Modelling of Enterprise Insider Threats

Puloma Roy and Chandan Mazumdar
Centre for Distributed Computing, Jadavpur University, Kolkata, India

Keywords: Insider Threat, Insider Attacker, Enterprise.

Abstract: In this paper, a position has been taken to include the non-human active agents as insiders of an enterprise, as opposed to only human insiders as found in the literature. This eliminates the necessity of including the psycho-social and criminological behavioural traits to be incorporated in the management of insider threats. A framework of an Enterprise has been developed and it is shown that within the framework, both the human and non-human agents can be modelled as insider threats in a uniform manner. An example case has been analysed as supporting evidences for the point of view.

1 INTRODUCTION

In the recent past, damaging attacks initiated by authorized insiders have become vital security issue for all business organizations. According to US CERT survey 2013, 53% of high impact enterprise security breaches are perpetrated by insiders (CERT, 2013). Recently the PWC survey of June 2013 assigns a figure of about 50% for the same scenarios (PWC, 2013). Thus for proper identification and mitigation of insider sabotages, it is imperative to model and analyse malicious insider entities of an enterprise.

According to general point of view, only human beings associated with an enterprise (e.g. employee, vendors etc.) and having malicious intentions are treated as insider threat. For modelling such threats, the psychological and social behavioural characteristics of these human agents are taken into account. But as these traits are extraneous to the software systems, it becomes difficult and sometimes controversial, to incorporate them into the analysis and implementation. On the other hand, in today's enterprises, some non-human active entities like rogue software or network elements with embedded malicious software, can also act as threat- and attack- agents to the system. Though failures of IT systems have long been taken into account for availability analysis and improvement, the role of non-human agents as insider threats has been largely ignored.

The position taken in this paper is that both human and non-human agents may be insider threats to an enterprise. The agents which are capable of subverting the Business Processes and Management Processes can become insider threats and insider attackers. Thus a single model of insider threat can encompass both the kinds of agents. It has been shown how such a model can be developed without considering psychological or criminological traits of the agents.

The rest of the paper is organized as follows: Section 2 discusses some related research. Section 3 introduces the proposed framework for modelling of the Enterprise to facilitate the identification of agents and insiders. In Section 4, an insider threat and attacker model has been proposed and two cases have been analysed as evidence. Finally, Section 5 concludes the paper with some pointers for further research.

2 RELATED WORK

A lot of research on insider threat modelling has already been done. Some of them are based on human behaviours. These models mainly depend on the psychosocial behaviour of malicious insiders (Greitzer, et. al., 2010), (Greitzer, et. al., 2009), (Legg, et. al, 2013), (Nurse, et. al., 2014); they consider an employee's "psychosocial" data to predict or detect insider threats and introduce a threat mitigation procedure. Some insider threat models are based on criminological theories (Coles-Kemp and Theoharidou, 2010), (Greitzer and Hohimer, 2011). The Crime Theory techniques are based on cultural response to enhance the

Roy P. and Mazumdar C..
Modelling of Enterprise Insider Threats.
DOI: 10.5220/0005327901320136
In *Proceedings of the 1st International Conference on Information Systems Security and Privacy* (ICISSP-2015), pages 132-136
ISBN: 978-989-758-081-9

information security management. The attributes which are considered for this type of model are: logical or physical location, authorization, expected behaviour, motivation and trust. According to this theory insider abuses can be controlled by four steps, which are: deterrence, prevention, detection and remediation (Coles-Kemp and Theoharidou, 2010). Other models deal with Intellectual properties (Moore, et. al., 2009), (Moore, et. al., 2011). In this approach, there exist two types of scenarios. One is termed Entitled Independence scenario. Here, it is assumed that an insider acts alone to steal information. The other scenario is known as Ambitious Leader scenario, in which a leader facilitates and influences insiders for stealing critical information. Some access control models based on graphical approach (Althebyan and Panda, 2008), (Eberle and Holder, 2009), or policy based representation (Bishop, et. al, 2010), (Bishop and Gates, 2008), are also used for insider threat modelling. These models help to identify the users who have access to high value resources and may cause damages to organizational assets. According to this approach, every insider of an organization should have a level of access which may be privileged, or ordinary, or full (Bishop, et. al, 2010). In case of graph-based approaches, a graphical representation of access control threat model is provided. On the other hand, Carlson's Unification Policy Hierarchy presents a hierarchical approach to insider threat modelling (Bishop, et. al, 2010), (Bishop, and Gates, 2008).

