Insider Threat Prediction Tool: Evaluating the probability of IT misuse

G.B.Magklaras, Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, UK

S.M. Furnell, Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, UK

ABSTRACT

Despite the well documented and emerging insider threat to information systems, there is currently no substantial effort devoted to addressing the problem of internal IT misuse. In fact, the great majority of misuse countermeasures address forms of abuse originating from external factors (i.e. the perceived threat from unauthorised users). This paper suggests a new and innovative approach of dealing with insiders that abuse IT systems. The proposed solution estimates the level of threat that is likely to originate from a particular insider by introducing a threat evaluation system based on certain profiles of user behavior. However, a substantial amount of work is required, in order to materialise and validate the proposed solutions.

Keywords: misfeasor detection, insider misuse, threat prediction, misuse models

Introduction

Information Technology systems have revolutionised our lives in many different ways: They have improved the way we do business, they give us great calculating power so that we can perform scientific calculations and advance our scientific horizon. Today we have reached the point where the smooth functioning of our world depends to a great extent on computer systems. Banking, telephony, air-traffic control, energy and healthcare Information Technology (IT) infrastructures constitute characteristic examples of our increasing dependency on computing systems. The term Information Technology (IT) infrastructure is used consistently in this paper to refer to all software and hardware components of an organisation that collaborate to perform some useful and/or mission critical function (desktop and server systems, computer network and telecommunication components, etc).

However, a great majority of the IT infrastructure components exhibit security flaws that render them susceptible to many forms of abuse. As a result, the IT industry launched a variety of security tools that help users and system administrators prevent, detect and -where possible- counteract IT abuse. Computer anti-virus toolkits, firewalls, Intrusion Detection Systems and IT security policy shaping tools are the most common approaches followed by security experts today.

A plethora of surveys focusing on the origin of these forms of abuse reveals more intriguing facts. The latest Computer Crime and Security Survey of the Computer Security Institute (CSI) **[1]** reports that forty-nine percent of the respondents faced IT security incidents due to the actions of legitimate users. Despite the well documented and emerging insider threat, there is no substantial effort devoted to addressing the problem of internal IT misuse. In fact, the great majority of misuse countermeasures address forms of abuse originating from external factors (i.e. the perceived threat from hackers).

This paper suggests a new innovative approach of dealing with insiders that abuse IT systems. The proposed solution estimates the level of threat that is likely to originate from a particular insider by introducing a threat evaluation system based on certain profiles of user behavior.

A structured approach is suggested that provides a preliminary method for predicting legitimate user misuse. Initially, the subjective nature of the term 'misuse' is addressed and a proposed taxonomy of insider misusers is introduced. A high level overview of the proposed Insider Threat Prediction Tool (ITPT) follows by first presenting a functional block view of the ITPT system and then by proposing a set of

specific insider monitoring criteria. This leads into the core idea of the Insider threat model, by examining the issues concerned with legitimate user threat prediction. Finally, the paper concludes with suggestions for future work that are necessary for the overall development of the system.

The nature of IT insider misuse and a proposed insider taxonomy

Misuse: ***to use (something) in a wrong way or for a wrong purpose***
Longman Dictionary of Contemporary English

Although the great majority of the people are familiar with the generic meaning of the word 'misuse', when we try to map it to an insider IT context, there is a need to clarify certain issues. Insider IT misuse can be a very subjective term. In fact, one of the most challenging tasks is to draw a clear line that separates an IT misuser from a person that is using the available resources in an acceptable way and for an approved purpose. The words 'acceptable' and 'approved' imply the presence of rules that qualify (or quantify) conditions of allowable usage for the resources concerned. These rules are often embodied within an IT usage policy. Part of this organisation-wide policy is the information security policy, defined as the '*set of laws, rules, practices, norms and fashions that regulate how an organisation manages, protects, and distributes the sensitive information and that regulates how an organisation protects system services*' **[2]**.

Different organisations pose different restrictions on IT usage, and this variety of rules adds a considerable level of ambiguity to the term 'misuser'. In order to overcome this uncertainty, it is necessary to introduce a taxonomy of insider misuse incidents. The derivation of such a taxonomy will systematise the deployment of an information security policy across an organisation and is the first step towards the establishment of a threat prediction model.

