A Study of CADS approach in Collaborative Information System for Detecting Anomalous Insiders

Gayatri K. Chaturvedi[1]
[1]Matoshri College of Engineering and Research Center, Nashik

Abstract—A group of users are allowed to communicate and cooperate over a common task with the help of Collaborative Information System. Collaborative information systems (CISs) are deployed within a diverse array of environments that manage sensitive information. Recent breakthroughs in networking, storage and ubiquitous computing have facilitated an explosion in the deployment of CIS across a wide range of environments. Current security mechanisms detect insider threats but they are not efficient 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. A 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). Based on the analysis of result illustrates when the number of 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.

Key words: Insider threat detection, CADS, MetaCADS

I. INTRODUCTION

In this section, collaborative information system is introduced. Recent breakthroughs in storage, ubiquitous computing and networking have facilitated the explosion in the deployment of CIS across wide range of environments.

A. Introduction

Group of users are allowed to communicate and co-operate over a common tasks with the help of collaborative information system. They have long been called upon to support and co-ordinate activities related to the domain of computer supported and cooperative work. CIS has been widely accepted for computational support. Due to the various features of CIS such as increasing organizational efficiency through efficient and quick workflows, reduction in administrative cost, assist innovation through brain-storming sessions and facilitate social engagement, the notion of CIS is typified in wikis, video conferencing, document sharing and editing as well as dynamic bookmarking on Internet.

At the same time, CIS are increasingly relied upon to manage sensitive information. Intelligence agencies have adopted CIS to enable timely access and collaboration between group of analysts using data on personal relationships, financial transactions and surveillance activities. Additionally hospitals have also adopted electronic health record (EHR) systems to decrease health care costs, strengthen care provider productivity and increase patient safety using vast quantities of personal medical data.

However, at the same time, the detail and sensitive nature of the information in such CIS make them attractive to numerous adversaries. A suspicious insider in this setting corresponds to an authenticated user whose actions run counter to the organization's policies.

In this paper, we study a framework to detect anomalous insiders from the access logs of a CIS by leveraging the relational nature of system users as well as the meta-information of the subjects accessed. The framework is called as the community anomaly detection system (CADS) and this framework accounts for the observations that in collaborative environments users tend to be team and goal oriented [6]. In this context, an arbitrary user should exhibit similar behavior to other users based on their co-access of similar subjects in the CIS.

B. Motivation of CADS

Current security mechanisms detect insider threats but they are not well suited to monitor systems in which users function in dynamic teams. The dynamic teams can be constructed on the fly based on the shifting needs of the operation and the availability of the users. To detect anomalous insiders in a CIS a community-based anomaly detection model (CADS) has been proposed that utilizes a relational framework.

C. Benefits of CADS

We utilize a real-world data set to systematically evaluate the effectiveness of anomaly detection framework. For the labeled anomalous users, we simulate insider threat behavior and empirically demonstrate that our models are more effective in performance than the state-of-the-art competitive anomaly detection approaches. Our analysis provides evidence that the typical system user is likely to join a community with other users whereas the likelihood that a simulated user will join a community is low. Based on our study, findings indicate that the quantity of illicit insiders in the system influences which model among CADS or MetaCADS is a more prudent solution.

D. Aim

In this paper we study CADS approach which aims to detect anomalous insiders that access subjects at random. We aim to design models to integrate our approach with others in the future.

E. Organization of Report

The report is organized as follows: First it describes the existing system and proposed system. Secondly, it describes the specific community extraction and anomaly detection methods that are integral part of CADS approach. Then the detailed experimental analysis of CADS model is illustrated.

Lastly, we present the future research and summarize the work

II. LITERATURE REVIEW

In general there are two types of security mechanisms that have been designed to address the insider threat. The first is to prevent illicit activity my modeling access rules for the system and its users. The second is to detect illicit activity post hoc by reviewing pattern of user behavior. Formal access control frameworks are designed to specify how resources in a system are made available to authenticated users. Most access control frameworks determine if a request to the system is permitted based on a set of static predefined rules.

In year 2001 the author J. Park and R. Sandhu introduces theory on role-based access control framework have been extended to address complex workflows by accounting for teams [2]. This framework assumes that system is static, limited to context that relate to activities, tasks or workflow progress and can be clearly modeled but the dynamic nature of modern CIS makes it difficult to apply these principles in a setting.

