The Optimization of Situational Awareness for Insider Threat Detection

Kenneth Brancik
Northrop Grumman Corporation
7575 Colshire Drive
McLean, VA 22102
703-883-8333
Kenneth.Brancik@ngc.com

Gabriel Ghinita
Purdue University
305 N. University St.
W. Lafayette, IN 47907
765-496-9390
gghinita@purdue.edu

ABSTRACT

In recent years, organizations ranging from defense and other government institutions to commercial enterprises, research labs, etc., have witnessed an increasing amount of sophisticated insider attacks that manage to bypass existing security controls. Insider threats are staged by either disgruntled employees, or employees engaged in malicious activities such as industrial espionage. The objectives of such threats range from sabotage, e.g., in order to disrupt the completion of a project, to exfiltration of sensitive data such as trade secrets, patents, etc. Insiders are often skilled and motivated individuals with good knowledge of internal security measures in the organization. They devise effective and carefully planned attacks, prepared over long periods of time and customized to inflict maximum damage. Such attacks are difficult to detect and protect against, because insiders have the proper credentials to access services and systems within the organization, and possess knowledge that may allow them to deceive network defense controls. As a result, a large number of hosts may be taken over, allowing malicious insiders to maintain control over the network even after leaving the organization.

The objective of this study is to identify a high-level architecture and mechanisms for early detection and protection against insider threats. One of the main aspects we focus on is preventing data exfiltration, which is known to cost billions of dollars in losses annually. The goal is to either *(i)* detect attacks as they occur and prevent insiders from gaining control over the network, or *(ii)* detect early hosts and services that are compromised such that malware is prevented from spreading/morphing, hence insiders are no longer able to control the network or to exfiltrate sensitive data. We envision a data-intensive approach that leverages large amounts of events collected from a diverse set of sources such as network sensors, intrusion detection systems, service logs, as well as known attack databases (e.g., virus signature collections, digital artifacts), security and service logs, etc. The proposed approach aims to study and understand the relationships and correlations between events, with the purpose of detecting anomalous and/or malicious behavior.

CODASPY'11, February 21–23, 2011, San Antonio, Texas, USA.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *Access controls, Authentication, Cryptographic controls, Information flow controls, Invasive software (e.g., viruses, worms, Trojan horses)*

General Terms

Management, Design, Security.

Keywords

Insider Threat, Data Exfiltration.

1. INTRODUCTION

Ever since the creation of the Internet more than two decades ago, cyber-attacks have increased in sophistication and frequency. Malware capabilities have gained more disruptive power, as well as faster velocity of spreading from one system to another. However, the conventional paradigm for cyber-attacks was to target a relatively small number of system vulnerabilities, write exploits, and then mass-distribute them indiscriminately to an as-large-as-possible number of Internet hosts. In many cases, the attacked hosts were not even running software that was subject to vulnerability, but the number of hosts that did and got compromised was still large enough to warrant the cyber-criminals' efforts. Defending against malware was thus a matter of making sure that all systems are timely patched with the most up-to-date version of operating systems, application libraries, etc. Therefore, most security tools to-date rely on signature-based detection that identifies malware based on the code structure of binaries and prevents execution of malicious programs.

However, conventional defenses are often insufficient to defend against a more powerful type of attacks staged by insiders. An insider is a current or former employee, a contractor or consultant, a software vendor, who possesses similar access rights and provisioning to data and systems as an employee. Insider threats have been identified as a very dangerous source of cyber-attacks. The motivation of insiders ranges from revengeful acts, in the case of disgruntled employees, to more serious scenarios of espionage. In the former case, employees or ex-employees that are not happy with the way that the organization treated them are infecting the network with malware, corrupting or deleting data, sabotaging projects, etc. On the other hand, the latter case typically involves the theft of trade secrets, patents or other confidential data. Exfiltration of such data can have disastrous effects, either in the form of financial losses, or the compromise of national security, e.g., in the case of military secrets.

The effectiveness of insider attacks is often higher than conventional attacks for a number of reasons:

- Insiders already possess credentials that allow them legitimate access to machines and service inside the organization network.
- Actions of insiders originate at a trusted domain within the network, and are not subjected to thorough security controls in the same way as external accesses. For instance within the organization network there is often no internal firewall, which allows insiders to stage a broader range of attacks.
- Insiders, especially trained computer technicians, have good knowledge about the internal configuration of the network and the security and auditing control deployed. Therefore, they may be able to by-pass security mechanisms.
- Insiders have physical access to organization machines. They could, for instance, insert removable media with malware in an organization machine and easily infect a large number of hosts.

