THINK INDIA (Quarterly Journal)

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

An Cyber Threat Prediction Mechanism Based on Behavioral Analysis

Swapna Siddamsetti
Assistant Professor
Department of CSE
Pallavi Engineering College

B.Roopa Devi
Assistant Professor
Department of CSE
Pallavi Engineering College

Abstract. Detection of insider cyber threats is a challenging problem that cannot be solved by existing approaches because insider attackers have already bypassed security systems like firewalls, Intrusion detection & prevention systems, etc. [1].With the traditional security systems rendered completely ineffective there is a need for a newer mechanism that based on the original traditional security systems that approaches insider threat as a new kind of cyber threat and helps preventit.

Keywords: *Insider cyber threats, threat detection, cyber threat prediction.*

1 Introduction

An insider cyber threat is a person or process with malicious intention with an access (authorized or non-authorized) to an organization's network, system, or data storage devices containing information in any form. Such an access has a potential capability to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems. Traditional network security systems like Intrusion Detection and Prevention Systems protect the network from external attackers by limiting network connectivity between the extranet and intranet and closely monitoring the networkstream.

Since an insider attack is “inside” the organization his activities are go undetected by such systems which are typically located outside the LAN as a network gateway – whereas the insider is able to access the LAN systems from behind the gateway. Also an insider is aware of the structure of the network systems and the organization in general which help him plan the attack quickly without being noticed.

Before executing an attack, an insider (like an outsider in a case of an outsider attack) exhibits several changes in the activities - known as *precursors* [2]. The precursors that are a resultant of the unmet expectations, disgruntlement and loss of trust are known as behavioral precursors. Since the insider is aware of the structure of the network systems and the organization he starts playing around with the systems with an attempts to masquerade or break the systems. These activities known as technical precursors are prologues of possible security attacks.

We propose a system that keeps a track of activities a user performs on a host and in a network via any static or mobile devices connected to the network. The activity log of a user can be then analyzed and this analysis can be used to predict the forthcoming actions of the user, based on which the user can be assigned a “threat- rank” on a scale of 1 and 10. Users with frequent deviations from their threat rank can be treated as insider threats and organization can take relevant action against them. The following paper describes the necessity and working of the proposed system.

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

2 Relatedwork

The recent techniques for detection of insider threats have been shown as follows:

2.1. NLP analysis of text communications

The paper Semantic Analysis for Monitoring Insider Threats [3], the authors have described semantic analysis using Natural Language Processing (NLP) system, of the insider's text-based communications produces conceptual representations that are clustered and compared on the expected vs. observed scope. The determined risk level produces an input to a risk analysis algorithm that is merged with outputs from the system's social network analysis and role-based monitoring modules. Finally the system defines a "threat level" for the person of interest.

The drawback of this method is that the only source of information is text-based communication between an insider and a perpetrator outside the organization.

2.2. Computer usage activity tracking

In the paper Detecting Insider Threats in a Real Corporate Database of Computer Usage Activity [4] the authors have developed a model called PRODIGAL (PROactive Detection of Insider threats with Graph Analysis and Learning) that applied and evaluated multiple AD algorithms and supporting technologies based on models of different aspects of user behavior; over 100 semantic (i.e., domain- knowledge-based) and structural (graph-based) features; a schema representation for comparing results of different AD algorithms; a visual AD language; data extraction, loading, and transformation components; and an integrating software framework for experimentation.

Their model relies on insider's interaction with the computer file system i.e. upload/download of files, copying files to removable media as well as sending in email attachments. This method is good for data protection but it ignores activities like communication via text chatting, internet browsingetc.

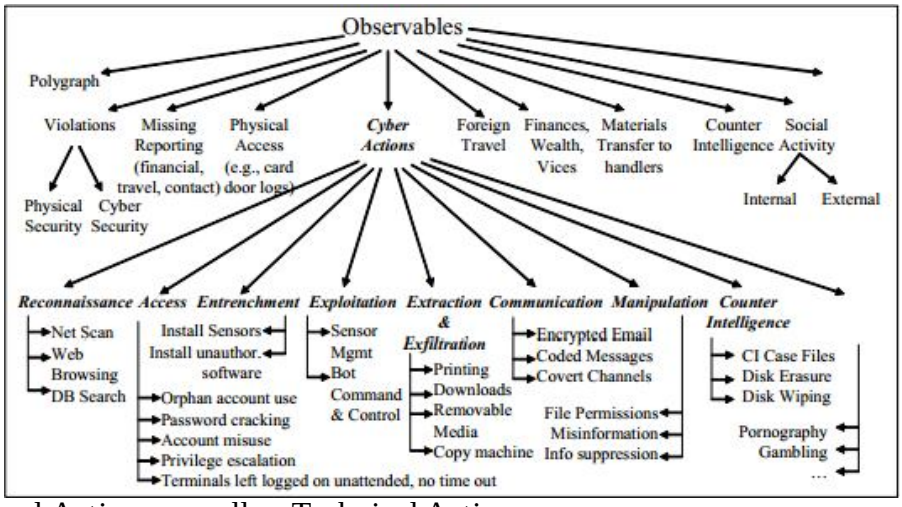
2.3. Mouse-pointer movement tracking for detection of insiderthreats