In year 2008 the model of pervasive computing has been implemented by D. Kulkarni and D. Tripathi this model is based on context-aware role based access control [3]. In the same year D. Dori et.al introduces situation based access control framework [4] in health care organization by characterizing situations of access to patient data.

These set of approaches strive to define "zones" in which a user can access and act upon subjects in a system. However, users can commit illicit actions in the zones in which they are entitled to function. In this case, there are mainly two classes of malicious insiders: 1) masqueraders 2) traitors. The masqueraders are the most familiar example of an insider. They have little knowledge of the system and the anticipated behavior. They may be a user that searches for knowledge to exploit or they may be users whose accounts have been compromised. Traitors on the other hand have complete knowledge of the system and its policies. A traitor may exhibit normal behavior and still perpetrate malicious acts.

In year 2011 J. Kim et.al focuses on detecting suspicious access to EHRs using statistical and machine learning [5]. The results suggest that statistical and machine-learning methods can play an important role in helping privacy officers detect suspicious accesses to EHRs. Anomaly and signature filtering concepts are applied to improve the classifier performance for detecting suspicious access to EHRs [7]. This concept is not successful in all manners as detection of rare but it's for important events.
Recently meta-community based anomaly detection system [6] is introduced by Bradley Malin et.al this system is less efficient when illicit users are more.

Summary

Various approaches have been developed to address the insider threat in collaborative environments. Formal access control frameworks have been adapted to model team and contextual scenarios [3], [4]. Recognizing that access control is necessary but not methods has been proposed to detect deviations from expected behavior. Recently some approaches have been proposed to detect deviations from expected behavior [5], [6], [7].These models construct a subject-specific graph which contains all users acting on particular subject. These models then inquire how the similarity of this network is affected by the removal of certain users.

III. EXISTING SYSTEM VS PROPOSED SYSTEM

This section describes the basic block diagram of existing security mechanism and proposed security system.

A. *Existing System*

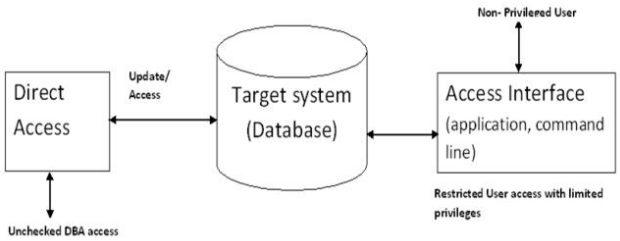

Fig. 1: A traditional approach to system protection

Here Fig. 1 illustrates the traditional approach for protecting database against insider threat. In this traditional approach the DBA has uncontrolled access to the system and is able to make any kind of changes without any restrictions.

A DBA can compromise in very obvious way. There may be situation which includes changing some configuration parameters that changes the behavior of a system. In this type of system protection there is no protection against the insiders.

B. *Proposed System*

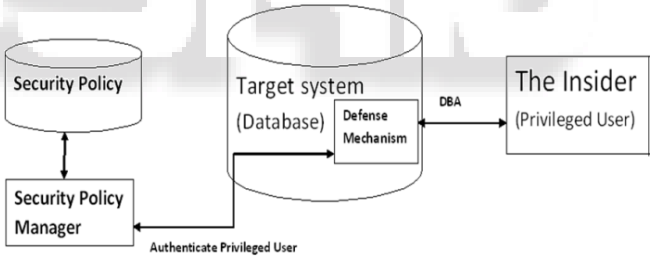

Fig. 2: Intrusion Threat Security Architecture enabled protection against insider threat

The Fig. 2 is diagram of proposed system which is based on Intrusion Threat Security Architecture (ITSA) framework shows that any user including DBA cannot make any changes to the system without going through the defense mechanism which is embedded inside the target system. The defense mechanism queries the security policy to verify the actions submitted against the system. The security policy can only be modified by the super system owner.

IV. ARCHITECURAL OVERVIEW

This section begins with an overview of the CADS framework. This is followed by a description of the empirical methods applied in the framework.