The insider threat component is one of the more elusive and insidious components of the threat landscape and represents a national security concern given its implications on all sectors of the critical infrastructure. There is little data available in the public domain that provides an accurate image of this threat. Consequently, the insider threat modeling is a process that has been long overlooked, leaving many organizations exposed to it.

A 2005 study by McAfee [1] presents several statistics about insider threats, covering both malicious insiders, as well as situations where insiders pose a security threat due to negligence. In the former category, the study found that five percent of employees have knowingly accessed areas of the corporate IT infrastructure that they were not supposed to access. In the latter category, the statistics show that one in five employees allow family and friends to use company laptops and PCs to access the Internet and install software. In addition, more than half of employees connect their own devices or gadgets to the company PC, creating the opportunity for malware to spread within the corporate network.

In this paper, we discuss the main elements of a solution to the problem of insider threat with focus on protecting against data exfiltration. Such elements are as follows:

- Techniques to identify data sources (e.g., security and service logs, network flow captures, etc.) that provide valuable information which helps in identifying malicious insider behavior
- A data-intensive architecture for a system that collects, indexes and processes event data. Data analysis and correlation is performed in order to identify malware based on signatures of known attacks and digital artifacts

Note that, with respect to the sophistication and complexity of the attack strategies used, there are many common characteristics between insider threats and advanced persistent threats (APT). Furthermore, the objectives of both categories of cyber attackers are often the same (e.g., data exfiltration). In our view, it is becoming increasingly more challenging to segregate insider threat attacks against other threat vectors which comprise the entire threatscape (e.g., external and APT attacks). Throughout the paper, we will emphasize the symbiotic relationship which exists between the three threat vectors (External, Insider and APT).

The rest of the paper is organized as follows: In Section 2, we present two representative insider attack scenarios. Section 3 outlines the proposed data-intensive architecture for detection and protection against insider threats. We survey related work in Section 4 and conclude with directions for future research in Section 5.

2. INSIDER THREAT ATTACK SCENARIOS

To illustrate the severe consequences and the difficult challenges posed by insider threats, we present two real-life attack scenarios that have as object a financial services institution. In the first case, an insider named Mallory is able to take control over a restricted organization machine in order to commit fraud and obtain financial gains by placing illegal trades. In the second case, Mallory exfiltrates a database with customers and trading positions which he can sell to a competitor financial services organization.

Case 1: Insider accesses unauthorized machine for own benefit. Mallory is a long-time employee who has been working with the *"sweat.equity.com"* investment company for more than ten years. He has been recently passed over for a long-waited promotion, and he is now planning to get his revenge and at the same time get rich quickly through misrepresentation and fraud. Mallory is a FX trader for private retail customers and all his accounts have a daily limit on the amount of money that can be invested. In addition, his accounts are audited daily. On the other hand, Alice is a recently hired and impressionable employee who is in charge of trades for large institutional investors. Institutional trades are placed from a restricted machine *MAE (Machine Attack and Exploit)* and trades are not subject to confirmation by the accounting department. Furthermore, auditing is only done on a monthly basis.

As a seasoned veteran with the company, Mallory is aware of the absence of daily checks for MAE trades, and he plans to use this to his own benefit. Specifically, Mallory sends an e-mail to Alice with a document that she must urgently review. The e-mail contains malware that installs a split VPN channel between the MAE and Mallory's machine. Even if the e-mail is marked as potentially malicious by the e-mail filter, Mallory sends follow-up messages to Alice claiming that false alarms often happen in the organization. He pressures Alice to open the document containing malware under the pretext of urgency.

Once the VPN channel is active, Mallory places his own orders into the MAE, and it appears as the trades are placed by Alice. Mallory transfers the trade proceeds to his own bank account, and then leaves the country long before the next monthly audit is scheduled. This way, he enjoys the financial benefits of the committed fraud, and he also feels vindicated for not getting the promotion, as the organization has to suffer both financially, as well as due to the loss of credibility in front of its customers.

Case 2: Insider exfiltrates sensitive data with the intent to sell critical information. Trade orders from both private and institutional investors are stored in a database as they are received, and then trade-specialized computers read the

information from the database and execute the trades. Knowing the trades in advance, even by just a few minutes, provides a competitor with valuable information. For instance, a competitor that learns that a large buy order exists for shares of company *XYZ* can buy the shares himself in advance, knowing that the price is very likely to increase.

