A Structured Methodology for Mitigating Enterprise Insider Threats

Puloma Roy, Anirban Sengupta, Chandan Mazumdar
Centre for Distributed Computing, Dept. of Comp. Sc. and Engg., Jadavpur University, Kolkata-700032
E-mail: {puloma.roy, anirban.sg, chandan.mazumdar}@gmail.com

Abstract— An insider is a person or software that has authorization to access the asset(s) of an enterprise. In recent years, security incidents perpetrated by enterprise insiders have increased manifold. Enterprises attempt to mitigate such threats by implementing controls intuitively, on an ad-hoc basis. However, such intuitive control implementation is both time-consuming, as wells as prone to errors, leading to insecure enterprise systems. The paper attempts to address this issue by proposing a structured methodology for the selection of relevant security controls. The technique is to first model insider threats and security controls, and then match their constituent components against each other. The proposed methodology has been illustrated with a few case studies.

Keywords— *asset; insider threat; security control; threat-control mapping; threat model*

I. INTRODUCTION

An *insider* is a person or software that has authorization to access the asset(s) of an enterprise. In recent years, the number of security incidents perpetrated by enterprise insiders, either deliberately or accidentally, have increased manifold. The US State Cyber Crime Report 2017 [1] shows that 30% of the insider attacks are more costly or damaging than the attacks perpetrated by external entities. Moreover, more than one-in-four of the attacks are committed by insiders. According to the Insider Threat Report 2018 presented by CA Technologies [2], 90% of enterprises feel that they are vulnerable to insider attacks; besides, 53% of the enterprises (that were surveyed) witnessed attacks by insiders during 2017-18.

Mitigation of insider threats poses serious challenges as the threat agents possess authorization to access the attack targets. Specific security controls are required to counter the threats owing to insiders. Enterprises usually select such controls from popular standards like ISO/IEC 27002:2013 [3], NIST SP 800-53 rev. 4 [4] etc. It is important for an enterprise to identify and assess the relevant insider threats, and select security controls accordingly. Owing to the lack of structured control selection mechanisms, enterprises usually implement controls by selecting them intuitively, on an ad-hoc basis. On one hand, such intuitive procedures are time-consuming and costly; on the other, they may lead to incorrect control selection that may render the entire exercise ineffective.

In this paper, we attempt to address the above issue by presenting a structured methodology for the selection of security controls that can mitigate insider threats. The proposed methodology models insider threats and security controls in a manner that enables such selection. For the purpose of this research, the controls listed in ISO/IEC 27002:2013 [3] have been referred. However, the methodology is generic enough to support the controls and best practices of other standards as well; this has been illustrated with the help of some controls derived from NIST SP 800-53 rev. 4 [4].

The rest of this paper is organized as follows: Section II presents some related work. Section III defines a model of insider threats, while Section IV contains a model of security controls. Section V describes an insider threat mitigation methodology. Section VI illustrates the proposed methodology with the help of two case studies. Finally, Section VII concludes the paper.

II. RELATED WORK

In this section, we analyze some of the insider threat mitigation techniques that have been published over the years. A recent report prepared by Carnegie Mellon University describes twenty-one best practices for detecting as well as preventing insider threats [5]. The report also includes a mapping of the best practices to relevant controls of widely accepted security standards and regulations like ISO/IEC 27002:2013 [3], NIST SP 800-53 rev. 4 [4], European Union's General Data Protection Regulation [6] etc. Successful analysis of insider threats hinges on the availability of appropriate data sources. Several enterprises utilize log data for insider threat analytics. The report also provides a comprehensive list of logs which can serve as essential data sources for insider threat detection processes.

According to SANS "Insider Threat Mitigation Guidance" [7], an enterprise can develop an insider threat mitigation program by mapping the enterprise-specific requirements to the INSA Insider Threat Mitigation Program Roadmap [8], CERT Insider Threat Program Best Practices and Components [5], and the NIST Cyber Security Framework [4].

Trzeciak and Costa [9] presented a process model for insider threat control, implementation and operation. They

provided a list of technical, physical and administrative controls for different stakeholders. They also discussed different control functions, namely "Prevent", "Detect", "Correct", "Recover", "Deter" and "Compensate".