As is obvious from the above discussion, the existing models of insider threats are usually based on social aspects like human behavior, mental state or access rights. In many of the cases, these parameters are fuzzy or statistical in nature. Use of these parameters is sometimes controversial also. Most of the published models concentrate only on the human agents. The behavioral and psychology-cal traits are basically extraneous to the enterprise information system. Moreover, these methods do not consider the technological details of enterprise information architectures. Also, these models do not capture active agents like malicious software and network components with embedded malicious software as insider threats.

3 A FRAMEWORK FOR ENTERPRISE MODELLING

Enterprise is the common illustration of organization. In general an "enterprise" is defined as an organization (Industry / Govt. / Academic) created for business ventures. In today's enterprises, because of web-connection and outsourcing of data and services, it is very difficult to delineate the boundary. Following are the definitions of Outsider and Insider of enterprises proposed in this Position paper.

Outsider and Insider are spatio-temporal concepts. We define an entity to be an outsider to an enterprise during a particular time interval, if the entity does not have any access to the enterprise assets. An Insider, on the other hand, has access to the enterprise assets. An Insider Threat is an insider entity of an enterprise that has the capability and intent to cause harm or danger to the assets. At a particular time interval an insider threat may become an Insider Attacker if it attempts to perpetrate an attack to an enterprise asset and cause some harmful effects by breaching any of the security properties of the enterprise.

3.1 Enterprise Model

An enterprise is characterised by a set of primary assets: Processes (both Business Processes and Management Processes), Information and some Intangible assets (e.g. reputation, goodwill, recommendation, and trust). Since the intangible assets do not play any direct role in enterprise security, we do not include them in our model of enterprise. Thus, an enterprise can be defined as follows:

$$En = \{\{P\}, \{Info\}\} \quad (1)$$

Where {**P**} is the set of processes and {**Info**} is the set of information assets of enterprise **En**.

Executions of processes are enabled by supporting assets: hardware, software, network, site, personnel, and organizational structure.

Information assets are usually utilized / created by Business Processes and are managed by Management Processes. Information assets are stored and manifested by data, which are stored in structured form or unstructured documents. A major goal of security is to maintain the confidentiality, integrity and availability of the structured and unstructured data of an enterprise.

An enterprise process is a workflow of a sequence of activities to achieve a certain goal. An activity includes task structures, which may be sequential, conditional, iterative or parallel. Each structure has single entry and single exit point. A task can be represented by a function having some input data and output data and causing a change of

state of the process. Processes can be represented at different levels of granularity depending on the level of details necessary. Goal of security is to ensure that the processes are not subverted and they are completed to achieve their designated goals.

3.2 Agent Model

An enterprise task requires a set of supporting assets or entities for its execution. Out of these entities, the personnel, software (running on some hardware) and active network components are termed as Agents. Agents can be command-initiated or self-initiated and can work in an unsupervised manner for a period of time. Agents are responsible for creating outputs and change of state of the process. Agents may be categorized as outsider or insider with respect to a process. These categorizations vary with time and access state.