Although the computer security research community has created a plethora of taxonomies that describe computer intrusions in general **[3]**, little effort has been placed on the construction of a taxonomy that specialises in insider incidents. The earliest attempt to classify internal misuse of computer systems is presented by Anderson **[4]** and discusses borders of distinction amongst **'masqueraders'**, **'misfeasors'** and **'clandestine'** users. 'Masqueraders' are insiders that exploit weaknesses of the authentication modules of a particular application or Operating System, thus gaining the identity of other legitimate users. A 'misfeasor' is an insider that does not need to masquerade, but abuses the power of his/her privileges to misuse the system. Finally, a 'clandestine' user is related with authorised users and their capabilities to bypass audit, control and access resource mechanisms in a particular computer system. However, Anderson's classification is considered too simplistic for the purposes of assessing insider threat: It is good to indicate the failures of authentication systems, as well as the allocation of privileges, but that is not enough information in order to estimate insider threat.

Some studies **[5]** tend to further classify insiders as logical and physical ones. A logical insider operates physically outside the context of an organisation. For instance, consider the case of an employee that uses telnet to connect to his UK company transaction server from China. Other factors, such as operating system authentication techniques, as well as the environment of the user might differentiate amongst logical insiders. On the other hand, a physical insider would connect to the same server, within the physical bounds of the IT infrastructure of the organisation (including buildings, or external trusted networks referred to as extranets). However, if we consider the increased levels of connectivity offered by the convergence of mobile computing and telecommunications platforms, the previously mentioned classification scheme will become less apparent in the near future.

A more recent and comprehensive reference to an insider taxonomy is discussed by Tuglular **[6]**. The taxonomy classifies computer misuse incidents in three dimensions: incident, response, and consequences. These dimensions can be divided into additional sub-dimensions that further classify a particular misfeasor. This approach is certainly an important step in systematising insider misuse classification for two reasons: Firstly, it introduces the first comprehensive taxonomy of misfeasor incidents. Secondly, the usage of a dimension-orientated classification method is particularly useful, not only for controlling the granularity of information presented in each insider class, but also in developing an appropriate set of monitoring tools for

threat estimation. However, the entire taxonomy is oriented towards insider incident response, rather than focusing on a set of classification criteria that could be used as threat evaluation factors. Hence, a different classification approach is needed and the rest of this section proposes a scheme that classifies insider threat in terms of the factors that create it.

At this point, it should be emphasised that the suggested taxonomy of this paper is human centric. It is people who design, use and attack the systems **[7]**. There are also other factors that influence the nature of an IT misuse act, such as the derivation and enforcement of a suitable information security policy and the level of technological complexity employed inside a corporate infrastructure. Nevertheless, all actions that constitute IT misuse lead back to human factors. Thus, a fundamental aspect of an insider taxonomy should be the classification of people in three basic dimensions: **system role**, **reason of misuse,** and **system consequences** as illustrated in Figure 1.

Figure 1: Insider IT misuse classification (top level and system role)

'System role' is concerned with the actual (or perceived) role of a particular person with reference to a *specific* computer system (workstation, server, telecommunication system). The basic criterion for classifying persons in the system role dimension is the type and level of system knowledge they possess. Insiders constitute a greater level of threat than outsiders because of the greater level of knowledge they posses about critical components of the IT infrastructure **[5]**. Hence, it makes sense to use the level and type of knowledge of a particular legitimate user as a threat estimation criterion. As a result, we classify insiders in three basic sub-dimensions:

- **System masters**: It includes all legitimate users of the system that have full administrative privileges to the majority of the system resources. Typical examples are head system and network administrators. This category of legitimate users poses a substantial level of threat to a corporate infrastructure because of the increased level of access and trust they are given.
- **Advanced users**: This sub-dimension includes all legitimate users of the system that have not got increased administrative privileges but do possess a substantial knowledge of the system internals. Application and system programmers, database administrators, as well as previous system masters and current shift operators belong to this category. Although they do not have access to a large number of system resources, they are aware of potential system vulnerabilities.
- **Application users**: This includes the rest of the legitimate users that utilise certain standard applications, such as World-Wide-Web (WWW) browsing, e-mail and database clients. They usually have no additional access to resources, other than the ones required to run their application. Hence, these users are likely to initiate some form of abuse that is related to the application they run (including the resources associated with it).

Another important factor that characterises the nature of insider misuse incidents is the reason they occur (reason of misuse). On this basis, misfeasor acts can be divided into two large categories: **intentional** and **accidental**. This classification is also employed by **[5]**, emphasizing the importance of considering accidental misuse incidents as equally important threats to intentional ones. Indeed, the commercial world is full of unintentional misuse acts that resulted in large financial losses for well-known companies.

