

## HIT-IT (Heuristic Identification & Tracking of Insider Threat)

**HIT-IT (Heuristic Identification and Tracking of Insider Threat)** - Insiders, those within or closely related to an organization, pose the greatest risk to an organization's information infrastructure. Organizations grant insiders both authorized access to and knowledge of their information systems, primarily computer systems and the organization's network. In the past, insiders have abused this trust by stealing or corrupting data, committing fraud, and modifying performance reports. Because malicious insiders may act within the bounds of their privileges, mitigation of the insider threat differs from that of external threats.

Detection of Undesirable Insider Behavior via Data Mining. Numerous existing systems seek to mitigate the threat that parties external to an organization pose to its information systems. Unfortunately, little research beyond access control strives to mitigate the threat that malicious or uninformed insiders may introduce. These insiders present a particularly insidious problem as they may behave adversely yet act fully within the bounds of their privileges. To assist administrators in detecting both known and novel insider threats, CS&IIR researchers are continuing research and development of a prototype hybrid system that simultaneously utilizes rule-based and data mining techniques. The continuing research is based on work performed at Oak Ridge National Laboratory by Joseph Calandrino, Princeton University, and Steven McKinney, North Carolina State, in 2006. The prototype Heuristic Identification and Tracking of Insider Threat (HIT-IT) system utilizes a technical approach similar to the Minnesota INtrusion Detection System (MINDS)<sup>19</sup>, a system under development at the University of Minnesota for the United States Army. While the MINDS objective is automatic detection of cyber attacks via analysis of data from various network sensors, the objective of HIT-IT is identification and tracking of the malicious insider threat. User behavior data is first acquired and then filtered to remove uninteresting patterns. Pre-processing of the data extracts basic features (e.g., number of logins or number of file deletions in a given day) along with derived features, such as statistics on the basic features. Knowledge discovery techniques identify very anomalous data, and the behaviors causing the anomalous scores are automatically identified and graphed for the system administrator. A human analyst (the sys admin in this case) assesses the results to discard false positives and to label the true alarms for inclusion in the signature detection component. Application of the HIT-IT system will illuminate many aspects of user behavior that are currently unexplored, such as consistency of activity over time, uniqueness of user behavior, and the minimum "fingerprint" size necessary to accurately model behavior and isolate anomalies – Calandrino (Princeton U)/McKinney /Neergaard/Sheldon/Ferragut/MacIntyre.

**POC:** Erik Ferragut, PhD; Michael Neergaard, MS  
Cyberspace Sciences & Information Intelligence Research (CSIIR) Group  
Oak Ridge National Laboratory P.O. Box 2008, Oak Ridge, TN 37831-6418  
[www.ioc.ornl.gov](http://www.ioc.ornl.gov)