An agent which is not getting access to any task of a process at a particular time in authorized or unauthorized way is an Outsider to the process. An agent having access to any task of a process in an authorized or unauthorized way is an Insider agent. Insider agents of a process may have the capability and intent of subverting a task and, hence a process. As such, all the insider agents can be treated as potential threats to the enterprise. Out of the potential threats, some agents may exploit the vulnerabilities existing in the process or the supporting assets by taking advantages of their insider properties (accessibility, authorization, specific inside knowledge, trust) for malicious motive. These agents are insider threat agents. At times an insider threat agent perpetrates an attack which leads to some damaging incidents, compromising the security of the enterprise. These insider threat agents are known as insider attack agents.

But it should be noted that all insiders may not exploit the vulnerabilities existing in the system. Among the insider agents a few Insider agents may also exploit the enterprise vulnerabilities in an unintentional (accidental / erroneous) way.

As far as IT behaviours are concerned, it is difficult to differentiate between the malicious and unintentional insider threat agents. The appropriate identification of insider threat agents and attack agents may give rise to better prevention, mitigation and recovery procedures for the enterprise.

4 MODELLING OF INSIDER AGENTS

Finite State Machines, particularly, Mealy Machines are being used for modelling various types of systems, including Synchronous digital hardware, Fault Tolerance, Software systems, etc. Recently some efforts have been reported to model enterprises using Mealy Machine (Meijer and Kapoor, 2014). There is a considerable amount of published work on learning of Mealy Machines in different domains, such as in (Shahbaz and Groz, 2009). In this paper we use the concept of Mealy Machine for modelling Business and Management Processes.

A Process (both Business and Management processes) can be defined by an Augmented Finite State Mealy Machine:

$$M_p = (I, O, St, Ag, f_{tr}, f_o, st_0) \quad (2)$$

Where,

I is a finite set of input data of the process P,

O is a finite set of output data of the process P,

St is a finite set of states of the process P,

Ag is a finite set of agents associated with process P,

$\mathbf{f_{tr}}: \mathbf{I} \times \mathbf{St} \xrightarrow{ag} \mathbf{St}$ | ag is a subset of **Ag**

is a state transition function,

$\mathbf{f_o}: \mathbf{I} \times \mathbf{St} \xrightarrow{ag} \mathbf{O}$ | ag is a subset of **Ag**

is an output function,

$\mathbf{st_0} \in \mathbf{St}$ is initial state of process P

Agents act as enablers of a process. These enablers have direct access rights to other supporting assets and use them to execute the activities of the process. Thus for a particular process state *st* of process P, the corresponding agent subset *ag* acts as insiders to the process.

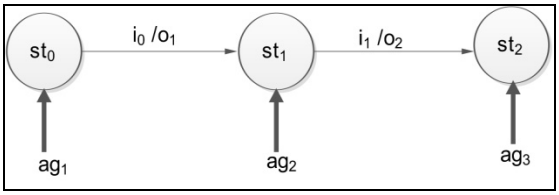

Figure 1: An Augmented Mealy Machine.

The above figure shows part of a process as an Augmented Mealy Machine. The transitions of the machine are labeled with the input and outputs.

The states are labeled with the agent subsets which are responsible to carry out the transition function and the output functions at that state. The processes are designed with the intention of keeping each state in a legitimate state, the so-called "secure state". But due to the presence of vulnerabilities in the states and the malicious activity of the agents, the output functions and the transition functions may be modified to produce undesired outputs, and taking the system to an "insecure state" respectively. These types of activities of agents are thus termed as "attempts" and "attacks".

The set of states **St** can be classified as *safe, unsafe* and *compromised*. A *safe state* is a legitimate state having no information compromised or no agent having gained access permission(s) in an unauthorized way. An *unsafe state* may be legitimate or illegitimate, with possibilities of an agent doing some malicious activity, but not yet having compromised any information or subverted any activity of the concerned Process. A *compromised state* is an illegitimate state where some information has been compromised or one or more activities have been subverted. An agent subset causing transition from one legitimate state to another legitimate state is a normal insider subset, possibly containing potential threat agents. An agent subset causing a transition from one legitimate state to an illegitimate unsafe state clearly contains one or more *insider threat agents*. Similarly, an agent subset causing a transition from one legitimate or unsafe state to a compromised state definitely contains one or more *insider attackers*. *Recovery transitions* consist of transforming a compromised state or an illegitimate unsafe state to a legitimate state.

