DETECTING UNKNOWN INSIDER THREAT SCENARIOS

Manvendra Singh Lodhi and Rahul Kaul

Department of Computer Science Engineering BMCT Indore, Madhya Pradesh, India

ABSTRACT

Problems from the inside of an organization's perimeters are a significant threat, since it is very difficult to differentiate them from outside activity. In this dissertation, evaluate an insider threat detection motto on its ability to detect different type of scenarios that have not previously been identify or contemplated by the developers of the system. We show the ability to detect a large variety of insider threat scenario instances We report results of an ensemble-based, unsupervised technique for detecting potential insider threat, insider threat scenarios that robustly achieves results. We explore factors that contribute to the success of the ensemble method, such as the number and variety of unsupervised detectors and the use of existing knowledge encoded in scenario based detectors made for different known activity patterns. We report results over the entire period of the ensemble approach and of ablation experiments that remove the scenario-based detectors.

KEYWORDS

Insider, Insider Threat, Scenario, Suspect, Unauthorized Device.

1. INTRODUCTION

WHAT IS AN "INSIDER"?

There exist many different definitions of the terms "insider" and "insider threat". One common definition is that "an insider is defined as an individual with privileged access to an electronic system". Second is, on the surface, this definition seems satisfactory. When machine access was limited and the tasks performed on electronic systems were well defined the term "privileged access to an electronic system" had a common and well-delineated meaning. Two developments in recent years have served to confound this picture. One is the now ubiquitous networked computing environment. The other is the increasingly dynamic and porous, if not ill-defined, boundary between the inside of the organization and the outside (consider the range of joint ventures, outsourcing arrangements, consultants and temporary workers in the business world today, for instance).

WHAT IS AN "INSIDER THREAT"?

A definition of what an insider threat is obviously depends heavily on the definition of what an insider is. If "an insider is a person that has been legitimately empowered with the right to access organization assets, representation of them, or decide about one or more assets of the

organization", then what is an insider threat?
One definition is that:
"An insider threat is an individual with privileges who misuses them or whose access results in misuse".

Many companies and organizations, at some point, have knowingly or unknowingly been subject to a cyber-attack. Many cyber attackers that exist on the outside of a company world or an organizational infrastructure hacking and breaking the information systems to execute their cyber-attacks. Others cyber-attacks are executed with the help of viruses or system/network intrusion. Until the past decade however, insiders were often overlooked as potential threats to commit cyber-attack. Although there are security and access control policies to prevent organizations from known threats, individuals that are trusted to follow these policies do not at times. When security policies and access control policies are not followed by anyone who is a part of organization, it typically exposes organizations to both external and internal cyber threats. Although the majority of cyber-attacks stem from external entities, insider attacks are often more damaging and costly due to the knowledge of and access to information systems. The intricacies surrounding insider threat are more complex than those dealing with external entities. This is because internal cyber-attacks do not always occur as a direct result of a breach of security or access policy. Some internal attacks occur without a breach of any security or access policy.

The company uses a patented process to produce goods that are applied in a variety of end-products. Because of the intellectual property and specific knowledge that is available to insiders (i.e. employees, business partners, visitors), the question rose on "How to protect intellectual property and other valuable information against misuse of these insiders?"

Many other modern organizations make use of a sheer amount of information and information systems. Organizations that value their information need to safeguard it from threat agents that exploit vulnerabilities in information systems and/or information security measures. Although attacks originating from outside threat agents, such as hacking attempts or viruses, have gained a lot of publicity, the more risky attacks come from inside (Schultz, 2002; Baker et al., 2008). Insiders are trusted and, therefore, have the necessary access to be able to exploit vulnerabilities more easily.