A. *Overview of Framework*

CADS consists of two primary components: 1) Pattern Extraction (CADS-PE) and 2) Anomaly Detection (CADS-AD)

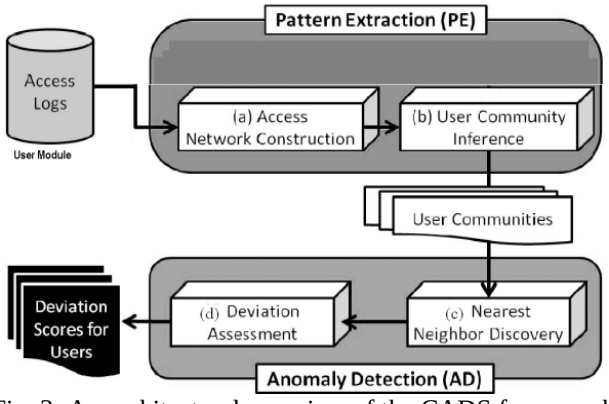

Fig. 3: An architectural overview of the CADS framework

1) Pattern extraction:

CADS-PE infers communities from the relationships observed between users and subjects records in the CIS access logs which derive community structures. CIS users tend to form community structures based on the subjects accessed.

2) Anomaly Detection:

We introduce a framework to detect anomalous insiders from the access logs of a CIS by leveraging the relational nature of system users as well as the Meta information of the subjects accessed which leverages a statistical model to determine when users have sufficiently deviated from communities.

B. Notation

To formalize the problem, we use the following notation. Let U, S, and G be the set of users, subjects, and categories to which a subject can belong in the CIS, respectively. Let DB be a database of access transactions, such that db Є DB is a tuple of the form < u, s, G', time >, where u Є U, s Є S, G' $\subseteq$ G, and time is the timestamp associated with the access. We use cardinality |. | To represent the number of elements in a set.

C. Pattern Extraction

The pattern extraction process consists of two primary steps: a) construction of the user-subject access network and b) user community inference.

1) Network Construction:

The extraction process begins by mapping T onto a tripartite graph. The graph represents the amalgamation of the user-subject access network and the subject-category assignment network. In the former an edge represents that a user accessed the subject's record. In the latter an edge represents that the subject's record is assigned to a particular category.

There are various aspects of a user's relationship to subjects that could be leveraged for measuring similarity. To mitigate bias and develop a generic approach, we focus our attention on the number of subjects a user accessed. Using this feature, we employ the inverse document frequency (IDF) model which is popularized by information retrieval systems and shown to be effective for weighting the affinity of individuals to subjects in friendship networks.

2) Community Inference:

To infer user communities CADS performs a spectral decomposition on a relational model of the users. In preparation for the decomposition CADS builds a matrix which is based on the access network.

This matrix implies the structure of the user communities, which CADS uses as the core patterns for anomaly detection.

D. Anomaly Detection

CADS-AD predicts which users in the CIS are anomalous by a) discovering a user's nearest neighbors and b) calculating the deviation of each user from their neighbors.

1) Nearest Neighbor Discovery:

To search for the k-nearest neighbors (KNNs) of a user, we adopt a modified Euclidean distance. This measure weights the principal components proportionally to the amount of variance they cover in the system. These distances are stored in a matrix DIS |U| × U|.

Algorithm 1: Minimization of the network community profile

Input: DIS is a distance matrix
Output: k is the number of nearest neighbors
1: k ← |U| {Initialize to all possible neighbors}
2: for i = 1 to |U| do
3: N = { }
4: for j = 1 to |U| do
5: N ← N U i - nn_j
{The i-nearest neighbor network for user u_j}
6: end for
7: for j = 1 to |U| do
8: if Ψ (g_j,N,i) < k then
9: k ← i {the conductance function}
10: end if
11: end for
12: end for

Here, Ψ corresponds the conductance which is a measure designed to characterize network quality. Let H be the union of the elements in N i.e. the union of nodes and edges in the nearest neighbor networks. Considering sub graph $g = (ng, eg) \in N$, Conductance is defined as,

$$\Psi(g) = \frac{N_g}{\text{Min}(\text{vol}(g),\text{vol}(H/g))} \quad (4.1)$$

Where,

N_g denotes the size of the edge boundary

$$Ng = |(y,z): y \varepsilon n_g, z \notin n_g|,$$

And

$$\text{Vol}(g) = \sum_{y \in n_g} \deg(y) \quad (4.2)$$

such that deg(y) is the degree of node y.

