Defense against Insider Threat: a Framework for Gathering Goal-based Requirements

Virginia N. L. Franqueira and Pascal van Eck

University of Twente
Department of Computer Science, Information Systems Group
Enschede, The Netherlands
{franqueirav,p.a.t.vaneck}@ewi.utwente.nl

Abstract. Insider threat is becoming comparable to outsider threat in frequency of security events. This is a very worrying situation, as insider attacks have a high probability of success because insiders have authorized access and legitimate privileges. As a result, organizations can suffer financial losses and damage to assets and to reputation. Despite their importance, insider threats are still not properly addressed by organizations. We contribute to reverse this situation by introducing a framework composed of a method and of supporting awareness deliverables. The method organizes the identification and assessment of insider threat risks from the perspective of the organization goal(s)/business mission. This method is supported by three deliverables. First, by attack strategies structured in four decomposition trees. Second, by a pattern of insider attack which reduces an insider attack step to six possible scenarios. Third, by a list of defense strategies which helps on the elicitation of requirements. The output of the method consists of goal-based requirements for the defense against insiders. Attack and defense strategies are collected from the literature and from organizational control principles.

Keywords: Insider threat, control principles, attack strategies, defense strategies, risk assessment

1 Introduction

According to recent surveys [1,2,3] and reports from studies carried out by the U.S. Secret Services and the CERT[1] (e.g [4,5]), insiders are responsible for major financial losses, damage to organizational reputation and assets and also for disruptions. Worse, insider attacks are tending to rise and to be comparable in frequency to security events originated by outsiders. We consider an insider, as defined by Bishop [6], as "a trusted entity that is given the power to violate one or more rules in a given security policy ... the insider threat occurs when a trusted entity abuses that power". The CERT categorizes insider crime in three

[1] Center of Internet Security from Carnegie Mellon University's Software Engineering Institute - http://www.cert.org/insider_threat/

major groups: fraud, theft of information and IT sabotage. The first one occurs when someone obtains unjustifiable services or property from the organization. The second one occurs when someone steals confidential or proprietary information from the organization. The third, and last, one occurs when someone harms, in any sense, the organization or individual(s) within the organization. Among these groups they found: (i) there is no conclusive evidence that a general profile of insiders exists, and (ii) in more than half of the cases studied, insiders exploited vulnerabilities in applications, processes and procedures/policies. Thus, the insiders problem is particularly different from the outsiders problem because it does not only involve technical aspects but also organizational and even psychological aspects, such as the ones related to unmet expectations and wish for revenge. Additionally, the technical aspect is also very distinct because, for insiders, it involves abuse of access and subtle violations of control principles while for outsiders, it involves forcing access and escalation of privileges. Furthermore, because insiders have authorized access and legitimate permissions to the organization inner network area, their malicious actions have high probability to be successful and to end up undetected.

To solve the insider threat problem, many challenges have yet to be overcome. One challenge is the identification and assessment of risks that insiders represent to an organization. This awareness of risks allows planning of detection and prevention countermeasures. Another challenge is the modeling and analysis of the insider threat in a practical way, as for example step-wise or very detailed approaches like attack trees [7], misuse cases [8] and defense trees [9] may become unusable due to the large number of possibilities to be considered. This large number is caused by, for example, the wide spectrum of insiders' goals. Even another challenge is the lack of tool support for organizations in the process of identification and assessment of insider risks.

The contribution of this paper is a framework that addresses the two first challenges mentioned above. The framework consists of a method for identification and assessment of insider threat risks and elicitation of goal-based requirements for defense against those risks, and of three deliverables. The deliverables are: (i) insider attack strategies structured in four decomposition trees, (ii) a pattern which provides the big picture of insiders attack and which can be instantiated with the attack strategies, and (iii) defense strategies against insiders that are useful for the requirements elicitation step. The purpose of these three deliverables is to increase awareness about the insider problem in general for a more efficient and effective application of the method in an organizational context. The deliverables which support the method take the perspective of control principles, which are exploited by attack strategies and enforced by defense strategies. This perspective enables to look at the insider problem as a whole and gather requirements against all insiders categories, i.e. fraud, theft of information and IT sabotage.

1.1 Organization of the paper

This paper is organized as follows. We first present the framework for the gathering of requirements for defense against insiders in Section 2. Then, in Section 3, we provide a taxonomy of control principles useful for the derivation of attack and defense strategies. Next, we organize insiders attack strategies in four decomposition trees and propose an insider attack pattern, in Section 4. Defense strategies matching the attack strategy trees are listed in Section 5. This section also presents a matrix connecting the three basic ingredients of our framework (i.e. control principles, attack strategies and defense strategies). In Section 6 the actual method, which is the core of the framework, is detailed. Section 7 describes an example application of the framework. In Section 8 the framework is discussed, in Sections 9 related work is reviewed, and in Section 10 we conclude and point to future work.

2 A framework for gathering requirements for defense against insider threat

This section provides a high level overview of the framework we propose in this paper. The goal of the framework is to help organizations to identify requirements for IT infrastructure, organizational structures, and policies, that enable its defense against insiders.

As shown in Figure 1, control principles are our starting point for reasoning about insider threats. The motivation for this choice is twofold. First, insiders exploit vulnerabilities and one alternative they have to achieve that relies on exploiting control principles. The link between vulnerability and control principles is observable in definitions of vulnerability such as the one by Stoneburner [10]: "[vulnerability] is a flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy". Second, control principles provide mechanisms for organizations to prevent and detect insiders activities. Thus, as represented in the figure, control principles are, on the one hand, exploited by attack strategies, due to flaws or weaknesses in processes, applications, infrastructure, etc, and, on the other hand, enforced by defense strategies to assure a certain level of security.