Michael R. Grimaila [10] introduced three types of insider threat detection approaches: "Staged", "Multi-perspective" and "Multi–disciplinary". Staged approach detects anomalies in user behavior to assess the risks from malicious insiders. Detection of anomalies in user behavior with respect to user-to-user, user-to-content, and user-to-resource relationships is referred to as Multi-perspective approach. The Multi–disciplinary approach performs the following types of activities for detecting insider threats: (i) Social Network Analysis – detection of anomalies in social behavior of users; (ii) Semantic Analysis – using natural language processing and machine learning to analyze textual data at semantic level; and (iii) Composite Role-based Analysis – analyzing application and operating system roles to detect anomalous behavior.

Bunn and Sagan [11] described the "worst practices" with respect to insider threats, drawing upon an analysis of serious mistakes committed earlier. Each of them is relatively rare and unique. The incidents focus on issues that exist in several contexts and that every security manager should consider.

In October 2011, the U.S. president issued the National Insider Threat Policy and established the National Insider Threat Task Force (NITTF) under the joint leadership of the Attorney General and the Director of National Intelligence. These policies strengthen the protection and safeguard of classified information [12].

Spooner et al [13] explored low-cost technical solutions that can help enterprises prevent, detect and respond to insider incidents. They discussed five types of insider threat detection tools and their implementations, as follows: (i) User Activity Monitoring tools; (ii) Data Loss Prevention tools; (iii) Security Information and Event Management tools; (iv) Analytics; and (v) Digital Forensic tools. They also considered selection, implementation and operating procedures of insider threat related controls.

Most of the papers and reports mentioned above define specific control functions for *all* types of insider threats. They also specify different security control frameworks for insider threat mitigation. There is lack of a methodology that can model insider threats and select the most appropriate controls from a knowledgebase. We attempt to fill this research gap by proposing such a comprehensive methodology in this paper.

III. INSIDER THREATS

The insiders (human or non-human agents) of an enterprise have authorized access to enterprise assets. The actions of insiders may be categorized as: normal, abnormal and malicious. Normal insider activities are those that do not pose any threat to the enterprise. Abnormal insider activities refer to routine errors that could cause minor problems or unintentional exposure of critical information. Malicious insiders attempt to cause harm to the enterprise by exploiting vulnerabilities within assets. Such insiders may not necessarily be employees (current or former) of the enterprise. They may actually be outsiders who are disguised as authorized and trusted users (e.g. "trusted" business partners and contractors) [14]. Insiders may also comprise of hardware, software or network services that are being controlled by someone from outside the enterprise security perimeter [15]. It is important to note that hardware or software assets, installed within an enterprise, may become corrupt (either due to technical reasons, or malicious activities) and begin to malfunction, thus causing harm to enterprise assets.

TABLE 1. AN INSIDER THREAT TAXONOMY

Affected Enterprise Asset	Insider Threat
Process	Attempt of log deletion
	Attempt to create unknown access paths (backdoor accounts)
	Attempt of improper process execution using legitimate access
	Attempt of unauthorized Changes in Access Patterns
	Authentication and Authorization Failure
Information Asset	Attempt of Data Ex-filtration (Print / Scan / Copy / Fax)
	Attempt of man in the middle attacks / session hijacking
	Illegal processing of data
	Attempt to Espionage for confidential information
	Attempt of information leakage
	Attempt of deletion or modification of data
	Illegal processing of data
Hardware Asset	Attempt to dislocate/steal the hardware equipment
	Attempt of hardware failure
	Attempt to tamper the hardware equipments for malfunctioning
Software Asset	Malicious debug attempt
	Attempt of Buffer Overflow
	Attempt to install malwares (Bots/worms/ Rootkits /Logic Bombs/spyware)
	Attempt to introduce unauthorized code within software
	Attempt of software (code or data) alteration
	Unauthorized attempt to access device software
Network	Attempt of network or host data ex-filtration
	Attempt of unauthorized port scan
	Attempt to access spam email (URL or attachment)
	Attempt to access malicious or phishing websites or web applications
	Attempt of distributed denial of network service (DDoS)
	Attempt to generate anonymous proxy
	Attempt of routing table manipulation
	Attempt of DNS spoofing
Personnel / User	Attempt to provoke co workers for doing malicious activity
	Attempt to misguide third party contractors and vendors