The following is an example case for arguing in favour of the proposed position.

In the example case, a malicious user installs a keystroke logger hardware or software on a shared computer and retrieves password information of other unsuspecting users from it. The example is depicted by three instances of the Mealy Machine in Fig. 2. Fig. 2(i) shows a legitimate transition, where User A logs into the System. Fig 2(ii) shows how a malicious user, User B, after login, installs and activates a key-logger, thereby transforming the Process state to an unsafe state. In Fig. 2(iii), User A logs in the system again, but this time start state S_4, is an unsafe state. Because of the presence of a non-human insider agent, the key-logger, the password of user A is stored into the cache of the key-logger. Thus the confidentiality of the

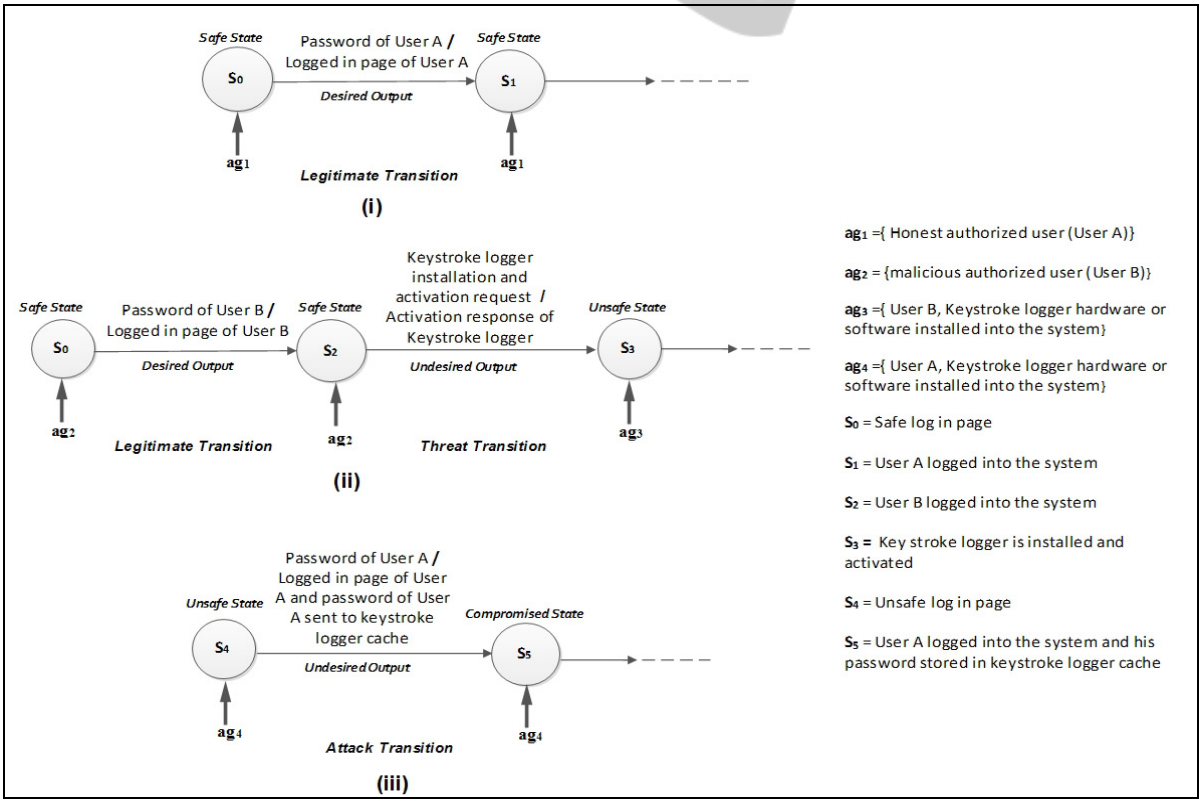

Figure 2: Example Case.

password of User A is breached and State S_5 is a compromised state. Thus the transition of Fig 2(iii) is an attack transition.