The framework is composed of a method and of supporting deliverables which provide awareness about insider threats in terms of attack and defense strategies. The method guides the organization through the identification and assessment of risks that insiders represent to its most critical assets and processes, defined according to the organization goal(s) and business mission. Attack strategies, as mentioned in the previous paragraph, have been derived from possible exploitations of control principles and from past insider cases documented in the literature [11,4,5,12]. From the latter we acknowledge insights about possible exploitations on applications, infrastructure and organizational structure. Defense strategies have also been derived from control principles and from defenses methods documented in the literature.

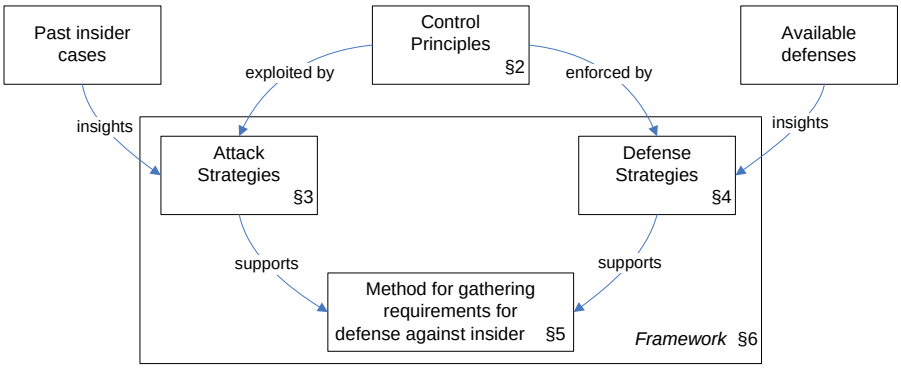

Fig. 1. Framework composed by a method and supporting attack and defense strategies

3 Taxonomy of organizational control principles

Cobit [13] defines *controls* as "the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.". Although each organization implements specific controls according to their goal(s)/business mission and overall security requirements, they are based on common control principles which apply to any organization. A taxonomy of control principles related to IT, composed from the literature [14,15,16,17], is presented next.

1. **Separation of Duty (SoD)**: from [16] "[SoD aims to ensure that] no employee or group should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties". This principle can be enforced in a static way, by not permitting one person to assume incompatible functions/permissions (i.e. exclusive roles), and in a dynamic way, by not permitting the activation of exclusive roles in the same session. Dynamic SoD can come in three flavours: (i) object SoD - same person prohibited to perform critical operations on a same object, (ii) operation SoD - same person prohibited to perform critical functions in a workflow, and (iii) history SoD - same person prohibited to perform all his authorizations on the same object over time. This principle can be difficult to achieve in small organizations. In this case, other principles [18] like reconciliation, review, audit and supervision can be used.
2. **Dual Control** (also called Two-Person Rule or Four-eye Principle): this principle aims to make sure that sensitive tasks require two individuals, usually with identical roles and hierarchical position, to perform.
3. **Delegation** and **Revocation**: delegation refers to a change in the assignment of authorization from one person to another. Revocation cancels delegation.

4. **Supervision**, **Review** and **Audit**: supervision [19] aims to make sure that subordinates execute assigned obligations. Review aims to control the execution of delegated obligations. Audit aims to allow tracing and analysis of events collected in audit logs.
5. **Accountability** and **Specification of Competence**: from [20] "[accountability] enables activities on a system to be traced to an individual who may be held responsible for their actions". Individuals should be accountable for what they are competent to do [14].
6. **Least Privilege** and **Need-to-know**: least privilege aims to ensure that individuals are only assigned to the minimum set of privileges needed to perform their duties. Need-to-know is a special case of least privilege used on military environments. It rely on labels for individuals and objects to restrict access to information.
7. **Non-repudiation**: from [21] "non-repudiation of action ensures that online actions taken by users, including system administrators and privileged users, can be attributed to the person that performed them". This is the meaning of non-repudiation that is more appropriate to the insiders scenario, nevertheless, for the sake of completeness, this principle is usually used in the context of ensuring that a transaction cannot be denied by the parties involved.
8. **Reconciliation**: control based on totals, balancing sheets, i.e. on cross-information checking.
9. **Classification of Assets**: classification of assets ensures CIA[2] via levels of security depending on the protection required. It is prescribed by security standards like ISO 17799 [17] as a means to maintain control over assets. It is important to have in mind that humans are also assets and thus the classification of users in roles, clearance levels or groups is also instrument of control.

In the next two sections, Sections 4 and 5, these control principles are taken into consideration from opposite perspectives. From the insider (i.e. attacker) perspective, the goal is to violate controls and perform malicious actions without being noticed. From the organization perspective, the goal is to employ controls to avoid and uncover malicious actions.

4 Attack strategies

There are many strategies that insiders can use to reach their goals. In this section, first of all, we consider the issue of how to structure these attack strategies. We do so with two goals. First, we want to abstract the big picture of insider attack to have a better understanding of the problem as a whole. Second, we want to acknowledge which attack alternatives can be exploited by insiders to have a better understanding of the problem in details. To meet these goals we review the structures we use in our framework: attack patterns and decomposition trees. Then, we describe how we applied these structures to the insider problem.

[2] Confidentiality, Integrity and Availability

Attack patterns [22] extend the idea of attack trees (introduced by Schneier [7]). Attack trees permit the modeling of security threats represented as the root of the tree. This threat is successively refined to a level of detail chosen by the designer of the tree. Nodes are connected by AND and OR joints, indicating conjunction and disjunction between pairs of nodes for the achievement of their parent node. Attack scenarios, i.e. sub-steps of an attack, are obtained by traversing the attack tree in a depth-first fashion. Attack patterns are generic and abstract from several attack trees. They do not only describe steps to achieve the root goal but also pre- and postconditions.