Insider threats may be categorized based on the type of enterprise asset(s) which they can affect; one such

categorization is shown in "*Table 1*". Some of the threats listed in Table 1 have been derived from [16]. Let us analyze some of these threats:

Example 1

Attempt of information leakage via web applications – This threat may be carried out by an employee to reveal confidential information to unauthorized entities, using web applications. The enterprise may have a documented policy to prevent usage of such web applications. However, lack of proper implementation of policies and procedures may allow the employee to carry out the threat, thus causing serious breach of data confidentiality.

Example 2

Unintentional attempt to open malicious email attachments – An employee may attempt to open malicious email attachments, thus causing her computer system, as well as the entire enterprise network, to be compromised. This may lead to serious breaches of confidentiality, integrity, availability and authenticity of enterprise data. Such actions may be due to lack of appropriate awareness, education and training on relevant organizational policies and procedures.

Example 3

Attempt to create unknown access paths (backdoors) to admin account – A malicious or adventurous insider may attempt such activities owing to improper role definition, lack of segregation of duties and / or lack of awareness and training on organizational policies and procedures. Such actions can lead to serious security breaches, including loss of confidentiality, integrity, availability and / or authenticity of sensitive data, as well as repudiation of user actions.

Example 4

Attempt to delete system logs using a malicious script – It may be possible for a malicious user to execute scripts to delete system logs. This would lead to loss of integrity and availability of log files, possibly leading to repudiation of user actions. Lack of proper control of operational software creates opportunities for the perpetration of such threats.

Example 5

Attempt of man in the middle attack – Malicious software may be used to carry out such attacks, causing breaches of confidentiality, integrity, availability and authenticity of sensitive data. Lack of proper network security controls may allow such attacks to the enterprise network.

The above analyses show that insider threats can be modeled with the help of the following constituent entities:

Affected Component(s) – This denotes the asset, system, process, information processing facility etc. that is impacted by the threat.

Threat Agent – This refers to the entity that is responsible for executing the threat. Since we are considering only insider threats, the *actor* is always an insider (employee or third party with authorized access to enterprise assets); hence we ignore explicit reference to the actor for the purpose of this model. The threat agent can be the actor herself, other personnel, or some software.

Threat Cause – This element describes the reason behind the successful execution of the threat. It can be the lack of appropriate policies, lack of, or improper implementation of, controls, lack of training etc.

Affected Security Properties – This identifies the specific security properties of data or business processes that may be breached by the threat. The properties can be confidentiality (C), integrity (I), availability (A), authenticity (Au) and / or non-repudiation (NR).

Impact – This indicates the harm that is caused by the threat.

Hence, insider threat (t) can be modeled as follows:

$$t \equiv \{ac, ta, tc, sp, imp\} \quad (1)$$

where, 'ac' denotes affected components; 'ta' denotes threat agent; 'tc' denotes threat cause; 'sp' denotes affected security properties; and 'imp' denotes threat impact.

It may be noted that a threat can be perpetrated by multiple threat agents, can occur owing to multiple causes, can breach multiple security properties and can have multiple impacts.

Let us now re-visit the above examples of threats and model them as per "(1)," the outcome is shown using JSON syntax in "*Table 2*".

It may be noted that though multiple values of a threat component have been shown within the same tuple, they should be considered as separate tuples in implementations. This means a single tuple will consist of only atomic values for each of the components. For example, the threat in Example 1 may be considered as a union of two sets of components as follows:

Attempt of information leakage via web applications ≡ { ac_1:"data", ta_1:"employee", tc_1:"lack of implementation of policies pertaining to usage of web applications", sp_1:"C", imp_1: "breach of organizational policies and procedures leading to information leakage"} ∪ { ac_2:"organizational policies and procedures", ta_2:"employee", tc_2:"lack of implementation of policies pertaining to usage of web applications", sp_2:"C", imp_2:"breach of organizational policies and procedures leading to information leakage"}.