This time, Mallory sends an email message to the database administrator (DBA). The e-mail contains a malicious attachment that connects to the database, queries the trades that are scheduled to be executed in that day, and immediately transmits the information to an adversary. To avoid detection, the malware first encrypts data contents, and may also use another machine to perform the transfer. This way, network sensor monitors are not able to detect unusual activity between the database server and a machine from outside the organization.

3. DATA-INTENSIVE ARCHITECTURE FOR DETECTION OF INSIDER THREATS

There is a broad area of insider threats in terms of the complexity of the attacks, the attack vectors employed, as well as the specific objective pursued by the attackers. Typical areas of concern in the case of insider threats are:

- *Compromise of information privacy*: e.g., identity theft, extortion against top executives in the organization, etc.
- *Unauthorized Transfer of Funds*
- *Unauthorized Manipulation of Data Input:* e.g., data suppression (denial of service), destruction and/or corruption

Note that, each insider attack typically consists of a combination of the above factors. In order to fully understand the intricacies and interrelationships between each of these components, the leadership and operational personnel need a full understanding the following areas [2]:

- The Insider Threat Planning Process
- Enterprise Architecture
- Protection of Web Sites from Insider Abuse and the IT Infrastructure
- Web Services and Control Considerations for Reducing Transaction Risks
- Application Security and Methods for Reducing Insider Computer Fraud (ICF)
- ICF Taxonomy and the Art of a Key Fraud Indicator (KFI) Selection Process
- Key Fraud Signatures (KFS)
- Application and System Journaling and the Software Engineering Process

3.1 Technical Aspects

Fighting against insider threats involves two distinct aspects: profiling the behavioral aspects of the insider and profiling the behavior of the data. Although the two approaches can be performed individually, studying them collectively helps developing a better understanding of threats. We envision detection and protection against the insider threat as a set of coordinated processes that collect network and service data, analyze patterns of network accesses and interactions, and correlate events in order to expose the tracks of malicious behavior. Typically, organizations collect large amounts of data, in the form of security and audit logs, traces of network flows, service logs such as email, web access, etc. All these represent valuable sources of information that we include in our insider threat detection framework.

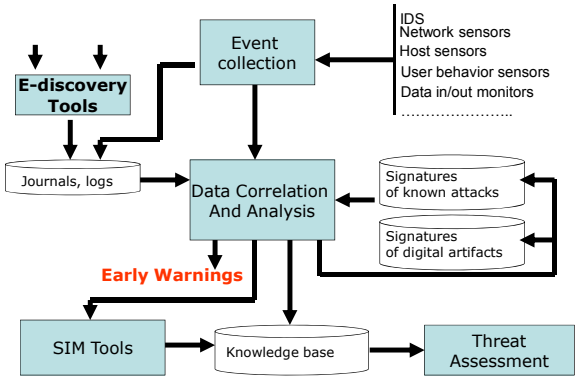

Figure 1: Data-intensive Architecture for Detection and Protection against Insider Threats

The proposed data-intensive architecture is presented in Figure 1, and consists of the following components:

- **Event and anomaly collection.** An essential component of the architecture is concerned with collection of data from a variety of sources, such as intrusion detection systems (IDS), network sensors, security and service logs, etc. As large amounts of data are available in an organization, this component will address issues such as effective and efficient data indexing, storage, querying and classification.
- **Data analysis and correlation.** Sophisticated attackers may customize their attack strategy in a manner that evades conventional signature-based detection systems (e.g., IDS). Still, some common traits do exist that allow the identification of common attack patterns. Such common characteristics can be found in the type of malware that is being used, the pattern of network communication and access to storage, etc. An essential component for insider threat anomaly detection will be represented by *Neural Networks and Associative Memories (NAM)*, which are able to recognize and predict patterns of activity and identify normalcy benchmarks for data/metadata values and associations between all the key people, processes, entities and data attributes. Any event identified as not fitting the benchmark needs to be surfaced and reported as a "red-flag": an early-warning indicator of malicious activity.
- **E-discovery tools.** Detected malicious activity must be properly documented to facilitate subsequent forensic analysis and prosecution of attackers. E-discovery tools allow the collection of necessary evidence, including e-mail, data and service access audit logs, etc.
- **Security Information Systems (SIM) tools.** The proposed threat detection architecture will interface with SIM tools that can process alarms and take appropriate action to confine and fight the attack.

An important aspect of data collection is to generate and maintain provenance and lineage information, in addition to the data contents. Data exfiltration is another major concern in the case of insider threats. To prevent exfiltration, malicious insiders will attempt to disguise the data such that security controls (e.g., deep packet inspection tools) will not detect the leakage of sensitive information. Maintaining secure and accurate provenance and lineage of data helps identifying and preventing attempts of data exfiltration.