Decomposition trees permit the breakdown of a tree root and sub-nodes, in terms of AND/OR relations. This kind of tree provides a structured way for the analysis of alternatives and has been used for goal-oriented analysis of requirements [23]. Towards its root, the tree allows for the abstraction of alternatives and, towards its leaves, the tree allows for precision of alternatives.

We structure attack strategies exploited by insiders in four strategy decomposition trees using two sources: literature [11,4,5,12,24] and the taxonomy of control principles presented in the previous section. The trees are "Pre-attack", "Gain access", "Abuse access" and "Abuse permission" and can be found in Appendix A. The main idea of these trees is to provide a wide spectrum of strategies used by insiders to launch attacks instead of providing a step-by-step analysis of a specific attack from an attacker's[3] goal.

An attack is defined as [25] "a series of steps taken by an attacker to achieve an unauthorized result". Thus, each attack step can also be composed of sub-steps. As an example, we consider two insiders: the first insider wants to cause major losses to the organization by deleting files from its servers, the second insider wants to collapse the organization's share prices in the market for personal financial benefit by denying services to its network. Although the insiders have different goals, a common way to accomplish these goals would be via deployment of logic bombs[4]. There are many alternatives for an insider to deploy a logic bomb such as: (ex.1) "use own legitimate account, create backdoor account", and then "use backdoor account, deploy logic bombs", or (ex.2) "use accounts not disabled on job termination, deploy logic bombs". Each of those sub-steps is represented in one of the attack strategy trees. The aim of these trees is to abstract from insiders' goals and concentrate on alternatives they can use, without going into details on how each alternative can be accomplished. In ex.1, the following two steps have been used: (step 1) "Gain access tree - node 1, Abuse access tree - node 2" and (step 2) "Gain access tree - node 15, Abuse access tree - node 21". In ex. 2, the following step has been used: (step 1) "Gain access tree - node 13, Abuse access tree - node 21".

We capture the "insider attack" in an attack pattern shown, in a textual manner, in Figure 2. This pattern models a step toward an insider attack. It means that using the pattern twice, steps 1 and 2 from ex.1 are represented

[3] In our context, the terms *attacker* and *insider* are used interchangeably.

[4] From Wikipedia "A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met"

and using the pattern once, step 1 from ex. 2 is also represented. Our insider attack pattern models the attack scenarios listed next. These scenarios help us to organize our perception of the insider threat as a whole and, at the same time, provide a choice of possible templates for their instantiation using the four attack strategy trees, as we demonstrated in ex.1 and ex.2.

<Pre-attack, Gain access, Abuse access, Abuse permission>
<Pre-attack, Gain access, Abuse access>
<Pre-attack, Gain access, Abuse permission>
<Gain access, Abuse access, Abuse permission>
<Gain access, Abuse access>
<Gain access, Abuse permission>

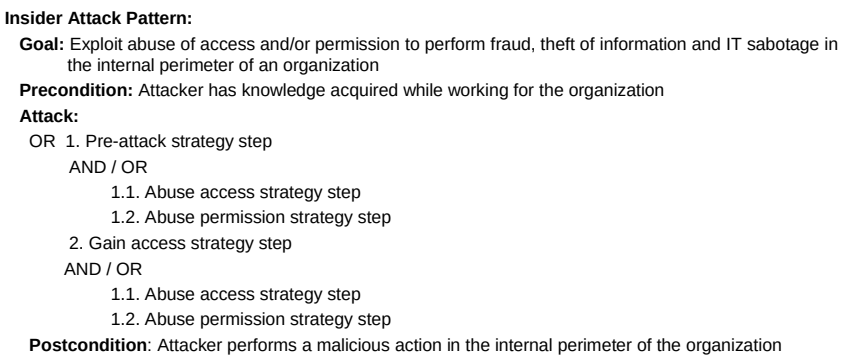

Fig. 2. Insiders attack pattern

In this section, we modeled insider threats and delivered an insider attack pattern and four attack strategy trees. The former provides, for example, awareness that access is the essential component of any insider attack, since all attack scenarios derived from the pattern include "Gain access". The latter provides, for example, awareness that insider access can be acquired for grant, can be created or discovered. In the next section we deal with defense strategies against these attack strategies.

5 Defense strategies

We present, in this section, a list of defense strategies derived from (i) the analysis of attack strategies which can be exploited by insiders, as discussed in Section 4, (ii) the taxonomy of control principles provided in Section 3, and (iii) literature review [11,4,5,12,24]. The defense strategies are organized in three lists, the first

corresponds to the attack strategy trees "Pre-attack" and "Gain access", the second corresponds to the tree "Abuse access" and the third corresponds to the tree "Abuse permission". These defense strategies have been composed with the same objective of broadness instead of deepness as we did for the attack strategies. They will be useful as a reference when eliciting requirements for the defense against insider risks, in step 5 6.5 of the framework method.

Defense strategies against "Pre-attack" and "Gain access" attack strategies:

1. review all access paths to assets periodically to ensure actual paths match expected paths
2. ensure that only access paths needed for an individual's job function are activated
3. ensure the deactivation of all paths available for an individual upon job termination
4. enforce tight password management: (i) adopt strong password, (ii) change passwords periodically, and (iii) check periodically all information systems administration passwords to identify out-of-box unchanged passwords
5. enforce strong authentication
6. ensure security patches are applied in a regular basis on every node of the inner network area
7. support security policies by education, i.e. organization-wide security awareness and training initiatives for potential insiders
8. watch for behavioral precursors like disruption, dissatisfaction, level of expectations

Defense strategies against "Abuse access" attack strategies:

1. adopt inventory and configuration management to audit whether hardware and software installed in desktops and servers comply with what is expected
2. use periodical data integrity checks on critical information
3. enforce physical measures for access to information
4. inspect code (e.g. via peer review) with the specific purpose of identifying trap doors (from CWE[5] "a feature intentionally placed in a program that facilitates remote debugging or system maintenance which can compromise the security of an application"), buffer overflows (from CWE "this condition exists when a program attempts to put more data in a buffer than it can hold"; it permits unauthorized access to memory area adjacent to the allocated buffer), logic/time bombs, validation errors, error handling failure, etc, left by developers intentionally or not
5. ensure audit data cannot be modified by anyone in the organization
6. analyze audit logs to track critical transactions and to track access, modification and deletion of critical information

Defense strategies against "Abuse permission" attack strategies:

[5] Common Weakness Enumeration: www.cwe.mitre.org, sponsored by the U.S. Department of Homeland Security

1. review objects classification periodically
2. check periodically expected users permissions, based on job function, and actual permissions, based on actions performed. However, individuals usually perform several roles within his/her job function. Thus, the set of expected permissions for an individual is the sum of all permissions acquired through (i) direct role assignment, (ii) indirect role assignment, i.e. role hierarchy, (iii) delegation, i.e. temporary permissions, and (iv) role management deficiencies, for example, an employee has been promoted to another function and his/her previous roles have not been disabled. Two controls are important. First, if the set of all actual permissions an individual has exceeds the expected permissions the organization defined for the job function. Second, if the set of permissions violates separation of duties, in this case a detailed analysis of critical assets and processes dealt by this individual is necessary
3. check if delegated permissions conflict with permissions an individual had at the time of delegation; in this case, static separation of duties are violated
4. check delegations followed by revocations; this scenario can be exploited to overcome object separation of duties [19]. A same object can be accessed by two exclusive roles, assuming delegation causes a temporary loss of the delegated permissions, which is then reacquired by revocation. Because this violation is dynamic, it can only be detected by the analysis of audit logs
5. review periodically execution of tasks which require two peers for completion
6. ensure that critical data, such as passwords to critical assets, are not exclusively handled by an uniquely privileged individual
7. review separation of duties at the functional level; a matrix with job functions both on columns and lines and a cross on conflicting intersections can help identifying SoD among job functions
8. review separation of duties at the process level through auditing. However, it is pre-requisite to have strong role management because, otherwise, even if the separation of operations is checked, it can happen that two critical operations are logged as being performed by different roles but, in practice, the same individual executed both. Critical operations can also span several applications and in this case a cross-application audit is necessary, and a manual mapping between roles from these applications is a pre-requisite for detecting violations of SoD
9. ensure non-repudiation of privileged actions: (i) set formal mechanisms for requesting services to administrators and establish a link between requests and actions performed by administrators can be checked via auditing; (ii) a profile of actions expected to be performed to resolve most common types of requests for administrators can be created to allow matching between expected and actual actions

Now, we match control principles, attack strategies, and defense strategies in a matrix, as shown in Table 1. The horizontal axis contains a concise list of defense strategies, derived from the lists described above. They have been composed with the same objective of broadness instead of deepness as we did for the attack strategies. They will be useful as a reference when deriving requirements

Table 1. Attack and defense strategies with control principles at intersections

CONTROL PRINCIPLES AT INTERSECTIONS

SD: Separation of Duties
DC: Dual Control
D/R: Delegation/Revocation
AU: Audit
CC: aCCountability
LP: Least Privilege
NR: Non-Repudiation
RC: ReConciliation
CL: CLassification of Assets
X: other forms of control

DEFENSE STRATEGIES \ ATTACK STRATEGIES	Get and use somebody else's password (PA-1 & GA-6) and use of shared password (AP-2)	Social engineering for pre-attack and to gain access (PA-2 & GA-5)	Use own legitimate access (GA-1)	Take advantage of unlocked machine (GA-2)	Exploit account management deficiencies (GA-3)	Exploit vulnerabilities on applications (GA-4)	Reconnaissance (AA-1)	Create backdoor accounts (AA-2)	Compromise data (AA-3)	Exploit several attempts with wrong password (AA-4)	Install/ insert/ execute malicious code (AA-5)	Disclose confidential information (AA-7)	Exploit least privilege breaches (AP-1)	Exploit two-person rule and separation of duties (AP-3 & AP-4)	Abuse privileged access (AP-5)
Review periodically actual access paths against expected paths	AU RC LP		AU RC LP		AU RC LP		AU LP	AU LP			AU LP	AU LP	AU NR		
Ensure only paths needed for job function are activated for an individual	LP		AU RC LP		AU RC LP		AU LP	AU LP			AU LP	AU LP	AU NR		
Ensure deactivation of paths upon job termination			AU RC NR		AU RC LP			AU			AU	AU	AU NR		AU NR
Enforce tight password management: (i) strong password, (ii) periodic changes, (iii) none out-of-box passwords	AU	AU NR	AU NR							AU		AU LP			AU NR
Enforce strong authentication	AU	AU NR										AU			
Ensure security patches are applied as soon as possible after they are available						AU RC NR					AU				
Support security policies by education, i.e. awareness and training		X		X								X			
Watch for individual behavioral changes like disruption and dissatisfaction		X													
Review periodically hardware inventory and software configuration								X			AU				
Check data integrity on critical information			AU						RC					AU RC	
Enforce physical measures for access to information				X					X		X	X			
Inspect code to identify trap doors, buffer overflow conditions, suspicious calls, validation errors, etc						X		X			X				
Ensure audit data cannot be modified by anyone			AU						X		X				AU
Review assets classification and role structure periodically			AU LP				AU LP					AU LP CL	AU NR	AU LP D/R	AU LP D/R
Review periodically actual users permissions against expected users permissions			AU RC LP, D/R									AU LP D/R, CL	AU RC D/R	AU LP D/R	AU LP D/R
Ensure that critical operations, transactions and data are not handled by an unique individual														AU D/R, LP, SD, DC	AU SD, DC
Enforce management of privileged actions			AU NR			AU NR		AU			AU NR	AU LP		AU D/R NR	AU LP

for the defense against insider risks, in step 5 (Section 6.5) of the framework method. The vertical axis contains the first level of nodes from the attack decomposition trees (where PA refers "Pre-attack", GA to "Gain access", AA to "Abuse access" and AP to "Abuse permission"). The intersections between defense and attack strategies provide insights on which control principles can be used to mitigate the threat of the attack strategy and strength the protection of the defense strategy.