Such representation would help during the mapping of insider threats with relevant security controls.

In the following section, we study the controls that may be implemented to mitigate such threats and describe a technique to model them.

TABLE 2. INSIDER THREAT MODEL (EXAMPLE)

Example No	Insider Threat (t)	Insider Threat Model t ≡ {ac, ta, tc, sp, imp}
1	Attempt of information leakage via web applications	{ac_1:"data", ac_2:"organizational policies and procedures"}, ta:"employee", tc: "lack of implementation of policies pertaining to usage of web

Example No	Insider Threat (t)	Insider Threat Model t ≡ {ac, ta, tc, sp, imp}
		applications", sp: "C", imp: "breach of organizational policies and procedures leading to information leakage"}
2	Unintentional attempt to open malicious email attachments	{{ac_1:"systems", ac_2:"network"}, ta:"employee", {tc_1:"lack of awareness, education and training on enterprise", tc_2:"email policy"}, {sp_1:"C", sp_2:"I", sp_3:"A", sp_3:"Au"}, imp: "compromise of enterprise systems and network"}
3	Attempt to create unknown access paths (backdoors) to admin account	{ac:"admin account", {ta_1:"organizational policies and procedures", ta_2: "employee",} {tc_1: "lack of proper role definition", tc_2: "segregation of duties", tc_3:" awareness, education and training on organizational policies and procedures"}, {sp_1:"C", sp_2:"I", sp_3:"A", sp_4:"Au", sp_5:"NR"}, imp: "misuse of admin access rights and modification of admin account"}
4	Attempt to delete system logs using a malicious script	{ ac: "system logs", ta: "malicious script", tc: "lack of control of operational software", {sp_1:"I", sp_2:"A, sp_3:"NR"}, imp: "deletion of system logs"}
5	Attempt of man in the middle attack	{ ac: "data", ta: "malicious software", tc: "lack of network security controls", {sp_1:"C", sp_2:"I", sp_1:"A", sp_1:"Au"}, imp: "breach of sensitive information"}

IV. SECURITY CONTROLS

Insider threats can be mitigated by implementing appropriate security controls. There are several standards that contain implementation details of security controls. Some of the widely accepted ones are ISO/IEC 27002:2013 [3], NIST SP 800-53 rev. 4 [4], European Union's General Data Protection Regulation [6] and COBIT 5 [17]. These standards have collected the best practices followed by different enterprises and formalized them as sets of well-defined controls. An enterprise can select controls from the available standards, or it may choose to design a customized control framework that meets its requirements.

Security controls can be grouped into four categories depending on the stakeholders who can be assigned the control implementation tasks [18]. The control categories are as follows:

Governance Controls – These are the controls that are either supervisory in nature or deal with critical business or policy decisions. These controls need to be initiated and controlled by the senior management of an enterprise. Governance controls drive the implementation of all other types of security controls.

Managerial Controls – They comprise of operational tasks that are non-technical in nature.

Technical Controls – These controls consist of operational tasks that are technical in nature. They usually require specific tools and techniques for implementation.

Legal Controls – Such controls are mandated by relevant laws, statutes and regulations.

TABLE 3. EXAMPLES OF SECURITY CONTROLS

Sl No	Control Category	Control Id and Name (derived from ISO/IEC 27002:2013)	Control Statement
1	Governance Control	7.2.3 Disciplinary process	There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
2	Managerial Control	8.1.1 Inventory of assets	Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.
3	Technical Control	9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.
4	Legal Control	18.1.2 Intellectual property rights	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

"*Table 3*" lists some examples of each category of security controls. It may be noted that some controls can belong to multiple categories as they contain tasks pertaining to different classes of stakeholders. For example, "18.1.2: Intellectual property rights" in "*Table 3*" (derived from ISO/IEC 27002:2013) comprises of tasks pertaining to the definition of an IPR (Intellectual Property Rights) policy (governance), implementing the policy (managerial) and ensuring compliance with legislative, regulatory and contractual requirements (legal). Such controls are categorized based on the category of stakeholders that are the primary drivers of those controls. In this example, laws and regulations primarily drive the implementation of IPR policy to ensure protection of intellectual properties and proprietary software products. Hence, the control has been categorized as a legal control.

