THE ABSTRACT

The project proposal is as follows

Initially we will record (EHR) system in a large medical centre. The results illustrate our models exhibit significant performance gains over state-of-the-art competitors. When the number of Collaborative information systems (CISs) are deployed within a diverse array of environments that manage sensitive information. Current security mechanisms detect insider threats, but they are ill-suited to monitor systems in which users function in dynamic teams. In this paper, we introduce the community anomaly detection system (CADS), an unsupervised learning framework to detect insider threats based on the access logs of collaborative environments. The framework is based on the observation that typical CIS users tend to form community structures based on the subjects accessed (e.g., patients' records viewed by healthcare providers).
CADS consists of two components: 1) relational pattern extraction, which derives community structures and 2) anomaly prediction, which leverages a statistical model to determine when users have sufficiently deviated from communities? We further extend CADS into MetaCADS to account for the semantics of subjects (e.g., patients' diagnoses). To empirically evaluate the framework, we perform an assessment with three months of access logs from a real electronic health illicit users is low, MetaCADS is the best model, but as the number grows, commonly accessed semantics lead to hiding in a crowd, such that CADS is more prudent.

How our proposal overcomes the limitations of existing

MetaCADS dominates when the mix rate is low, but CADS dominates when the mix rate is high. Notably the disparity between MetaCADS and CADS is more pronounced at the low mix rate (0.91 versus 0.88) in this setting than in the previous setting. However, at lower false positive operating points, CADS appears to dominate MetaCADS.

Proposed system

Several notable approaches have been proposed to address this type of intruder. The first is nearest neighbour anomaly detection techniques, which are designed to measure the distances between instances by assessing their relationship to "close"
Instances. If the instance is not sufficiently close, then it may be classified as an anomaly. However, social structures in a CIS are not explicitly defined and need to be inferred from the utilization of system resources. If distance measurement procedures are not tuned to the way in which social structures have been constructed, the distances will not represent the structures well. Our experimental results confirm this notion.

Modules:

- Pattern Extraction
- Anomaly Detection
- Detection Performance Metrics
- Varying Number of Accessed Subjects

LIST OF FIGURES

LIST OF TABLES