Intentional misfeasor cases are performed for a variety of reasons. The best way to sub-divide them is to consider the motives in a way that could detect the ultimate goal of the abuser. It might be inferred, for example, that a legitimate user is trying to access sensitive data (data theft), take revenge against a particular person or an entire organisation (personal differences), cover indications of unprofessional behaviour or deliberately ignore a particular regulation of the information security policy. The later sub-dimension includes all goals that have not been stated and acts as a mechanism of expanding/matching the suggested taxonomy to a specific information security policy.

Data theft is in fact a traditional example of the materiality of intentional IT misuse in several corporate and government organisations. Security surveys and mass media reports are full of cases of ‘industrial espionage’, where legitimate employees have stolen sensitive information for money or for a higher level job in a competitor company. The 2001 CSI/FBI Security Survey cited the case of Robert Hanssen [1], a

56 year-old FBI veteran. It was proven that Hanssen abused his trusted access to the FBI Automated Case Support System that contained classified information about ongoing investigations and handed critical information to Russian agencies. In return, he was receiving large sums of money. Needless to say, the amount of damage inflicted upon the national security, and to the prestigious image of the Federal Bureau of Investigation, was incalculable.

The same CSI/FBI survey also references the case of Abdelkader Smires, a database engineer who worked with Internet Trading Technologies. Smires had personal differences with his employer, and decided to take revenge by using the computers of his previous employer (Queens College) to launch a Denial of Service (DoS) attack - causing several hours of downtime (and lost revenue) over a three day period.

Garfinkel and Spafford [8] examine a different part of the insider misuse spectrum, by briefly mentioning the Leeson-Iguchi case. Nick Leeson (Barings Bank – Singapore) and Toshihibe Iguchi (Daiwa Bank – New York) were investment traders working together for two major financial organisations. They made risky investments and lost large amounts of investment capital. However, instead of admitting their losses, they illegitimately modified computer records in order to obtain more money to cover their losses. The case is certainly a good example of misusing the IT infrastructure in order to cover professional mistakes. The result was catastrophic - Barings was forced to insolvency, Daiwa lost its entire United States customer base, and more that one billion dollars of investment capital vanished.

Despite representing different insider misuse motives, the previously mentioned cases have several things in common. Firstly, all misusers were trusted. They all had important roles inside the organisation and their actions were not questioned. Moreover, they all had intermediate to advanced knowledge of the IT infrastructure. Hanssen was using specially formatted 40-track mode diskettes, in order to hide the sensitive information in (what it appeared to be) a blank area of the disk [9]. Smires exploited certain Operating System vulnerabilities, whereas Leeson and Iguchi knew how to bypass the audit mechanisms of the funding records database. This is a strong point for classifying insider roles in relation to the system infrastructure knowledge they possess.

On the other hand, accidental computer system misuse can be further categorised according to the real reasons that led the legitimate user to the wrong action. Issues such as inadequate knowledge of the system (due to lack of training for example) and factors that can affect work-related performance (excessive workload, emotional problems), have not been addressed adequately and constitute a fruitful area of research. Finally, it is possible that a user is unaware of a particular regulation of the information security policy. Figure 2 illustrates these concepts.

Figure 2: Classification of misusers by reason

The last dimension of our classification **('system consequences')** is concerned with the way a misuse act is manifested at system level. The classification of these consequences forms a very important foundation for the Insider Threat Prediction Tool because it will be the basis for the establishment of its monitoring criteria. It is also greatly influenced by the generic architecture of a computer system. This influence is based on the following rationale: There is a plethora of criteria that could be applied in order to evaluate insider threat. For example, social engineering and pre-employment screening procedures might provide valuable information about the motives and the nature of the misfeasor. However, this type of information is often subjective- thus error prone- as well as difficult to qualify. Hence, it makes sense (especially when building an automated threat prediction tool) to classify the consequences in terms of criteria that can be easily detected by an automated software process. It can, therefore, be proven that almost every form of insider IT abuse (or attempt to abuse) leaves certain traces in basic components of the IT infrastructure.