Let us now analyze the controls stated in "*Table* 3".

7.2.3 Disciplinary process

As is obvious from the control statement, it aims to take action against employees found guilty of breaching information security (by not adhering to organizational policies and procedures). Such breaches may lead to loss of confidentiality, integrity, availability and / or authenticity of data, or repudiation of user actions.

8.1.1 Inventory of assets

This control attempts to prepare and maintain an asset inventory. This is necessary for the identification of assets and

definition of appropriate protection responsibilities so as to ensure their availability.

9.4.3 Password management system

This control would help protect systems and applications by implementing an interactive password management system. This would prevent unauthorized access to systems and applications and help protect the confidentiality, integrity, availability and authenticity of information and other assets.

18.1.2 Intellectual property rights

This control helps protect intellectual property and proprietary software by ensuring compliance with appropriate legislative, regulatory and contractual requirements. This would address the confidentiality, integrity, availability and authenticity requirements of information and software assets.

The above analyses show that security controls can be modeled with the help of the following entities:

Target – This denotes the asset, system, process, information processing facility etc. that is protected or addressed by the control.

Host – This refers to the entity on which the control is applied. The host can be an employee, contractor, software, information processing facility etc.

Protection Mechanism – This element describes the mechanism by which the control attempts to mitigate corresponding threat(s). The mechanism can be establishment of appropriate policies, implementation of security infrastructure, conduct of training etc.

Addressed Security Properties – This identifies the security properties of data or business processes that are addressed by the control. The properties can be confidentiality (C), integrity (I), availability (A), authenticity (Au) and / or non-repudiation (NR).

Outcome – This indicates the effect of implementing the control.

Hence, security control (sc) can be modeled as follows:

$$sc \equiv \{tg, ht, pm, as, out\} \quad (2)$$

where, 'tg' denotes target; 'ht' denotes host; 'pm' denotes protection mechanism; 'as' denotes addressed security properties; and 'out' denotes outcome.

It may be noted that a security control can help mitigate multiple threats, while an insider threat can be mitigated by multiple controls. This aspect will be discussed further in the next section.

Let us now re-visit the security controls described above and model them as per "(2)"; the outcome is shown using JSON syntax in "*Table 4*". During implementations, a single tuple for a control should contain only atomic values for each of the components (as stated for insider threats).

TABLE 4. SECURITY CONTROL MODEL (EXAMPLE)

Control Id and Name (derived from ISO/IEC 27002:2013)	**Security Control Model sc ≡ {tg, ht, pm, as, out}**
7.2.3 Disciplinary process	{tg:"organizational policies and procedures", ht: "employees", pm: "disciplinary process against employees who commit information security breach", {as_1:"C", as_2:"I", as_1:"A", as_1:"Au", as_1:"NR"}, out: "ensuring that employees fulfill their information security responsibilities"}
8.1.1 Inventory of assets	{tg: "assets", ht: "assets", pm: "compilation and maintenance of asset inventory", as: "A", out:"identification of assets and definition of appropriate protection responsibilities"}
9.4.3 Password management system	{tg: "assets", ht: "operating systems and other software", pm: "implementation of interactive password management systems that ensure quality passwords", {as_1:"C", as_2:"I", as_3:"A", as_4:"Au"}, out: "prevention of unauthorized access to systems and applications"}
18.1.2 Intellectual property rights	{{tg_1: "intellectual property", tg_2: "employees"},{ ht_1:"contractors", ht_1:"software",{ pm_1: "implementation of procedures to ensure compliance with legislative, pm_2:regulatory and contractual requirements"}, {as_1:"C", as_2:"I", as_3:"A", as_4:"Au",{ out_1: "avoiding breaches of legal, statutory", out_2:"regulatory or contractual obligations pertaining to intellectual property and proprietary software"}}

Hence, it is possible to model security controls as per the elements stated in "(2)". It may be noted that though we have referred to the controls of ISO/IEC 27002:2013 for the purpose of this model, the same methodology may be applied to model the controls listed in other standards, as well. This is owing to the fact that almost all accepted standards [4, 17] follow a similar control structure; this is obvious from the mappings that exist between the controls of different security standards [4, 17].