2) Measuring Deviation from nearest neighbors:

The radius of a user u_i is defined as the distance to its k^{th} nearest neighbor excluding it. The radius of u_i is r_i = sort (DIS (i, :))(i, k+1), where sort is a function that ranks distances in increasing order from smallest to largest. Users are thus characterized as a vector of radius r = [r_1, r_2..., $r_{|U|}$] and set of neighbors knn = [knn_1, knn2… $knn_{|U|}$].The smaller the radius, the higher the density of the user's network. Anomalous users cannot be detected through radius alone and direct application of such a measure can lead to undesirable results.

We calculate the deviation of a node's radius from those of its k-nearest neighbors to assess the degree to which

it is anomalous. For a user ui, we calculate the deviation of their radius as

$$Dev(u_i) = \sqrt{\frac{\sum_{u_j \in knn_i} (r_j - \bar{r})^2}{k-1}} \quad (4.3)$$

Where $\bar{r} = \frac{\sum_{u_j \in knn_i} r_j}{k}$

V. SIMULATION

A. Anomaly Detection Models

There are alternative anomaly detection models that have been proposed in the literature. There are three of the most related models. The first two are based on supervised classification and assume there exists a training set of anomalous and non-anomalous user class labels whereas the final model is an unsupervised heuristic.

1) k-nearest neighbors:

This model predicts the label for a user based on their k-nearest neighbors in the training set. The labels are weighted based on the cosine similarity of each neighbor to the user.

2) Principle components analysis (PCA):

This model predicts if a user is closer to normal or abnormal users according to the weighted principal components model.

3) High volume users (HVUs):

This model is based on a rule invoked by privacy officials at several healthcare providers. It ranks users based on the number of subjects they accessed. The greater the number of subjects accessed the higher the rank.

B. Simulation of Users

One of the challenges of working with real data from an operational setting is that it is unknown if there is abnormal behavior in the data set. Thus, to test the performance of the models an evaluation process mixes simulated users with the real users of the EHR data set. This process worked under the assumption that an anomalous user would not exhibit steady behavior and believe that such a behavior is indicative of users that access patient records for malicious purposes such as identity theft. The evaluation is divided into three categories of settings.

1) Sensitivity to number of records accessed:

This setting investigates how the number of subjects accessed by a simulated user influences the extent to which the user can be predicted as anomalous. In this case, a lone simulated user is mixed into the set of real users. The simulated user accesses a set of randomly selected subjects the size of which ranges from 1 to 120.

2) Sensitivity to number of anomalous users:

This setting investigates how the number of simulated users influences the rate of detection. In this case, the numbers of simulated users are varied from 0.5 to five percent of the total number of users. Each of the simulated users access an equivalent-sized set of random subjects' records.

3) Sensitivity to diversity:

The third setting investigates a more diverse environment.

C. Setting the Neighborhood Parameter

The community-based models incorporate a parameter k to modulate the community size. This parameter tuned empirically using the network community profile.

D. Results

The set of experiments focus on the sensitivity of anomaly detection models. Here a single simulated user mixed with the real users. The number of subjects accessed by the simulated user is varied to investigate how volume impacts the deviation score and the performance of the anomaly detection models in general. For illustration, the CADS deviation scores for the simulated users in the EHR data set are summarized in Fig. 3.

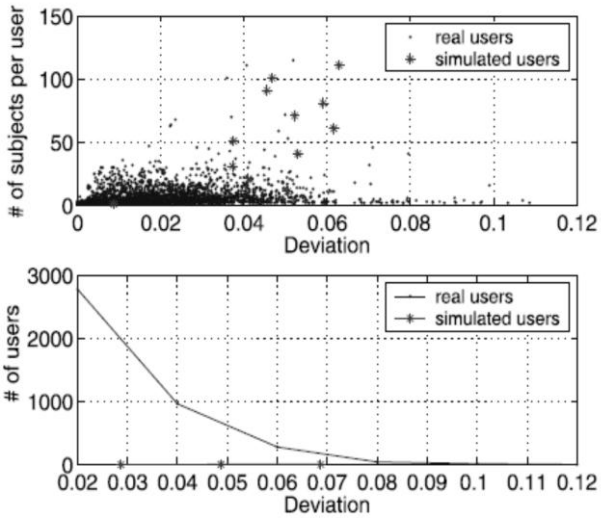

Fig. 3: The CADS deviation scores of real and Simulated users as a function of number of Subjects accessed

The low deviation score indicates the number of subjects accessed by the simulated users is small. Whereas when the number of subjects accessed is larger than 20, the deviation scores of simulated users increase significantly.