As a result, there are three primary levels that address these consequences (see Figure 3). The first concerns issues affecting Operating System components (**O/S based**), the second examines threat evidence originating from network traffic (**network data**), and the last concerns any modifications of the physical (**hardware**) architecture of the system. These levels are not mutually exclusive. For example, it is certainly possible (and common) that a particular system misuse can be traced in network data, Operating System components and hardware configuration alterations. It should be noted that the 'system consequences'

classification is in line with the generic division of Intrusion Detection Systems into Host and Network based ones. The similarity is not accidental. An insider threat prediction tool is, in essence, a module of an Intrusion Detection System.

It should be also clear that the Operating System plays a vital role in the process of collecting information about system consequences. Although we separate these consequences into three different types, it is fair to say that Operating System utilities provide access to data concerning all of these categories. Thus, a compromise of basic O/S components may affect the validity of the collected evidence and special care must be taken in order to protect the integrity of systems that collect and manage this type of information.

Figure 3: Categorisation of IT misuse incidents according to system consequences

There are many texts that describe the generic architecture of the two commercially dominant Operating Systems: UNIX **[10]** and Microsoft Windows **[11]**. Despite the substantial differences in the philosophy of their design, it is interesting to note that the core modules of a UNIX or Windows kernel provide (amongst others) two important functions: filesystem and memory management. A large number of recorded security incidents **[12]**, as well as security faults **[13]** involve filesystem and memory management issues. Hence, it is safe to assume that these two kernel functional attributes can be used as a strong criterion for further classifying system consequences.

Attempts to modify the structure of a filesystem, to erase or modify or execute a particular file, as well as the storage of unauthorised software (such as unlicensed software tools, pornographic materials, games and trojan horses) are good ways to illustrate how an insider misuse act can be traced by inspecting the filesystem. The Hanssen and Leeson-Iguchi cases are traditional examples. In the earlier case, the fact that several files were transferred into a specially formatted floppy diskette would be suspicious evidence, if it was recorded on an audit file. In the later case, the fact that critical records files were updated by means of an unusual tool (other than the record database application itself), or perhaps during unusual times, would reveal the effort of trying to cover up strong evidence. On the other hand, excessive memory usage as well as attempts to access protected memory areas that are related to a legitimate user account can serve as good indicators of insider misuse at Operating System level.

Network traffic is another factor that could be taken into consideration, in order to classify insider misuse. Network packets may be carrying unauthorised content of interest and/or constitute protocols, as well as source and destination address endpoints that might be forbidden. For example, the Smires case should leave plenty of footprints for the system and security administrators. The misuser used specific hosts to launch his attacks. If somebody is able to trace (prior the commencement of the attacks) certain probes with an IP address that points to a specific academic domain, then that would look fairly suspicious with regards to what is about to follow.

Finally, the hardware configuration of a particular machine plays an important role in preventing a number of computer system threats. Removal and vandalism of components, as well as accidental or intentional modifications of their default configuration, are important classifiers of the way certain misuse acts are manifested in a computer system.

The Insider Threat Prediction Tool: Architectural considerations

After the derivation of a suitable taxonomy for insiders, this section discusses the model itself and its surrounding framework. The fundamental idea behind the model is explained and its modular architecture is presented.

The best way to introduce the ITPT system is to examine how it differs from current computer security tools. The majority of computer security tools are designed to address '*threats*'. In this context, a threat is defined as a mechanism or event that has the potential to harm the system. For insider misuse cases, the harm can be in the form of one of several misuse incidents as described in the proposed taxonomy of the previous section.

The difference between the suggested model and traditional security tools lies in the way threats are addressed. For example, firewalls and anti-virus tools detect threat by considering certain signs of the occurrence of the misuse: capturing of connection attempts to an unauthorised IP address and the presence of a particular file in a specific directory structure are some characteristic examples. An Intrusion Detection System (IDS) provides a more comprehensive framework for the detection of a greater variety of threats, by using different analysis approaches discussed in **[14]**. An IDS may also address issues such as automated threat response.

All the previously mentioned tools address a particular threat at the moment of its occurrence. The Insider Threat Prediction Tool follows a different approach by detecting signs that could lead to a particular misuse act. Thus, although it can detect certain misuse actions, it is primarily a threat predicting tool rather than a pure threat detection tool. Moreover, the overall architecture should be Operating System independent: every organisation is likely to employ more than one Operating System in its infrastructure. The system is also intended to be part of the Intrusion Monitoring System, a conceptual architecture for real-time monitoring of computer system intrusions **[15]**.