In the next section, we propose a methodology for mapping insider threats with relevant security controls. This will help in selecting controls for mitigating insider threats in an enterprise.

V. MITIGATING INSIDER THREATS

In the previous sections, we have shown how insider threats and security controls can be decomposed into a set of specific elements. We now use those elements to propose a structured methodology that can select appropriate controls for mitigating insider threats. It is important to note that insider threats and security controls share a many-to-many relation between them. This implies that alternative controls may exist that can mitigate the same insider threat. Also, an enterprise may choose to implement multiple controls to deal with a critical threat. On the other hand, a control can be such that it is able to mitigate multiple insider threats. The following examples illustrate the relation between threats and controls.

Example 6

The threat stated in Example 2, namely "Unintentional attempt to open malicious email attachments", can be mitigated by implementing control "7.2.2: Information security awareness, education and training" of ISO/IEC 27002:2013.

Example 7

The threat stated in Example 3, namely "Attempt to create unknown access paths (backdoors) to admin account", can be mitigated by implementing the following controls of ISO/IEC 27002:2013: "6.1.2: Segregation of duties", "7.2.2: Information security awareness, education and training" and "9.2.3: Management of privileged access rights".

Example 6 shows that it may be possible to mitigate an insider threat by implementing a single security control. On the other hand, Example 7 presents a case where multiple controls may be needed to handle a threat. Moreover, the same control may be used to address multiple threats as illustrated by "7.2.2: Information security awareness, education and training". Thus, these examples corroborate the earlier statement that a many-to-many relation exists between the set of insider threats and set of security controls.

The models of insider threats and security controls, as represented by Equations "(1)" and "(2)", respectively, have led us to propose the following methodology for control selection.

Step 1: Firstly, the enterprise should perform a threat analysis to identify the insider threats that are significant for its assets and information processing facilities.

Step 2: The threats should be decomposed into their individual elements as per "(1)".

Step 3: The enterprise should prepare a knowledgebase of security controls (either from accepted standards, or indigenously developed) and decompose them into their constituent elements as per "(2)".

Step 4: The elements of insider threats should be matched against those of security controls as follows:

a) Since, the control aims to protect the entity that is targeted by a threat, the *affected component* of insider threat should be matched against the *target* element of security control: t[ac] ↔ sc[tg];

b) Since, a control is applied on the entity that perpetrates a threat, the *threat agent* of insider threat should be matched against the *host* element of security control: t[ta] ↔ sc[ht];

c) A control tries to mitigate a threat by eliminating the cause that triggers it. Hence, the *threat cause* of insider threat should be matched against the *protection mechanism* of security control: t[tc] ↔ sc[pm];

d) The *affected security property* of insider threat should be matched against the *addressed security property* of security control: t[sp] ↔ sc[as]; and

e) The outcome of implementing a control is the reduction of negative impacts of the corresponding threats. Hence, the *impact* of insider threat should be matched against the *outcome* element of security control: t[imp] ↔ sc[out]

Step 5: For a particular insider threat, those security controls should be selected whose elements match exactly with those of the threat. In other words, if security control sc_j is selected for mitigating insider threat t_i, it implies that:

a) $t_i[ac] \leftrightarrow sc_j[tg]$

b) $t_i[ta] \leftrightarrow sc_j[ht]$

c) $t_i[tc] \leftrightarrow sc_j[pm]$

d) $t_i[sp] \leftrightarrow sc_j[as]$

e) $t_i[imp] \leftrightarrow sc_j[out]$

Step 6: If multiple controls exist for mitigating a single threat, the enterprise may either choose to implement *all* of them, or perform a cost-benefit analysis to select the best option(s).

The above steps should be performed by an enterprise at regular intervals to mitigate insider threats. It is important to measure the effectiveness of implemented controls and monitor and review them periodically. The enterprise should also maintain an updated knowledgebase of security controls so as to be able to address new threats that appear over time.