It is widely accepted that the insider threat activities to enterprises is increasing, and that significant costs are being incurred. Since insider threat and compromising actions can take a multitude of forms, there is a diverse experience and understanding of what insider threats are, and how to detect or prevent them. The purpose of this research is to investigate the potential for near real-time detection of insider threat activities within a large enterprise environment using monitoring tools centered on the information infrastructure. As insider threat activities are not confined solely to cyber-based threats, the research will explore the potential for harnessing a variety of threat indicators buried in a different enterprise operations connected to or interfacing with the information infrastructure, enabling human analysts to make informed decisions efficiently and effectively.

2. RELATED WORKS

Real insider threats are complex and adversarial, which leads us to conclude that an effective system for detecting these threats must detect scenarios that builders of the system never planned

for or contemplated. Therefore, it is important to evaluate systems on their ability to detect previously unknown scenarios in real data.

William T. Young, Alex Memory, Henry G. Goldberg, Ted E. Senator in at [1] evaluate some prototype in their setting and show that by using a variety of diverse individual detectors combined using an anomaly detection ensemble technique, they achieve a final detection result with performance that consistently approaches that of the unidentified detector among the set tested that was found to perform best on each dataset in after-the-fact analysis. Their result holds on many data sets, including ones containing scenarios they had not contemplated when designing the detectors. The ensemble result also outperforms many anomaly detectors that are specifically focused on the scenarios that are known, on data sets containing those scenarios.

Aleksandar Lazarevic, Vipin Kumar in at [2] worked on novel general framework for combining outlier detection algorithms. Experiments on several synthetic and various real life data sets indicate that proposed combining methods can result in much better detection performance than the single outlier detection algorithms. The proposed combining methods successfully utilize benefits from combining multiple outputs and diversifying individual predictions through focusing on smaller feature projections. Data sets used in our experiments contained different percentage of outliers, different sizes and different number of features, thus providing a diverse test bed and showing wide capabilities of the proposed framework. The universal nature of the proposed framework allows that the combining schemes can be applied to any combination of outlier detection algorithms thus enhancing their usefulness in real life applications. Although performed experiments have provided evidence that the proposed methods can be very successful for the outlier detection task, future work is needed to fully characterize them especially in very large and high dimensional databases, where new algorithms for combining outputs from multiple outlier detection algorithms are worth considering. It would also be interesting to examine the influence of changing the data distributions when detecting outliers in every round of combining methods, employing not only the distance-based but also other types of outlier detection approaches.

3. PROBLEM STATEMENT

Find the Unknown and new scenario which helps to achieves consistent result and performance without relying any single detector or the best unidentified detector for each analysis.

4. SOLUTION APPROACH AND METHODOLOGY

Find new scenario that are able to incorporate scenario-focused detectors effectively to increase confidence in results when known scenarios do match with ones in the data. We will also begin incorporating explanation capabilities with the ensemble approach so that underlying reasons for detection from individual detectors can be combined in the final result presented to analysts.

In this research, I introduce some new scenarios and their solutions which help any security system to increase their success percentage by grabbing any suspect and those new scenarios are:

1. Wearable technologies.
2. The conscientious objector
3. Hide system which is handled by outsider.

4. User knows about insider threat detection OR Hiding the illegal activities information from investigators.
5. Analyzing employee activity outside the origination. All above scenarios have their own problem as well as own solution by which insider threat system is affected.

4.1 WEARABLE TECHNOLOGIES

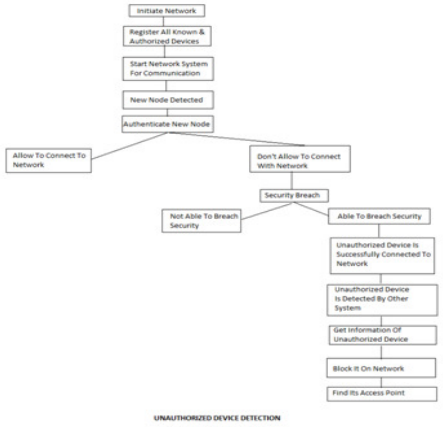
Technically, just about any device that's worn on the body (like a headset) can be considered wearable technology. We have had smart phones with cameras for years. However, others can see when someone is taking pictures with a smart phone. New wearable technology could be recording conversations or copying intellectual property without being detected. They can connect with network unethically and do whatever they want with the data flow on the network.

