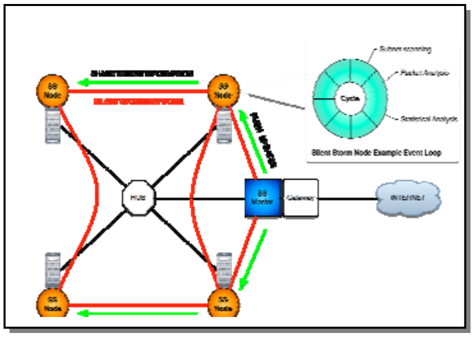
OAK RIDGE NATIONAL LABORATORY FACT SHEET

MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

SILENT STORM – Distributed Active Response System for Cyber Defense

Traditional intrusion detection systems (IDS's) are localized at a single point within a network—usually at or near the network gateway. Using a combination of signature and rule based detections; these systems identify anomalous network traffic or host behavior and generate alerts to a centralized user. Our approach to intrusion detection is different. SILENT STORM is a distributed system composed of intelligent processing agents that reside at multiple hosts within the enterprise and at the network gateway. Individual hosts are monitored by the SILENT STORM intelligent agents. When anomalies occur, these agents can communicate their finding to other agents for corroboration. If multiple anomalies are detected an alert can be generated to the user. Additionally, distributed storage and processing ensures that information cannot be lost if the SILENT STORM network is itself attacked as a part of an intrusion.



SILENT STORM nodes are based upon leveraging the Ubiquitous Network Transient Autonomous Mission Entity (UNTAME) system developed at ORNL over the past 10 years. UNTAME is a computational framework for deploying an autonomous self-replicating and self-healing system. The deployed system is capable of harnessing the power of distributed computational intelligence for knowledge discovery, statistical analysis and anomaly detection. The SILENT STORM framework correlates intrusion detection incidents to enable faster-than-human response to network attacks; and has the capability for online distributed learning of normal and abnormal traffic patterns for advanced insider threat detection and mitigation

SILENT STORM is ubiquitous, distributed, computationally intelligent, and autonomous. IDS's are plagued with the problems of a high false positive rate and are not designed to operate within a distributed computational framework. When multiple data flows are analyzed, data overload occurs quickly increasing false positive rate and reducing effectiveness. Current IDS' are also not capable of active online learning of new patterns from observed data. By its very nature, SILENT STORM addresses a problem not currently dealt with in the marketplace and therefore it must enhance the current state of the practice.

POC: Joseph P. Trien, Christopher Griffin, Louis Wilder, Bob Schlicher
Cyberspace Sciences & Information Intelligence Research (CSIIR) Group
Oak Ridge National Laboratory P.O. Box 2008, Oak Ridge, TN 37831-6418
www.ioc.ornl.gov

UT-BATTELLE