The following section describes two cases that illustrate our proposed control selection methodology.

VI. CASE STUDY

In this section, we consider two insider threats and apply the proposed methodology to derive appropriate security controls for mitigating them.

Case 1

An enterprise detects the following threat (t_1): "Attempt of information leakage via web applications". Using "(1)" and "*Table 2*", t_1 can be m2 odeled as:

$t_1 \equiv$ {{$t_1[ac]_1$:"data", $t_1[ac]_2$:"organizational policies and procedures"}, t_1[ta]: "employee", t_1[tc] : "lack of implementation of policies pertaining to usage of web applications", t_1[sp]: "C", t_1[imp]: "breach of organizational policies and procedures leading to information leakage"} (3)

On scanning the security controls of ISO/IEC 27002:2013, it is found that the components of Control "7.2.1: Management responsibilities" (sc_1) match with the components of t_1.

sc1 ≡ {sc1[tg]: "assets", {$sc1[ht]_1$:"employees", $sc1[ht]_2$: "contractors"}, sc1[pm]: "application of information security in accordance with organizational policies and procedures", {$sc1[as]_1$:"C, $sc1[as]_2$:"I", $sc1[as]_3$:"A", $sc1[as]_4$:"Au",

$sc1[as]_5$:"NR"}, sc1[out]: "adherence to organizational policies and procedures"} (4)

Since, "data" and "organizational policies and procedures" are types of "assets", it can be easily seen that each component of t_1 matches exactly with the corresponding components of sc_1. Thus, the Control "7.2.1: Management responsibilities" can be selected to mitigate the threat "Attempt of information leakage via web applications". Intuitively, it is the responsibility of the management of an enterprise to ensure that information security is applied in accordance with organizational policies and procedures. This would ensure the maintenance of data security and prevent any unauthorized leakages. Thus, the control selected intuitively matches with the one selected by the proposed methodology, hence proving its correctness.

Case 2

An enterprise detects the following threat (t_2): "Attempt to create unknown access paths (backdoors) to admin account". Using "(1)" and Table 2, t_2 can be modeled as:

$t_2 \equiv$ { t_2[ac]: "admin account, organizational policies and procedures", t_2[ta]:"employee", {$t_2[tc]_1$: "lack of proper role definition", $t_2[tc]_2$:"segregation of duties and awareness", $t_2[tc]_3$:"education and training on organizational policies and procedures" }, {$t_2[sp]_1$:"C", $t_2[sp]_2$:I, $t_2[sp]_3$:A, $t_2[sp]_4$:Au, $t_2[sp]_5$:"NR"}, t_2[imp]: "misuse of admin access rights and modification of admin account"} (5)

On scanning the security controls of ISO/IEC 27002:2013, it is found that the components of Controls "6.1.2: Segregation of duties" (sc_2), "7.2.2: Information security awareness, education and training (sc_3)" and "9.2.3: Management of privileged access rights" (sc_4).

$sc_2 \equiv$ {sc_2[tg]: "assets", sc_2[ht]: "employees", sc_2[pm]: "segregation of duties", {$sc_2[as]_1$:"C", $sc_2[as]_2$:"I", $sc_2[as]_3$: "Au"}, sc_2[out]: "protection against modification or misuse of assets"} (6)

$sc_3 \equiv$ {sc_3[tg]: "organizational policies and procedures", sc_3[ht]: "employees and contractors", sc_3[pm]: "imparting regular awareness, education and training on relevant organizational policies and procedures",{ $sc_3[as]_1$: "C", $sc_3[as]_2$:"I", $sc_3[as]_3$:"A", $sc_3[as]_4$:"Au", $sc_3[as]_5$: 'NR"}, sc_3[out]: "awareness and knowledge of relevant organizational policies and procedures"} (7)

$sc_4 \equiv$ {sc_4[tg]: "assets", {$sc_4[ht]_1$: "employees, $sc_4[ht]_2$: external parties"}, sc_4[pm]: "control of allocation and use of privileged access rights", {$sc_4[as]_1$:"C", $sc_4[as]_2$:"I", $sc_4[as]_3$:"A", $sc_4[as]_4$:"Au", $sc_4[as]_1$:"NR"}, {$sc_4[out]_1$: "ensuring authorized privileged user access", $sc_4[out]_2$: "prevention of unauthorized privileged access to systems and services"} (8)

It can be seen that the components of t_2 match with the corresponding components of sc_2, sc_3 and sc_4. Thus, these controls can be selected to mitigate the threat "Attempt to create unknown access paths (backdoors) to admin account". As in Case 1, it can be proved that this selection matches exactly with manual (intuitive) control selection.