This matrix is an example and needs to be customized by organizations according to the controls they use. Furthermore, it can be refined to a more concrete level by replacing a control by tools, policies and procedures that implement that control. If kept up-to-date, this matrix can provide insights about weaknesses in controls applied to some defenses against attack strategies.

So far, we reviewed control principles (Section 3) which are relevant either from the perspective of attack strategies, discussed in Section 4, and from the perspective of defense strategies, discussed in Section 5. We also explicitely connected these three elements in a matrix and presented deliverables corresponding to attack and defense strategies. The next section describes a method for the assessment of risks represented by insiders against the organization critical assets/processes. This assessment provides means for the organization to gather requirements for defense, in terms of prevention and detection of insiders.

6 Method steps: gathering requirements for defense against insider

The concepts presented in the previous sections are used in our method for requirements gathering that is presented in this section. The method, shown in IDEF0 notation in Figure 3, consists of 5 steps. The boxes represent functions, i.e. steps of the method. Horizontal arrows coming into the boxes are inputs which are transformed by the functions into outputs, which are represented by arrows coming out of the boxes. Vertical arrows represent inputs which are not transformed by the functions into outputs.

The next sub-sections 6.1 to 6.5 provide an overview of each step of the method. The main idea underlying the method is to keep alignment between organizational goal(s)/business mission, the input of the method as a whole, and defense against insider threats as captured by requirements. These requirements are the output of the method as a whole.

6.1 Step 1: Identify critical assets and processes

The main goal of the first step is to narrow the scope of the investigation about insider threat to the core business of the organization by identifying critical assets and processes. Critical assets may include data, information systems and services as well as processes concentrated on one application or spanning several applications.

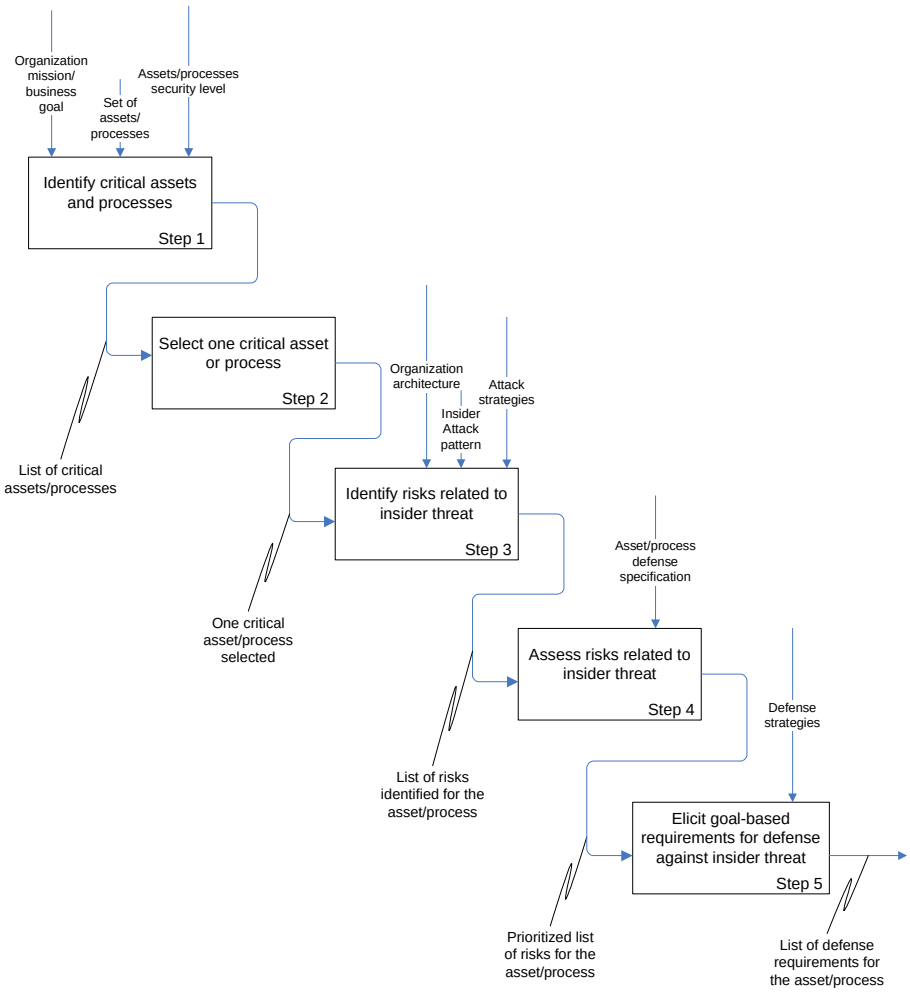

Fig. 3. Method for gathering requirements for defense against insiders

Two elements are input for this step: (i) the organization goal(s)/business mission, and (ii) the set of all assets and processes of the organization. We do not prescribe any method for determining the criticality of assets. Nevertheless, *Critical Impact Factors* , proposed on previous work from one of the authors [26], is a promising way to determine critical assets while keeping a straight alignment with the organization goal(s)/business mission. The list of critical assets and processes should be a consensus among stakeholders.