3.2 Governance Aspects

At the organizational level, understanding insider threats is a very complex task that involves various methods and means to evaluate many existing interacting factors in order to achieve a complete situational awareness. In brief, there are three fundamental components which need to be evaluated and addressed in any insider threat solution and to strengthen Cyber Situational Awareness (CSA) between all related components:

1) Enterprise Risk Management (ERM): Performing a continuous assessment and evaluation of the integrated business/operational/technology risks is critical to evaluating asset vulnerabilities and requisite layers of protection
2) Threat Modeling: The ability to accurately assess the likelihood and probability of a specific threat vector impacting an enterprise will facilitate the ability to assign a more accurate threat rating which factors in probability and damage potential, as well as operational resiliency into a quantitative and/or qualitative scoring
3) Enterprise Security Architecture (ESA): The effectiveness of establishing the appropriate governance processes over the insider threat issue as well as its many interconnections between other threat vectors (namely, external and APT scenarios), will allow for a greater insight and fusion of seemingly disparate pieces and parts of the insider threat challenge

Using ERM and threat modeling as a backdrop and general context prior to evaluating feasible insider threat solutions, the thrust of the following proposed solution should not be a point in time solution, but rather a solution which originates from continuous monitoring of the enterprise risk assessments, which should include an evaluation of the overall cyber-hygiene of each individual IT infrastructure component, in addition to factoring the situational awareness implications of pervasive cyber risks which factors the confluence of external and insider threats.

An important component in the layered defense associated with insider threat detection is represented by journaling. Keeping logs of events and activities is required from an investigatory, legal and compliance perspective. There needs to be a logical and repeatable process for identifying when journaling for various IT infrastructure components are necessary for digital forensics, trace-back and attribution purposes. To meet the digital forensics purpose, there needs to be some means of capturing data at key points in the creation, transference and storage of these key data attributes at various control points or gates, where personally-identifiable information (PII), classified data or other key information is either inputted into a system, processing is occurring, data is being output and/or transferred within an enterprise or beyond and eventually into storage. The ultimate goal for journaling to detect an insider threat early in the process is to avoid the many complications associated within Massive Information Management (MIM) and data archiving challenges involved with this process, based on the myriad of legal, regulatory and other organizational requirements to ensure the integrity of that data. The second benefit of performing the journaling in the context of insider computer fraud is the importance of having this information to establish a profile of the nominal data values, i.e., values that occur in the absence of attacks. For example, if the normal data value for a given financial transaction ranges between $5 – 10 million and the transaction occurs consistently from only one static IP address, then being able to establish a journaling "clipping level" will be important in the identification of anomalous activity which either exceed or falls below a particular level of normalcy based on the pattern of that data profile.

Finally, the confluence between various cyber attack vectors often make outsiders look like insiders and insiders appear as outsiders. Through enhanced situational awareness, the ability to effectively connect the dots between cyber attack tactics, techniques and procedures and general modus operandi of seemingly disparate conventional network attacks will allow the security architecture designers and others to proactively identify changes in the security architecture of an enterprise from a preventive and not a reactive perspective.

3.3 An Overview of Data Exfiltration Threats

One important aspect in detecting malicious insiders is to track closely their activities. So far we have discussed the importance of monitoring and logging network events. However, tracking individual, disparate events may not always give a clear indication of malicious activity. In addition, in order to correlate multiple events, it is often required to track data items, and to know what were the activities that led to the generation of those data items.

Consider that an insider plants malware in one of the organization machines. In turn, the malware will affect certain files, either local or remote. Since insiders may try to cover their tracks before staging an attack, the malware may travel across several hosts before starting to execute the attack proper. Provenance and lineage techniques can help in the early identification of malware propagation.

Tracking data and event lineage may be achieved using additional tags that can be attached at various layers of abstraction (e.g., inside each network packet). On the other hand, such explicit tags may be visible to the attacker, and alert the insider that his or her actions are being monitored. Therefore, it is desirable to devise tracking mechanisms that are implicit and transparent, in the form of watermarks.