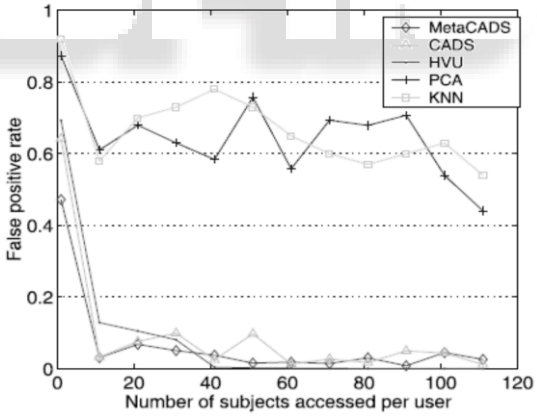

Fig. 4: False positive rate of detection for a simulated user with an increasing number of accessed subjects

Fig. 4 shows how the number of subjects accessed by the simulated user influences the performance of the anomaly detection models. When the number of accessed subjects for the simulated user is small it is difficult for all of the models to discover the user via the largest deviation score. This is expected because all of the models except for HVU are evidence-based. They need to accumulate a certain amount of statistical evidence before they can determine that the actions of the user are not the result of noise in the system.

The performance of all models generally increases with the number of subjects accessed. However, the performance gain is relatively minor for the classification models such as KNN and PCA.

VI. CONCLUSION AND FUTURE WORK

In this paper, a small step is taken toward understanding the detection of insider threat. We have studied basic block diagram of existing security mechanism and proposed detection security mechanism. The CADS approach is proposed to detect anomalous insiders in CIS that utilizes relational framework. This model is based on the observation that normal users tend to form communities unlike illicit insiders.

With the basis of entire seminar I can summarize that various techniques to prevent insider threat based on access control framework is developed then CADS and MetaCADS to detect the insider threat developed in a decade. Based on empirical results we can conclude that the MetaCADS is best model when the numbers of illicit users are less but CADS is more quick and efficient when number of illicit users grows.

– *Future Work*

Since the CADS framework is an unsupervised system it may be implemented in real time environments with offline training. There are limitations of the system, however and in particular to validate and improve CADS approach in CIS with adjudication through real human experts.

REFERENCES

[1] You Chen, Steve Nyemba, and Bradley Malin," Detecting Anomalous Insiders in Collaborative Information Systems ", IEEE transactions on dependable and secure computing, vol. 9, no. 3, pp 332-343, may/June 2012.

[2] J. Park, R. Sandhu, and G. Ahn, "Role-Based Access Control on the Web," ACM Trans. Information System Security, vol. 4, no. 1, pp. 37-71, 2001.

[3] D. Kulkarni and A. Tripathi, "Context-Aware Role-Based Access Control in Pervasive Computing Systems," Proc. 13th ACM Symp. Access Control Models and Technologies, pp. 113-122, 2008.

[4] M. Peleg, D. Beimel, D. Dori, and Y. Denekamp, "Situation-Based Access Control: Privacy Management via Modeling of Patient Data Access Scenarios," J. Biomedical Informatics, vol. 41, no. 6, pp. 1028-1040, 2008.

[5] A. A. Boxwala, J. Kim, J. M. Grillo, and L.O. Machado, "Using Statistical and machine Learning to Help Institutions Detect Suspicious Access to Electronic Health Records," J. Am. Medical Informatics Assoc., vol. 18, pp. 498-505, 2011.

[6] Y. Chen, S. Nyemba, W. Zhang, and B. Malin, "Leveraging Social Networks to Detect Anomalous Insider Actions in Collaborative Environments," Proc. IEEE Ninth Intelligence and Security Informatics, pp. 119-124, 2011.

[7] J. Kim, J. Grillo, A. Boxwala, X. Jiang, R. Mandelbaum, B. Patel, D. Mikels, S. Vinterbo, and L. Ohno-Machado, "Anomaly and Signature Filtering Improve Classifier Performance for Detection of Suspicious Access to EHRs," Proc. Ann. Symp. Am. Medical Informatics Assoc., pp. 723-731, 2011.