Output: list of critical assets/processes

6.2 Step 2: Select one critical asset/process

From the previous step we acquire knowledge about the organization main targets of control. The goal of the second step is to narrow the scope of the insider threat investigation even further by prioritizing the critical assets/processes. The advantage of doing this is two-fold. The first advantage follows the known *Divide and Conquer* strategy. It helps providing a short-term estimation for the number of identification/assessment sessions and a longer-term estimation for the number of iterations necessary to cover the whole set of critical assets/processes. The second advantage is the re-use of defense requirements among critical assets/processes.

No specific method for prioritization, allowing selection of one critical asset/process, is prescribed. It remains up to the organization to decide which criteria to use for the selection.

Output: one critical asset/process selected

6.3 Step 3: Identify risks related to insider threat

The previous step provides an unique focus for the remaining three steps. The objective of step 3 is to identify risks which turn the critical asset/process vulnerable to insiders. We divide this step in two stages. In the first stage, a representative of security is nominated the champion. This person will use system architecture diagrams, the Insider Attack Pattern (in Section 4) and the attack strategy trees (in Appendix A) to list risks he believes are relevant for the critical asset/process. In the second stage, stakeholders will get together to discuss risks represented by insiders and it will be more effective if they have spent some time to build a short list of the top risks in their view, using the attack strategy trees as reference. The session(s), conducted by the champion, aims to get agreement about the risks.

It is worth mentioning that the attack strategy trees can be used either to identify one step which represents a risk on its own or to identify an insider scenario according to the Insider Attack Pattern instantiated with the attack strategy trees. As an example of the former case, stakeholders can think about "accumulate privileges" (Abuse permission tree - node 14) as a risk to a loan process. As an example of the latter case, stakeholders can think about the attack steps "use legitimate access (developer), insert trap door in application" (Gain access tree - node 1, Abuse access tree - node 19) and then "exploit vulnerability

on application , modify/delete critical data" (Gain access tree - node 4, Abuse access tree - node 13) as a risk to a human resource database.

Output: list of risks identified for the asset/process

6.4 Step 4: Assess risks related to insider threat

This step aims to prioritize the risks for a particular asset/process that have been identified in the previous step. One input for this assessment phase is the critical asset/process defense specification, i.e. defense mechanisms and methods already implemented. The defense specification allows for the determination of a defense level for the asset/process in respect to the risk under consideration. This defense level may either be considered "high" or "low" and consequently the risk level is derived as the opposite. Determining the defense level can be straightforward. For example, if the human resource database uses strong authentication methods and the risk being analyzed is "get password" then the defense level will probably be considered as "high", and consequently the risk as "low". As another example, for the "accumulate privileges" risk, determining the defense level would involve auditing a structure of role assignments, which might be complicated at this point. In this case, considering the defense level as "low" would be the most appropriate decision because the risk would then be forwarded to the next step as "high" priority. We acknowledge that this defense classification is a weak point of the method because it relies completely on the subjective judgment of the champion, or any security specialist, and agreement among stakeholders. Tool support for the evaluation of defense levels would be an advantage. Nevertheless, we also believe this weakness does not invalidate the method since the determination of the defense level follows a clear rationale.

The process of risk assessment described should be followed for each risk identified for the asset/process. It remains open to organizations to set limits in terms of the number of risks analyzed, carried over or postponed to a new round of the method.

Output: prioritized list of risks for the asset/process

6.5 Step 5: Elicit defense goals against insider threat for the asset/process

From the previous step the organization acquires awareness about which insider risks are top priority for the asset/process. In this step the focus is to look at which defense strategies can be used to bring the asset/process to a level of defense which avoids/uncovers those risks. The defense strategies listed in Section 5 are elaborated in the format of defense goals, which match Anton's [27] definition of goals: "goals are high level objectives of the business, organization, or system. They capture the reasons why a system is needed and guide decisions at various levels within the enterprise". Thus, we aim in this step to identify, for each risk within the asset/process risk list, a list of defense goals, using as reference the defense strategies provided.

After applying the method to all critical assets/processes, overlapping defense goals among several assets/processes should be identified and the priority of defense goals should be determined. Therefore, the complete list of defense goals needs to be analyzed, refined and decomposed into requirements for implementation in the organization. Several researchers have proposed methods and tools for the goal-based requirements (e.g. [27,28,29]) but it is out of the scope of this method.

Output: list of defense requirements for the asset/process

7 The framework applied: an example

Figure 4 shows an example scenario, collected from Chinchani et al. [30], for a fictitious financial institution. We first provide an overview of the example scenario and then apply our framework to the scenario in Section 7.1.

Basically, a teller can complete any personal account transaction involving $5,000 or less, accessing the *personal account database*, but only a manager can complete transactions, initiated by a teller, above this limit. Only managers can perform transactions on business accounts. Communication between computers and databases is encrypted. A manager needs to provide his credentials to a PKI server to be authenticated. Upon successful authentication, he receives a session key to access the *business account database*. Both databases are protected by firewalls to prevent external attacks. We assume the personal account transactions are performed via application A and the business account transactions are performed via application B.