Figure 4 below illustrates the functional blocks of the Insider Threat Prediction Tool, providing an insight of the high-level implementation details of the proposed tool. The arrows represent the direction of information flow amongst the various system modules.

Figure 4: High-level architecture of the ITPT system

The *'ITPT manager'* coordinates the operation of the various modules and provides the Graphical User Interface (GUI) for the human operator. The GUI sub-module should provide an easy-to-use interface for constructing suitable monitoring criteria (thus embedding the information security policy in the ITPT system), as well as a way to display the results obtained after analysing the collected data.

The 'collected data' buffer will be read by the 'ITPT analyser' module that constitutes the heart of the overall system. The purpose of this module is to perform the actual process of insider threat estimation. It represents a separate entity itself, mainly because it is possible to use a variety of algorithms to predict threats. In fact, the use of more than one algorithm to predict the level of threat is a desirable feature. If someone considers the research and development efforts in the Intrusion Detection Systems area, it is clear that certain intrusions are best detected by using statistical processing techniques, whereas others are more reliably detected by pattern matching (signature-based) approaches **[14]**. Hence, being able to utilise a variety of approaches to process the collected data is an important feature that will increase the reliability of the ITPT analyser and ease the process of updating the system with improved algorithms. The definition of suitable algorithms for insider threat prediction is out of the scope of this paper, however a preliminary Insider Threat Prediction Model (ITPM) is discussed later in this paper.

The output of the ITPT analyser is a set of 'threat profiles' for all users of the system. Each threat profile classifies a user into one of four main insider **categories:**

- **Possible intentional threat:** The system has found evidence which suggests that it is very likely a particular user will initiate a specific misuse action.
- **Potential accidental threat:** The system has detected evidence that a user is about to perform a particular type of misuse, by accident.
- **Suspicious:** The system has detected a set of suspicious user activities, but it is not clear whether these actions indicate potential misuse activities.
- **Harmless:** There is no evidence that the user is likely to initiate any sort of undesirable action.

A system administrator can then view an individual's profile, read the current level of estimated misuse threat and be informed about its nature and the action(s) that the system believes are a good indication of what is likely to occur.

The '*monitoring module*' is responsible for the collection of all types of data as dictated by the '*monitoring criteria*' configuration file. The module controls a series of data collection sub-modules. At this point, it

becomes clear that the suggested type of the data collectors is in line with the suggested taxonomy of insider misuse system consequences. This coherence is an intentional architectural choice and it indicates the importance of deriving an insider taxonomy, which justifies types of suitable monitoring criteria. The data collection modules will finally report their results back to the monitoring module and the file containing the 'collected data' will be updated.

Every sub-module provides a 'monitoring abstraction' mechanism. This means that a monitoring sub-module separates the high-level action details that indicate signs of insider misuse from the low-level procedures of their manifestation. In other words, we should be able to obtain facts about suspicious file, memory, network or hardware configuration operations without caring whether these occur on a Microsoft Windows NT system running NTFS or a UNIX flavor that employs a less common filesystem format. The idea is that the monitoring sub-modules report events in a standardised way and the extraction of the abstract details is done by interacting with the Operating System Applications Programming Interface (API). As a consequence, cross-platform compliance issues concern only the monitoring sub-modules themselves and not the rest of the functional blocks of the system.

The filesystem sub-module is responsible for detecting the following high-level file operations:

- **File and directory location:** Locating the presence of certain files and directories, according to the following criteria: file or directory name, file extension, file type (data versus binary). Certain misuse actions might include the placement of certain files in particular places. For example, when somebody installs unauthorised software, the executable files usually reside in certain directories.
- **File content extraction services:** Extraction of strings or desired data patterns from files. A typical example is the detection of suspicious words, virus signatures, log files that indicate configuration information or evidence of executing certain applications.
- **File integrity check:** It includes checksum operations (generation and verification), as well as examination of file timestamps (creation, last read and last write dates) ownership and change of file ownership detection.

