify individual users. Identifying information is masked and actual text is not viewed by researchers. These data are then prepared for analysis using an internet application written by research staff.
- Linguistic analysis performed by a Linguistic Inquiry Word Count (LIWC) test.
- Structural characteristics obtained with natural applications.

Initial Results
Comparing data sets and linguistic features to see if same user similar for typical vs. spoken words?

Network Authentication Graphs
These directed graphs represent a user's authentication activity between networked computers over a predefined period. Research shows that administrative users generally have larger, more complex graphs than normal users (Kant 2013). Furthermore, it is possible to profile each user's authentication activity, resulting in the ability to detect abnormal and potentially malicious activity. Empirical research on malicious insiders shows that many insiders engage in reconnaissance and information-gathering activities, accessing numerous network locations that often differ from the insider’s normal work activity.

Keystroke/Mouse Biometrics
Using metrics like keystroke latency or mouse dynamics, researchers have shown how individual users can be identified (Kant 2013). Furthermore, evidence suggests changes in a user's personal state, such as increased stress, is also detectable.

Visualization
Issues of concern must be visible and apparent to analysts. In cooperation with the Cyber Security Centre at Oxford, we will leverage an existing insider threat visualization tool to represent the data and associated activity we find in a clear and actionable manner.