A watermark embedded in the network packets can serve the purpose of tracking malicious activities in a stealthy fashion. Furthermore, unauthorized access to data by malicious insiders may also be achieved with watermarks. Consider that an insider gathers sensitive data from within the organization and stores them on a compromised staging machine or server with the purpose of exfiltrating them at a later time. If data are watermarked, then a simple scanning software function can detect

Method	Frequency
Native Remote Access Applications	27%
Microsoft Windows Network Shares	28%
Malware Capability: FTP	17%
Malware Capability: IRC	2%
Malware Capability: SMTP	4%
HTTP File Upload Site	1.5%
Native FTP Client	10%
SQL Injection	6%
Encrypted Backdoor	<1%

Figure 2: Breakdown of Data Exfiltration Attacks per Transport Mechanism Used

the presence of such data (e.g., a plug-in for an anti-virus tool may achieve this functionality).

In practice, full protection against attacks may be an unfeasible goal, due to the complexity of organization-level networks that often include a large variety of applications, protocols, services, etc. This heterogeneity provides adversaries with a broad spectrum of attack vectors, which complicates the task of defending such networks. Heterogeneity is one of the reasons why conventional firewalls/IDS are not able to defend against data exfiltration, because insiders and APT may choose among many available venues to transfer data beyond organizational boundaries. Often, exfiltrated data are piggybacked on top of conventional traffic, such as web, email or instant messaging. Figure 2 shows the result of a study [3] that measures the breakdown of attacks involving data exfiltration with respect to the network protocols and services used for transport. Note that, due to the flexibility available to attackers, traditional filtering/blocking approaches are not feasible. If attackers use the same channel of communication that is used by legitimate applications, then filtering will block non-malicious traffic as well. Deep-packet inspection is also not suitable, as attackers often use encryption before shipping data off-site. Thus, packet inspection tools that check for tokens that may indicate sensitive packet contents are easily circumvented. Therefore, a data-intensive architecture that relies on correlation of large amount of captured events is required to detect exfiltration.

4. RELATED WORK

Insider threat has been widely acknowledged [1,2] as a very serious and difficult to address cyber-security concern. There are several factors [2] that make insider threats very effective, such as knowledge of the organization network, possession of valid credentials, and the benefit of trust.

Data Exfiltration has been recently acknowledged as an important research problem, and studied in several contexts. In [5], it is shown how data can be exfiltrated by embedding sensitive information in conventional browser HTTP requests. In [6], the authors study exfiltration through covert channels. For instance, the rate of sending packets to a destination can be tuned such that the frequency or inter-arrival time of packets corresponds to an encoding of the data.

Protection of data in the presence of untrusted users or software has been addressed in [4], where a virtual machine monitor is deployed to separate sensitive data and applications from other malicious or untrusted software, e.g., malware, compromised operating system, etc.

5. CONCLUSION

Insider attacks are very effective and often highly damaging, due to the fact that insiders reside within the trust domain of an organization, they are not subject to many security controls that keep external attackers at bay, and they have valid credentials to access systems and services within the organization. In addition, they have knowledge about security configurations that safeguard the network, and they are able to exploit more easily technical, as well as human factor weaknesses within the organization.

The creation of an effective insider threat cyber ecosystem is a significant challenge and requires a robust and mature cybersecurity governance process, which effectively incorporates: enterprise risk management, threat modeling and the enterprise security architecture, which should be a manifestation of understanding the integrated risks and selected mitigated controls, through the addition of new or reinforced security access layers from the network perimeter through to the data layer. The new frontier for anomalistic insider threat detection, monitoring and mitigation will include means of capturing data normalcy and patterns of suspicious activity and predictive modeling that can incorporate "what-if" scenarios that can make the correct associations between various activities and events for optimizing situational awareness for insider threat detection.

6. REFERENCES

[1] J. Leyden, "Geeks, squatters and saboteurs threaten corporate security", http://www.theregister.co.uk/2005/12/15/mcafee_internal_security_survey/

[2] K. Brancik, "Insider Computer Fraud – An In-Depth Framework for Detecting and Defending Against Insider IT Attacks.", Taylor and Francis Group LLC, 2008.

[3] N. J. Percoco, "Data exfiltration: how data gets out", Spiderlabs report. Available online at http://www.csoonline.com/article/570813/data-exfiltration-how-data-gets-out

[4] X. Chen et al, "Overshadow: A Virtualization-Based Approach to Retrofitting Protection in Commodity Operating Systems", In Proc. Of the 13th Intl. Conf. on Architectural Support for Programming Languages and OS, 2008

[5] K. Born, "Browser-Based Covert Data Exfiltration", In Proceedings of the 9th Annual Security Conference, Las Vegas, NV, April 7-8, 2010

[6] A. Giani, V. H. Berk, G. V. Cybenko, "Data exfiltration and covert channels", In Proceedings of Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense, 2006