Agent sets ag_2, ag_3 and ag_4 contain one or more insider threats of human or non-human kind. The process states associated with these agent sets depict the transitions corresponding to the malicious activities of the insider threat agents, leading the process to the unsafe and compromised state. Thus this simple model can describe both human and non-human insider threats uniformly. There is no need to include the psycho-social behaviours in the model. Only State monitors are sufficient for detection and management of Insider threats.

5 CONCLUSIONS

The position taken in this paper that both human and non-human agents may be insider threats to an enterprise, has been shown by the example case. Use of Mealy Machine to model the Processes enables the modelling of human and non-human insider threats uniformly without the use of the Psycho-social behaviour of human agents.

Further research is geared towards including time and space parameters in the Augmented Mealy machine representation of processes. Based on this complete model of processes, algorithms will be developed to ascertain the level of insider threat and for threat mitigation, attack detection and corresponding recovery procedures.

ACKNOWLEDGEMENTS

This research was partially supported by grants allocated by the Department of Electronics and Information Technology, Govt. of India.

REFERENCES

Althebyan, Q., Panda, B., 2008. Performance *Analysis of An Insider Threat Mitigation Model*. In *3rd International Conference on Digital Information Management*, ICDIM IEEE.

Bishop, M., et. al, 2010. *A Risk Management Approach To The "Insider Threat"*. In *The Insider Threats in Cyber Security, Advances in Information Security*, SPRINGER.

Bishop, M., Gates, *C.,* 2008. *We Have Met The Enemy And He Is Us*. In *The workshop on New security paradigms,* ACM.

Coles-Kemp, L., Theoharidou, M., 2010. *Insider Threat and Information Security Management.* In *Insider Threats in Cyber Security*, SPRINGER.

CERT, 2013.*Cyber Security Watch Survey, "How Bad Is the Insider Threat?*", Carnegie, Mellon University.

Eberle,W., Holder, L., 2009. *Insider Threat Detection Using Graph-Based Approaches*. In *Cyber security Applications & Technology Conference For Homeland Security*, IEEE.

Greitzer, FL., et. al, 2010. *Identifying at-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats*. Pacific Northwest National Laboratory Richland, Washington.

Greitzer, FL., et. al., 2009. *Predictive Modeling for Insider Threat Mitigation*. Pacific Northwest National Laboratory, Washington.

Greitzer, FL., Hohimer, RE., 2011. *Modeling Human Behavior to Anticipate InsiderAttacks*. In Journal of Strategic Security, HMU.

Meijer, E. And Kapoor, V, 2014. *The Responsive Enterprise: Embracing the Hacker Way,* Communications of the ACM.

Moore, AP., et. al., 2009. *Insider Theft Of Intellectual Property For Business Advantage: A Preliminary Model*. In *1st International Workshop on Managing Insider Security Threats CERT Program*, Software Engineering Institute and CyLab at Carnegie Mellon University.

Legg, P., et. al, 2013. *Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection*, In *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, ISYOU.

Moore, AP., et. al., 2011. *.A Preliminary Model of Insider Theft of Intellectual Property*. In *Technical note Carnegie Mellon University*, CERT.

Nurse, J., et. al, 2014.*Understanding Insider Threat: A Framework For Characterising Attacks*, In *Security and Privacy Workshops,* IEEE.

Pwc., 2013..*Key findings from the 2013 US State of Cybercrime Survey*.

Shahbaz, M., Groz, R., 2009. *Inferring Mealy Machines*. In *2nd World Congress on Formal Methods*, SPRINGER.