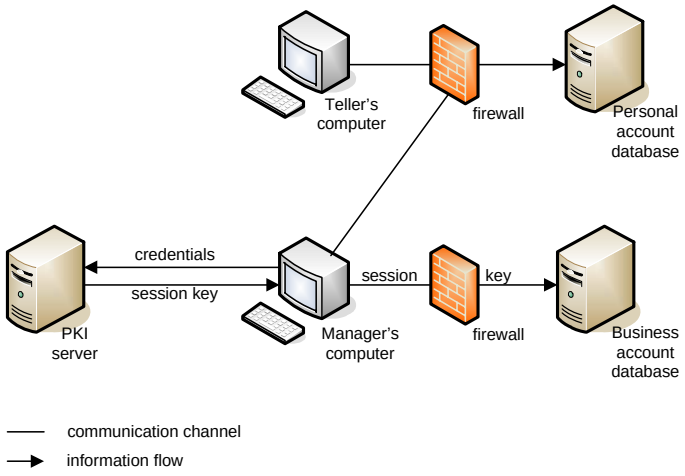

Fig. 4. Example scenario from a fictitious financial institution(adapted from [30])

7.1 Example - step 1

A standard business mission for financial institutions is usually in the line of "provide high quality banking services/financial solutions". Thus, it implies on the high criticality of assets and processes related to monetary transactions for customers. In step 1, management identifies the critical assets/processes. In this very simple example, we assume that this results in the following list:

- asset: personal account database
- process: endorsement of personal account transactions over $5,000
- asset: business account database
- process: business account transactions

7.2 Example - step 2

We select the process "business account transactions" because, although this process seems already well protected, the board of directors want to re-assure whether there is any risk left.

7.3 Example - step 3 and 4

We simulate the role of champion and stakeholders to identify risks using as reference the Insider Attack Pattern and the four attack strategy trees. They look at each branch of the trees and decide if the risk reported is relevant for the process and if it suggests another situation (i.e. sequence of steps) also relevant.

The table 2 shows the risks identified and assessed.

The risks marked in bold are the ones considered high priority to be carried over to step 5.

7.4 Example - step 5

In this step we only identify the defense strategies which seem appropriate as countermeasures for the five risks selected in the previous step. In a real situation, the defense strategies need to be adapted and refined. Table 3 contains the output of the method, i.e. goal-based requirements for defense against the organizations' insiders.

The example demonstrates the potential applicability of the framework for the identification of insider risks and corresponding defenses. We have seen that the process analyzed, which seemed already well protected, is in fact subject to risks which might not be evident.

8 Discussion

In this section, we discuss the proposed framework around three topics which, we believe, turn it interesting: (i) merging of access-oriented and permission-oriented approaches for the insider problem, (ii) abstraction from attacker *goals*

	Risk	Defense level	Risk level
R1	terminated manager uses his account and credentials soon after his termination to perform fraudulent business transactions	high	low
R2	terminated manager uses a backdoor account and his "old" credentials to perform business transactions	low	high
R3	insider gains physical access to a manager's authenticated computer and performs business transactions	high	low
R4	insider (e.g. a teller) *learns* a vulnerability specific to the organization, i.e. that the manager does not apply security patches on a regular basis and exploit a known vulnerability to get the manager's credentials, then obtain a session key from the PKI sever and perform business transactions	low	high
R5	manager deploys a logic/time bomb in the business account database	low	high
R6	manager performs fraudulent business transactions applied to, for example, wife or boyfriend accounts (as beneficiaries)	high	low
R7	insider discloses information about business transactions to competitors or press	low	high
R8	insider, member of application B developers team, insert a trap door in the application (e.g. if sessionKey = 999 then authenticated = true), and perform business transactions	low	high
R9	manager shares his password and credentials with a teller or another manager (e.g. in case of an emergency), and they perform business transaction in the "name" of the original manager	high	low

Table 2. Example: risks for the critical process "business account transactions" identified and assessed

and focus on attacker *means*, organized in four blocks, i.e. "Pre-attack", "Gain access", "Abuse access" and "Abuse permission", and (iii) the shift from risk-based to defense-based assessment of insider threat risks.

The problem of insider threat needs to be analyzed not only from the "abuse access" perspective but also from the "abuse permission" perspective to be able to address the three categories of insiders intention, i.e. IT sabotage, fraud and theft of information. While the first is more related to "abuse access", the other two are more related to "abuse permission". The permission concern has been extensively tackled within the research community related to the formalization and automatic enforcement of policies, surveyed by Damianou et al. [31]. In this line of research, the overall aim is to constraint potential insiders within the boundaries of access control. However, the management of access control

	Defense goal
D1	review all access paths to assets periodically to ensure actual paths match expected paths
D2	ensure security patches are applied in a regular basis on every node of the inner network area
D3	adopt inventory and configuration management to audit if hardware and software installed in desktops and servers comply with expected
D4	analyze audit logs to track critical transactions and to track access, modification and deletion of critical information
D5	inspect code (e.g. via peer review)
D6	support security policies by education, i.e. organization-wide security awareness and training initiatives for potential insiders

Table 3. Example: defense goals for the critical process "business account transactions" elicited

may deteriorate over time, opening security breaches for abuse. So, we aim to gather requirements for defending an organization against insiders by detecting permission abuse as well as access abuse.

Our approach to the modeling of insider threat concentrates on the spectrum of alternatives an insider can exploit to reach individual intentions, secret goals. This approach enables the representation of insiders activities categorized in four blocks, i.e. "Pre-attack", "Gain access", "Abuse access" and "Abuse permission", while still capturing a broad range of abuses, either from the access domain and from the permission domain. Other researchers have split the insider problem into different main blocks. For example, in the Insider Threat 2004 Workshop [12], the Attacker Models group divided the possible actions an insider can take in four categories: obtaining access, reconnaissance, entrenchment and exploitation, and extraction and exfiltration. Butts et al. [32] categorize the type of actions an insider can perform in: alteration, distribution, snooping and elevation. We believe our division is particular in the sense that it derives from control principles and therefore also deals with exploitations related to more sophisticated access control breaches such as the ones related to roles and separation of duties, not present on these other works.

We prioritize risks represented by insiders using the level of defense of the asset/process under analysis for a specific risk. The most used approach to prioritize risks related to attacks rely on measures of attack likelihood or impact (e.g. [33,10]). However, it is difficult to determine probability measures for the likelihood of an insider attack in a meaningful way. Furthermore, it is also difficult to evaluate the impact of an insider attack since it depends on the insider intents/goals. Chinchani et al. [30] quantify attacks by assigning a cost based on the resistance of an asset, provided by access control mechanisms and determined by security experts. This last approach is similar to ours in the sense that it shifts the focus of risk assessment from the attack itself, like it happens when measuring likelihood and impact, to the defense. This shift allows the classifi-

cation of a same risk differently according to the level of defense or degree of resistance of the asset/process under this risk.