OUR PROPOSED ALGORITHM:

- New network set-up initiate.
- Register all known authorized devices by their MAC address in network.
- Start network scan for new node periodically.
- Authenticate new device by MAC address while making connection to the network.
- Generate alert if any unauthorized device is connected to network.
- Block that unauthorized device on network.
- Find access point of that unauthorized device.
- Find unauthorized user.

Find unauthorized device which is connected to network using proposed algorithm:

```
Given
    t : time interval for network Net scan
    N : total number of devices connected to network Net
    n : number of unauthorized devices connected to network Net
    L : List of registered MAC addresses on network Net
    l : List of unauthorized MAC addresses on network Net
    Initialize network Net;
    Register all known devices MAC address in Net;
    Initialize N = total number devices registered on Net; Initialize n  = 0;
    Initialize L = devices registered with MAC on Net;
    Initialize l = 0;
    Scan network with t interval; If(unauthorized device found on Net)
    {
    n = number of unauthorized devices;
    l  =  MAC  address  of unauthorized
    devices;
    findIntersectionOf(L,  l);//  this uses simple intersection algorithm
    raiseAlertToAdmin();
    blockUnauthorizedDevicesOnNet();
    findAccessPointOfUnauthorizedDe
    vicesOnNet();
    }
```



It uses simple mapping algorithm which just calculate intersection of registered MAC addresses and connected MAC addressed and gave unauthorized connected MAC information as an result. By finding correct access point from where unauthorized person establish its connection to the network, we can find rouge person. This scenario and its solution help us to find any unauthorized device which is connected to the network weather it is wearable or any other device like computer, laptop, mobile or any other device which is able to establish connection to the network and capture the data for any purpose.

4.2 HIDE SYSTEM WHICH IS HANDLED BY OUTSIDER.

In thus technical era, there is a boom of technology in every field. People have such type of electronic devices which are easy to hide and control. Those devices either wired or wireless, people are able to do their data transmission by using those devices. People use hardware or software for which are able to transmit data, sniff data and collect sensitive data unethically. Always monitor your network by both means i.e. software as well as hardware.

Monitor unwanted or untrusted software or hardware on network continuously and whenever those kinds of things are found then take proper action by investigating it properly.

We can imply all these above things by:

a) Scan physical state of network i.e. scan for unknown hardware part in network, in computers like data packet sniffing card, mini USB devices, network taps, port mirroring switches etc.
b) Scan all the machines for untrusted software like Wireshark, Smartsniff etc.
c) Remove USB ports/ CD-DVD drives from all machines, deploy them on employee request.
d) any type of downloading on the network, if any one wants any software then he/ she request the same from admin.
e) Assign static IP's to all the system which will help admin to track every system in the organization.

4.3 USER KNOWS ABOUT INSIDER THREAT DETECTION OR HIDING THE ILLEGAL ACTIVITIES INFORMATION FROM INVESTIGATORS.

For insider threat detection, organization deploys an insider threat detection system in organization. But what happened when employee wants to be whistleblower or wants to perform illegal activity in organization which will harmful for organization?
What happens when an employee is a part of threat detection system team member or know everything which will makes him/ her to hide every illegal activity from the system?
Recent exploration performed by the popular security corporation reveals that your computer and mobile phones can still get hacked even if they aren't connected to the internet or by malicious system which is not connected to your network. People uses ELECTROMAGNETIC RADIATION for tracking down the keyboard activity and get every single key pressed on keyboard.

To avoid theft of information from such type of techniques, organizations have to monitor their workplace for such kind of devices or system periodically.