A unique technique of identifying insider threats from large dataset of suspects is discussed in the paper Identifying Insider Threats through Monitoring Mouse Movements in Concealed Information Tests [5]. In this paper the authors describe a mechanism that measures the deviation in patterns of mouse-pointer usage of a person to identify if that person has been a part of an insider attack. The observations are made when the persons are made to use a specially developed application that asks multiple choice questions relevant to the security threat and records the mouse pointer movements of the person.

This technique is very easy to implement but just like any other polygraph test it cannot be guaranteed. However it can be used along with other techniques to reduce chances of false-positives as well as false negatives.

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

In Analysis and Detection of Malicious Insiders [6] the authors explain the various observable actions that an insider may exhibit as anomolous. These actions can be classified into



Behavioural Actions as well as Technical Actions.

Fig. 2. Cyber Event/Observable Taxonomy [6]

Collection of technical action data is possible but without correlating that with behavioral profile of a person there would be many false positives or false negatives.

2.4. Behavioral profiling for insider threatdetection.

Remote assessment of insiders and content analysis of activities done by them are important methods described in the paper The role of behavioral research and profiling in malicious cyber insider investigations [7]. Remote assessment means working with surveillance teams, review of archived records including personnel records, call records, attendance records etc. Content analysis builds up the psychological profile of the person by lexical analysis of the textual content involved. Specific markers like spelling and grammar mistake, frequent occurrence of words, abbreviations, tone etc. are used as a parameter for identifying original author of the text data by correlation with the writing behaviors of all personnel in a network.

2.4 Cyber Behavior Analysis and Detection Method, System and Architecture[8]

This US Patent has been published on 06/05/2014. The description of the patent is given as:

"A scalable cyber-security system, method and architecture for the identification of malware and malicious behavior in a computer network. Host flow, host port usage, host information and network data at the application, transport and network layers are aggregated from within the network and correlated to identify a network behavior such as the presence of maliciouscode."

However Insider Threat Detection is more difficult than many other anomaly detection (AD) problems [4] not only because insiders are knowledgeable about an organization's computer systems and procedures and authorized to use these systems, but also, and more important, because malicious activity by insiders is a small but critical portion of their overall activity on

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

suchsystems.

2.5 Proactive or Predictive Insider ThreatDetection

In the paper “Modeling Human Behavior to Anticipate Insider Attacks” [9] the authors have described about a system that collects data from various sources like SEIM systems, IDS systems, DLP systems, packet tracking systems, HR systems, etc. Each of the data source has an ontology defined which identifies the data-type for that particular domain. This comprehensive threat assessment framework promises to automate the detection of high-risk, concerning behaviors ("precursors" or "triggers") on which to focus the attention and inform the analysis of cyber-security personnel, who would otherwise be required to analyze and correlate an overwhelming amount of data. Incorporating psychosocial data along with cyber data into the analysis offers an additional dimension upon which to assess potential threats within a comprehensive, integrated threat analysis framework.

3 Comparison of techniques

Preliminary analysis of the above techniques gives us the following observations.

Name	Advantage	Drawback	Approach
NLP Analysis of Text Communication	Fast	Limited to text communication	Proactive
Computer Activity Usage & Tracking	Accurate	Limited to compute activities	Proactive
Mouse Pointer Movement Tracking	Cost-effective	Not proactive Not reliable	Reactive
Cyber Behaviour Analysis	Accurate	Relies on Network Traffic only Expensive	Proactive
Predictive Insider Threat Detection	Can predict future behaviour	Still in experimental stage	Proactive

Based on the above criteria we have identified that while current systems have advancements in behavioral threat detection and ranking, they lack in user-based threat detection.
However for complete evaluation we devised a few evaluation criteria which are mentioned as below:

A. Host Audit

The ability of the system to collect usage information from the system logs, application logs and other various logs for investigation purpose.

B. Host Monitoring

The ability of the system to monitor activity that is happening currently on the host. This may include processes running, files accessed, applications opened, network connections, input devices like mice, keyboard, etc.

C. LAN Audit

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

The ability of the system to collect information of all the devices that are connected or removed from the local area network along with specifics like MAC address, host OS, IP address etc.

D. LAN Monitoring
The ability of the system to capture network packets in real time and inspect them for anomalous activity.

E. User Detection
The ability of the system to identify activity by an individual user from various hosts on a network based on the activity logs collected from hosts or network.

F. Behaviour Detection
The ability of the system to identify the type of behavior based on actions carried out by a specific host or a user.

G. Threat Detection
The ability of the system to identify and predict current or forthcoming threats based on the actions carried out by a specific host or a user.