VII. Conclusion and Future Work

The paper began by defining and modeling insider threats to enterprise assets. It showed how each threat comprises of specific entities that can be identified by analyzing the same. The security controls, which can help mitigate insider threats, were then described and modeled. Like threats, each control can also be decomposed into specific components. Though the paper has referred the controls of ISO/IEC 27002:2013, security controls of other accepted standards can be modeled in the same manner as their structures are similar. Finally, a methodology for the selection of security controls, corresponding to insider threats, has been proposed. The paper also includes case studies to illustrate the proposed methodology.

The novelty of this research lies in the fact that it would be possible to select relevant security controls for mitigating insider threats based on a structured mapping of individual entities. This would eliminate the need for intuitive control selection and result in the implementation of a cost-effective methodology that produces consistent and accurate results.

Future work is geared towards the development of an exhaustive knowledgebase for the possible values of threat and control components. Besides, we also intend to develop a knowledgebase that would contain the components of security controls that are listed in all widely accepted standards. This would help in the development of an automated tool that would accept insider threats and enterprise description as input and generate a list of possible security controls to mitigate them.

References

[1] "US State Cyber Crime Executive Summary", CSO, 2017.
[2] "Insider Threat Report 2018, Cyber Security Insiders", CA Technologies, 2018.
[3] "ISO/IEC International Standard 27002-2013, Information technology - Security techniques - Code of practice for information security controls", 2016.
[4] NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations,2013
[5] "Common Sense Guide to Mitigating Insider Threats, Sixth Edition" The CERT Insider Threat Center, Technical Report, December 2018.
[6] "General Data Protection Regulation (GDPR)", 2018.
[7] B. Balakrishnan, "Insider Threat Mitigation Guidance" SANS Institute Information Security Reading Room, 2019.
[8] https://www.insaonline.org/insider-threat-roadmap
[9] R. Trzeciak and D. Costa "A Framework to Effectively Develop Insider Threat Control", RSA Conference 2018.
[10] M. Grimaila, "Log Analysis for Insider Threat Detection" Cyber Security Expo University of Memphis, 2010
[11] M. Bunn and S. D. Sagan "A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes"
[12] https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf

[13] D. Spooner, G. Silowash, D. Costa, M Albrethsen, "Navigating The Insider Threat Tool Landscape: Low Cost Technical Solutions To Jump-Start An Insider Threat Program" Carnegie Mellon University, Software Engineering Institute, 2018.
[14] P. Roy and C. Mazumdar, "Modelling of enterprise insider threat," 1st International Conference on Information Systems Security and Privacy, Sitepress, 2015.
[15] P. Roy and C. Mazumdar, "Modelling insider threat using Enterprise Autometon," Fifth International Conference on Emerging Applications of Information Technology (EAIT), 2018.
[16] https://www.enisa.europa.eu/topics/threat-risk_management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view
[17] "A Business Framework for the Governance and Management of Enterprise IT", (COBIT 5). 2012. ISACA.
[18] A. Sengupta, "Modeling Dependencies of ISO/IEC 27002:2013 Security Controls", SSCC, 2015, pp. 354-357.

Puloma Roy is a research scholar at Centre for Distributed Computing, Jadavpur University. Her research interests include Enterprise Insider Threat modelling, risk assement etc.

Dr. Anirban Sengupta is a research associate at Centre for Distributed Computing, Jadavpur University. His research interests include information security, privacy etc.

Proff. Chandan Mazumdar is a senior professor of Computer Science and Engg. Department, Jadavpur University. His research interests include information security modelling, security metrics, threat analysis, privacy etc.