The memory monitoring sub-module watches for irregular memory usage patterns. The inner nature of buffer overflow attacks points to memory mismanagement techniques **[16]**, whereas **[17]** outlines how primary memory can be manipulated for initiating a variety of network based attacks. Hence, traditional Intrusion Detection Systems view suspiciously applications that suddenly request large memory chunks, or try to repeatedly access a classified memory area. When it comes to potential insider threat detection, the most important thing to consider is the content of particular memory locations, where an application resides. This is important for two reasons: First of all, a program is a process in execution. It is imperative that we know what applications the user is running. The only way to achieve this is to be able to inspect the running program. The memory footprint of an application provides an indisputable proof of its execution. In addition, it is better to examine a program in execution, simply because its contents (instructions and data) can then be viewed in their native format. For example, it is possible that a particular application file contains suspicious content. However, the content might be compressed and/or encrypted prior to the execution of the application. As a consequence, the filesystem and network monitoring modules could fail to spot the presence of the 'payload' in the system. The only culprit with memory monitoring is that it is computationally intensive. Hence, system administrators are likely to reject this method due to its severe impact on system performance. Further processing can then follow and record suspicious contents. The extracted content could then be cross-referenced with results from other monitoring modules to make deductions about the level of potential threat (ITPT analyser). Finally, the memory module should keep account of the amount of total amount of memory used per user.

Certain aspects of the 'Input/Output' (I/O) mechanisms of a computer system could be exploited to launch severe IT attacks. In the context of this paper, the term 'Input/Output' refers to a structured path of information flow between running programs (interprocess communication) or discrete hosts (end-to-end communication) **[18]**. The earlier case is difficult to handle from a security point of view. It concerns certain kernel Operating System blocks that are difficult to inspect and modify. On the other hand, end-to-end communication is a more approachable area, giving birth to the field of Network Intrusion Detection. A comprehensive and up-to-date description of all aspects of network originated threats is given by **[17]**.

Frequently used intrusion detection techniques try to intercept threats by means of packet payload pattern matching or network traffic examination (traffic analysis based on protocol and bandwidth monitoring). However, these techniques are computationally expensive. In a system with thousands of users and enterprise networking backbones that reach speeds in the region of several Gigabits per second, it will not be feasible to perform all these actions on a real time basis. Instead, we need more threat prediction orientated criteria that are less expensive in terms of CPU and primary memory resources.

A set of 'well-known ports' (TCP and UDP ports 0-1,023) is listed in **[19]**. These ports correspond to particular services that introduce a number of vulnerabilities for the computing system and the entire enterprise IT infrastructure. An excellent reference that associates the set of well-known ports to particular vulnerabilities can be found in **[20]**. It is possible to use this association in order to aid the process of legitimate user threat prediction. The principle dictates that a legitimate user constitutes an accidental system threat element, if he/she uses protocols that have been associated with security incidents.
There is a good reason why we associate network monitoring with accidental misuse: If a legitimate user x is about to misuse a particular system intentionally, proper engineering of the filesystem and memory monitoring modules should ensure that some evidence about user x intentions should be intercepted. However, if another legitimate user y (of the same organisation but **acting from a different system**) attempts to misuse the same system via the network, the host is prone to misuse via user x actions, simply because user x is utilising protocols that are vulnerable.

The exact details of the protocol-vulnerability association and the way it affects the perceived potential threat create the need for a database of network port vulnerabilities. The ITPT analyser module should then consult this database, monitor the relative usage of networking protocols information from the I/O module and adjust the potential threat accordingly (per single user basis).

Finally, the hardware monitoring module has the special role of associating changes of the physical configuration of the machine to users with advanced privileges in the system. A number of insider misuse cases prove that head system or network administrators constitute a substantial element of threat. In some cases, before performing intentional or accidental misuse actions they had performed minor hardware changes. The identification of these changes and their classification in terms of threat prediction is a fruitful area of research.

The Insider Threat Prediction Model: A preliminary design

After discussing the high-level architectural details of the ITPT system, this section presents the Insider Threat Prediction Model (ITPM), which constitutes the central element of the ITPT analyser module. The development of such a model is of outmost importance for the function of the ITPT system, because it qualifies (and quantifies) certain metrics of threat estimation. The qualification of metrics is the procedure that decides which aspects of a legitimate user actions and attributes can be used for the purposes of threat prediction. The quantification of metrics determines the relative weight of each metric within the overall threat prediction process. Some metrics are more important than others, and their overall contribution towards the threat assessment process should be adjusted accordingly.

Prior describing the proposed model, it should be stated that the development of insider threat models is not a new idea. The first comprehensive approach for devising a model that simulates the behavior of a malicious insider is discussed by **[21]**. The paper provides an excellent basis for qualifying a set of metrics to mitigate insider threat. Most of these criteria are in line with the ones proposed by the previously presented insider misuse taxonomy. However, due to its introductory scope, the description of the model does not deal with the quantification of insider threat metrics. It also concentrates on malicious (i.e. intentional activities) without considering accidental insider misuse actions. Hence, we need a more formalised and broader model description. The following paragraphs provide a preliminary description of the proposed model.