4.4 ANALYZING EMPLOYEE ACTIVITY OUTSIDE THE ORIGINATION

This is not an ethical way to monitor any employee beyond the organization boundaries but, now days, this is an important thing to monitor your employee 24/7 because of security threat fear.
Let's take an example, for work flexibility, organization allowed employees to "work from home" and employees work from home by various remote desktop tools which help them to access organization non- disclosure environment.
Now, what happened, if any employee of organization misuse this facility and leak organization classified information to competitor or any other outsider which is harmful for the organization?
These types of scenarios are not adjustable and must be figure out by some ways to resolve such type of issues.
It is not possible to monitor all employees all the time outside the working place but if admin have any suspect then organization will have to monitor that suspect outside the working place for bringing more information for the same.

4.5 THE CONSCIENTIOUS OBJECTOR (GAIN TRUST AND MISUSE IT)

An individual who refuse to follow organization policies weather those policies are right or wrong. This is a very complex threat for organizations because trust is not any a physical thing and it cannot be measurable.

What organizations do is, organizations can check background, take feedback from past organizations, put a legal clause for confidentiality etc. and after doing all the possible validation of employee, organization allow employee to be a part of organization.

5. CONCLUSIONS AND FUTURE WORK

Dealing with insider threats has been hard for years. No one is exempt from dealing with our changing technological landscape or our own role in helping secure the enterprise. I added up some more scenarios by which we can increase the probability of success in capturing the suspect red handed with proof.As this is not a one-time problem or solution which is stop at

certain point where we can find a static solution for this. In future, there are, for sure, more scenarios are emerged to breach organizations security or confidentiality which must be resolved after finding them for avoiding any type of leakages of sensitive data outside the world.

6. ACKNOWLEDGMENTS

This Research Was Supported/Partially Supported By "BM Group Of Colleges Indore". I Thank My Mentor From "BM Group Of Colleges Indore" Who Provided Insight And Expertise That Greatly Assisted The Research. I Thank Rahul Kaul, Professor Of BM Group Of Colleges For Assistance With Finding New Algorithm, And Kapil Vyas, Professor Of BM Group Of Colleges For Comments That Greatly Improved The Manuscript.

REFERENCES

[1] Detecting Unknown Insider Threat Scenarios William T. Young, Alex Memory, Henry G. Goldberg, Ted E. Senator Leidos, Inc. Arlington, VA, USA {youngwil, memoryac, goldberghg, senatort}@leidos.com

[2] Feature Bagging for Outlier Detection, Aleksandar Lazarevic, United Technologies Research Center, University of Minnesota, Vipin Kumar, Department of Computer Science, University of Minnesota, USA.

[3] SC Magazine. (2012) Danger within: Insider threat. [Online]. Available: http://www.scmagazine.com/report-insider-threat-more-dangerous-than-external-risks/article/455117/

[4] CERT Insider Threat Team.(2013)Unintentional insider threats : A foundational study.[Online].Available:http://resources.sei.cmu.edu/library/assetview.cfm?assetid=51648

[5] J. Hunker and C. W. Probst, "Insiders and insider threats – an overview of definitions and mitigation techniques," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 2, no. 1, pp. 4–27, 2011

[6] T. E. Senator et. al., "Detecting Insider Threats in a Real Corporate Database of Computer Usage Activity," in Proceedings of the ACM SIGKDD Conference on Knowledge Discovery and Data Mining, page 1393- 1401, ACM (2013)

[7] T. Dietterich. "Ensemble Methods in Machine Learning." In Multiple Classifier Systems, 1–15. Springer, 2000.

[8] J. Glasser and B. Lindauer. "Bridging the Gap: A Pragmatic Approach to Gneerating Insider Threat Data," in Proceedings of the Workshop on Research for Insider Threat, IEEE CS Security and Privacy Workshops, San Francisco, CA, 23-24 May 2013.

[9] A. Lazarevic and V. Kumar. "Feature Bagging for Outlier Detection." In Proceedings of the Eleventh ACM SIGKDD International Conference on Knowledge Discovery in Data Mining, 157–166, 2005.