

ITD (Insider Threat Detection) system

ITD (Insider Threat Detection) system - Insiders, those within or closely related to an organization, pose the greatest risk to an organization's information infrastructure. They are purposefully given access to and knowledge of information systems, primarily computer systems and the organization's network, which differentiates insider from external threat. In the past, insiders have used their access privileges to cause harm to organizations by stealing or corrupting data, committing fraud, and modifying performance reports. Due to the authorized access that insiders are given, it is much different detecting threat posed by insiders than for those external to the organization. Common security applications such as firewalls and Intrusion Detection Systems (IDSs) are in place to prevent external threat, but in most cases insiders are not restricted or monitored by these mechanisms. The majority IDSs that have been developed are for detecting external threat, but comparatively little time has been spent researching insider IDSs. During a recent survey conducted by the US Secret Service, 29% of respondents which were able to determine the source of intrusion, stated the threat came from insiders. Given this, and that a single malicious insider can cause significant financial damage (500 million dollars in one case) to an organization, it is easy too see the need for research and development of insider threat detection systems.

ITD is based, in part, on research conducted at ORNL during the summer of 2005 by Dr. Seong-Moo Yoo and Dr. Frederick Sheldon (SNORT+). Their research has proved useful in providing a foundation from which to begin this work and identifying Bayesian network software that can be used to implement the Bayesian network for this project. However, ITD is markedly different from SNORT+ and other research conducted in the areas of insider threat detection and distributed intrusion detection. SNORT+ was a plug-in to the existing IDS, Snort. ITD uses Snort as well, but as a resource, where Snort's log data is consumed by the system. In general, the other systems mentioned are targeted at external threat detection, do not use Bayesian networks to determine threat levels, or do not allow dynamic, intelligent modification to rule-sets. The Intelligent Insider Threat Detection (ITD) system is a distributed, hierarchical, multi-faceted, multi-level, rule based intrusion detection system. The system uses a client-server architecture and provides scalability because of its hierarchical nature. It is multi-faceted in that it monitors an insider's local system activities, their network based activities, and is extensible so other aspects of the information system may be monitored – McKinney (NCSU)/Neergaard/Sheldon/Ferragut

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