The core of the Insider Threat Prediction Model is a three-level hierarchy of mathematical functions evaluated in a bottom-up approach. At the top, the **Evaluated Potential Threat (EPT)** function provides a value that classifies each legitimate user into one of the four insider categories described in the previous

section (i.e. possible internal threat, potential accidental threat, suspicious, harmless). The input of this function consists of the mathematical summation of the threat component function outputs. Each of the threat component functions models particular aspects of insider attributes and behavior. At the moment, in order to devise a well structured organisation of threat components, the suggestion is to provide three threat component functions. The first one considers legitimate user attributes, the second evaluates potential threat simply by examining aspects of user behavior at the system level. Finally, the third one considers evidence provided by external modules providing an integration gateway with the Intrusion Monitoring System (IMS) architecture described in **[15]**. Figure 5 below illustrates the proposed formulae.

Figure 5: The three-layer ITPM function hierarchy

The attributes of a legitimate user can be viewed as the sum of weighted constants and functions produced by considering the role he/she has in the organisation (C_{role}), as well as his/her level of access. This paper has already proposed three different insider system roles (system masters, advanced users and application users) and indicated the level of threat they introduce. Later refinement of the model can assign a constant numerical value for each one of them, in order to associate the system role to the threat prediction process. On the other hand, the system access level should also be defined as a sum of weighted factors that link access to critical system components with threat prediction. Access to sensitive data files and configuration tools (C_{data}), as well as the ability to alter physical components ($C_{hardware}$) of the machine can serve as a useful metric of legitimate user misuse prediction.

The threat prediction metrics associated with the system behavior of a legitimate user evaluate the level of his/her system knowledge, the entities in their personal filesystem space (file content) and the type of networking traffic they generate. Each of these criteria is evaluated by a specialised function that resides at the third level of the ITPT function hierarchy. $F_{knowledge}$ examines the types of applications invoked by the user, as well as the various commands he/she issues in the system. By looking at these parameters, we can infer the level of sophistication of the user in terms of his/her system knowledge. $F_{content}$ assesses various file entities owned by a particular user. The name, content and validity of certain files (suspicious executables, scripts, files uploaded as e-mail attachments) contain evidence about the intentions of legitimate users. Lastly, $F_{network}$ associates the usage of certain networking protocols with the possibility of accidental misuse, as described earlier in the paper.

The description of this preliminary Insider Threat Prediction Model concludes with a discussion of the $F_{imsinfo}$. The role of this function is to parse the records produced by the Intrusion Monitoring System '*Archiver*' module. The format of the records is discussed in **[15]**. In particular, the function parses the '*User/Process ID*' and '*Logged Event*' record fields and updates the Estimated Potential Threat (EPT) by considering previous intrusive incidents of a particular user. Hence, this mechanism provides an integration path that transfers information from the Intrusion Monitoring system to the Insider Threat Prediction System. This information is used to enhance the reliability of the insider threat prediction process, as previously detected user intrusions indicate a greater level of potential threat. In addition, it is possible to disseminate useful information in the opposite direction. Large user EPT values can be used by the IMS '*Collector*' and '*Controller*' modules, in order to adjust the auditing resolution of certain user profile metrics and make the system more efficient.

Conclusions and future work recommendations

This paper has described a taxonomy of insider misuse actions. The proposed taxonomy is the basis for devising the high-level architecture of the Insider Threat Prediction Tool (ITPT), a system that aims to predict both intentional and accidental computer system misuse that originates from legitimate users. At the heart of this tool lies the Insider Threat Prediction Model, which performs the actual process of threat prediction.

The proposed architecture is a result of empirical research efforts, after reviewing recent case studies and advances in the field of Intrusion Detection Systems and Insider Threat modeling. However, this is not adequate for deploying an ITPT prototype system. Further investigation, coupled with applied systematic research is required in a number of areas outlined in the following paragraphs.

Firstly, the definition of a more precise architectural framework for the system is required. This will address issues such as the selection of appropriate development tools and a standardised protocol for message exchange amongst the various ITPT components. It will also consider the development of mechanisms to enhance the cross-platform compatibility, scalability and integrity of the ITPT system.