H. Threat Ranking
The ability of the system to allocate a threat rank which may be a number between 1 and 100 based on the actions carried out by the specific host or a user.

4 Proposed system

Based on the mechanisms that we have reviewed till now we have come up with a proposed solution which we call “Scalable Automated Technology for Analysis and Ranking of Known threats” known asSATARK.

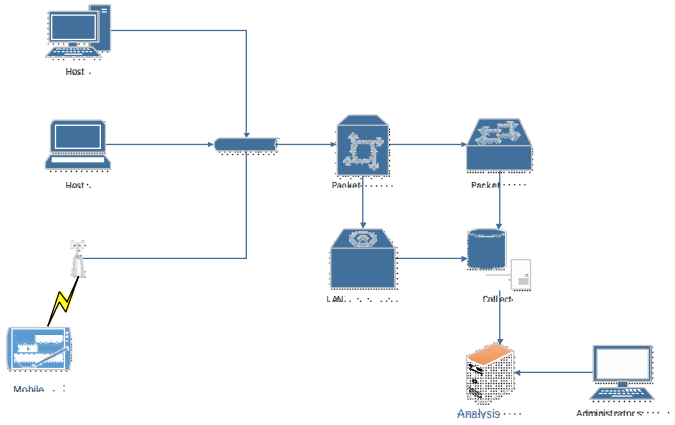


Fig. 2. Arrangement for SATARK system in a network

We propose addition of a few components in a local area network which has several wired, wireless and mobile devices connected to it. They are asfollows:

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

4.1 Host Unit

The host unit is a software package installed on each host belonging to a network which contains a Host OS, a Host Collector that identifies key information from the logs of the host operating system and a Host Monitor that keeps a track on events happening on the host operating system like file access, program launch, network connectivity etc.

4.2 LAN Unit

The LAN unit tracks network packets. It is necessary for hosts which do not have the host unit software installed i.e. mobile hosts. Additionally it injects a unique ID in the network packet in order to associate the data packet with the unique identity of the user that has transmitted the packet.

4.3 Central Detection Unit

It collects log data from the host unit and LAN unit, storing it into log database for further analysis by reading the log data stored into log database and tries to define possible anomalous events. It then provides a threat rank between 1 and 10 based on the factors like severity of the threat detected and frequency of anomalous behavior of a user or a host. The system calculates the deviation between historical threat ranks of a particular user or a host and suggests to the administrator.

SATARK will initially collect forensic data from the computer and it will use that data as a training data as well as it will calculate a threat-rank. This will be done for all person s in the computer network. After that SATARK will keep monitoring applications, networks, text input etc. At the end of the day it will create another threat rank for that person. There will be a deviation in threat rank of person if the type of usage has changed from regular usagepattern.

Each daily ranks will be collected and deviations will be recorded, to build a “threat-profile” of the person. This will help in detection of insider threat before they perform any threatful activity.

5. Advantages

Our method is a Reactive approach and it does not need a large amount of “training data” to get it working so it can be effective from first day, minimizing the chances of a zero-day threat. Also our method relies on “ranking” instead of binary-classification like “theat/non-threat”. Setting various threat levels helps reduce chances of false positives and false negatives as it can be correlated with psychological parameters observed by people of organization.

6. Conclusion

Detection of Insider Cyber Threats is a difficult task because the threats might not be malicious in nature. Building a psychological profile of the personnel by tracking changes in technical behavior and comparing this pro

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

7. References

1. A. Ginter, "DuQu, Stuxnet, APT and Other Failures of ICS Security," in *AFPM Q&A and Technology Forum*, 2012.
2. S. J. Stolfo and M. S. Bellovin, Insider Attack and Cyber Security: Beyond the Hacker, Springer, 2008.
3. S. Symonenko and E. D. Liddy, "Semantic Analysis for Monitoring Insider Threats," *Lecture Notes in Computer Science Volume 3073,* pp. 492-500, 2004.

4. T. Senator and D. Bader, "Detecting Insider Threats in a Real Corporate Database," in *19th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD),* Chicago, IL, 2013.
5. J. S. Valacich and J. L. Jenkins, "Identifying Insider Threats throughMonitoring Mouse Movements in," in *Hawaii International Conference on SystemSciences. Deception Detection Symposium*,2013.
6. M. Maybury, P. Chase and B. Cheikes, "Analysis and Detection of Malicious Insiders," *International Conference on Intelligence Analysis, McLean, VA,* 2005 .
7. B. Joll and K. Ross, "Cyber Behavior Analysis and Detection Method, System and Architecture". USA Patent 20140157405, 2014.
8. F. L. Greitzer and R. E. Hohimer, "Modeling Human Behavior to Anticipate Insider Attacks," *Journal of Strategic Security Volume 4*, pp. 24-47, 2011.
9. F. Greitzer and D. Frincke, "Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation," *Advances in Information Security Volume 49,* pp. 85-113, 2010.