An additional area of recommended work concerns the algorithmic development of the proposed Insider Threat Prediction Model (ITPM). This will involve the development of detailed functions and the challenging process of producing a suitable data set, in order to validate the refined model.

Finally, the integration of the system with the Intrusion Monitoring System (IMS) architecture, as well as other Intrusion Detection System approaches, is another working area that should be considered during the last stages of the prototype development.

Nevertheless, the authors hope that the discussed architecture will contribute towards the solution of the insider threat problem, and provide a framework for further discussion and refinement of processes and tools that aim to address the problem of insider threat in Information systems.

References

[1] Power, R.|(2001), '2001 CSI/FBI Computer Crime and Security Survey', Volume VII- No.1, Computer.

[2] Caelli W., Longley D. and Shain M. (1991), 'Information Security Handbook', Stockton Press.

[3] Furnell S.M., Magklaras G.B., Papadaki M. and Dowland P.S. (2001), 'A generic taxonomy for Intrusion Specification and Response', Proceedings of Euromedia 2001, Valencia, Spain, 18-20 April 2001.

[4] Anderson, J.P. (1980), 'Computer Security Threat Monitoring and Surveillance', 1980.

[5] Neumann, P.G. (1999), 'The challenges of Insider Misuse', SRI Computer Science Laboratory, Paper prepared for the Workshop on Preventing, Detecting, and Responding to Malicious Insider Misuse, 16-18 August 1999, at RAND, Santa Monica, CA.

[6] Tuglular, T. (2000), ' A preliminary Structural Approach to Insider Computer Misuse Incidents', EICAR 2000 Best Paper Proceedings: pages 105-125.

[7] Shaw E.D., Ruby K.G. and Post J.M. (1998), 'The Insider Threat to Information Systems'**,** Security Awareness Bulletin, No 2/98, Political Psychology Associates, Ltd.

[8] Garfinkel S. and Spafford G. (1996), 'Practical Unix & Internet Security', O'Reilly & Associates, Cambridge, 1996: Chapter 13.

[9] Verton, D. (2001), "Spy case demos insider threat", Computerworld.com news report, 26 February 2001. http://www.computerworld.com/cwi/story/0%2c1199%2CNAV47_STO58062%2C00.html

[10] Bach, M. (1986), 'The design of the UNIX Operating System', Prentice Hall International Editions, NJ, 1986.

[11] Richter, J. (1997), 'Advanced Windows', Microsoft Press, Redmond, Washington, 1997.

[12] Howard, J.D. (1995), 'An analysis of Security Incidents on the Internet [1989-1995], PhD Thesis, Carnegie Institute of Technology, Carnegie Mellon University.

[13] Aslam T., Krsul I. and Spafford E. (1996), 'Use of a Taxonomy of Security Faults', Technical Report TR-96-051, COAST Laboratory, Department of Computer Sciences, Purdue University, IN, 1996.

[14] Bace, R.B. (2000), 'Intrusion Detection', Macmillan Technical Publishing, Technology Series, IN, 2000: Chapter 5.

[15] Furnell S.M. and Dowland P.S. (2000), 'A conceptual architecture for real-time intrusion, monitoring", Information Management and Computer Security, Volume 8, Number 2, MCB University Press, 2000: pages 65-74.

[16] Frykholm, N. (2000), 'Countermeasures against Buffer Overflow Attacks', White Paper, RSA laboratories, November 2000.

[17] Moore D., Voelker G.M. and Savage S. (2001), 'Inferring Internet Denial of Service Activity', paper to appear at the USENIX Security Symposium, Washington DC, August 2001.

[18] Spatscheck, O. and Peterson, L. (1997), 'ESCORT - A path-based OS Security Architecture.',Technical Report TR-97-17, Department of Computer Science, The University of Arizona, Tucson, November 1997.

[19] Reynolds J. and Postel J. (1994), 'Assigned Numbers', Request For Comment (RFC) No. 1700, Network Working Group, Internet Engineering Task Force.

[20] Chirillo J. (2001), 'Hack attacks revealed: A complete reference with custom security hacking toolkit', Wiley Computer Publishing, New York.

[21] Wood, B. (2000), 'An insider threat model for adversary simulation', Cyber Defense Research Center, SRI International, position paper presented at the Proceedings of a Workshop with title 'Research on Mitigating the Insider Threat to Information Systems', at RAND, Held August 2000, Arlington VA.