In this section, we presented some strong points of the proposed framework. However the framework has still another strong point. It is simple enough to be useful in organizations of any size.

9 Related work

The framework presented in this paper is related to insider threat modeling and risk management, the main ingredients of our approach. With respect to the latter, we review two risk management frameworks, OCTAVE [33] and NIST SP 800-30 [10], considered of relevance for our work. With respect to the former, we already reviewed along the paper relevant related work [7,8,9,12,32].

The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk evaluation methodology also based on a triplex similar to those used in our framework: critical assets, threats to those assets and vulnerabilities that expose the assets to threats. It is composed of three phases, each one composed of several processes. The first phase uses enterprise knowledge from many hierarchical levels to identify assets, threats, risk indicators and security requirements. OCTAVE uses the concept of threat profile for an asset based on five properties: asset, actor, motive/access (optional), and outcome (disclosure, modification, destruction, loss, interruption). The second phase deals with the identification of infrastructure vulnerabilities. Assets are prioritized based on threats identified on previous phase and vulnerabilities are evaluated based standard catalogs such as known intrusion scenarios. The third phase prioritizes risks based on impact and probability derived from risk indicators gathered from staff and develop a plan to manage the risks. Three points from OCTAVE are of interest for our work: (i) threats are gathered from enterprise knowledge. Although it is a powerful approach similar to a broad brainstorm it can also be time consuming and inefficient; (ii) assets are prioritized based on threats. We believe our approach which considers critical assets determined by organization goal(s)/business mission more to be appropriate. For example, an asset can be highly critical business wise and therefore very well protected, thus being subject to low threat; (iii) vulnerabilities are identified based on catalogs of known intrusion scenarios. Vulnerabilities in our framework are implicitly evaluated in terms of the asset/process defense level specific for the threat under analysis. So, when assessing the threat "accumulation of privileges" this is the focus of the evaluation of defense level, and is hardly found on catalogs. So, in this sense we believe our framework allows a broader assessment of risk for the insider problem and consequently a broader view on requirements for defense.

NIST SP 800-30 is a standard which provides guidance for risk management through a system's life cycle. It comprehends three processes, i.e. risk assessment, risk mitigation, and evaluation/assessment. We concentrate on some aspects of the first process, composed of nine steps, which overlaps with our framework. Threat identification is based on threat-source analysis, i.e. natural

threats, human threats (e.g. terminated employees, unauthorized users), and environmental threats. Vulnerability identification is performed independently of threat identification, from the perspective of system flaws or weaknesses which can be exploited by threat-sources. Then, a matching between vulnerability and threat is performed. Control analysis identifies the implemented, or planned to be implemented, controls to minimize the likelihood of a threat. The framework provides a list of preventive controls, which can be technical (e.g. access control enforcement, authentication, encryption) or non-technical, i.e. management and operational controls, and detective controls (e.g. Intrusion Detection Systems, audit trails, checksums). Likelihood is determined in terms of high/medium/low, based on threat-source, vulnerability and existence/effectiveness of controls. Impact is also determined in terms of high/medium/low, based on system mission, system/data criticality and system/data sensitivity. Two points from this NIST standard are worth emphasizing in respect to our work: (i) threats are derived from threat-sources. Thus, in terms of insiders, the focus would be on human threats. We believe our approach of attack strategies induces a broader vision of the insider problem, since it provides insights not commonly explored, as for example, separation of duty scenarios, which are unlikely to be considered in threat-source reasoning; (ii) vulnerabilities and controls have to be analyzed. We have a more focused approach when we evaluate defense level for one specific threat, indirectly combining the two.

10 Conclusion

Recent surveys have shown that the insider threat problem is getting equally important to the outsider threat problem. However, the latter has received more attention from the research community. We address the former by proposing a framework composed of a method for gathering goal-based requirements for defense against insiders. The method is supported by attack strategies structured in four decomposition trees, an Insider Attack Pattern and defense strategies. The framework aims to help organizations to get awareness about the insider problem in their environment and about defenses for addressing the problem, in a systematic way.

As short-term future work we plan to apply our framework in practice as an action research study in a large Dutch organization. It will enable us to validate and calibrate the framework. Additionally, it will also provide insights about our long-term future work towards developing tools to address the insider threat problem. As an example, we think of a tool for the evaluation of the defense level of an asset, to make the process of risk assessment of our framework less dependent on expert judgment.

Acknowledgments

This research is supported by the research program Sentinels (www.sentinels.nl). Sentinels is being financed by Technology Foundation STW, the Netherlands Or-

ganization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs.

References

1. Survey: E-Crime Watch 2006, CSO Magazine and U.S. Secret Service and CERT Coordination Center and Microsoft Corporation (2006) http://www.cert.org/archive/pdf/ecrimesurvey06.pdf.
2. Gordon, L.A., Loeb, M.P., Lucyshyn, W., Richardson, R.: 2006 CSI/FBI Computer Crime and Security Survey (2006) http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.
3. Gordon, L.A., Loeb, M.P., Lucyshyn, W., Richardson, R.: 2005 CSI/FBI Computer Crime and Security Survey (2005) http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf.
4. Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., Rogers, S.: Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors (2005) U.S. Secret Service and CERT Coordination Center.
5. Randazzo, M.R., Keeney, M., Kowalski, E., Cappelli, D., Moore, A.: Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector (2004) U.S. Secret Service and CERT Coordination Center.
6. Bishop, M.: Position: Insider is relative. In: NSPW '05: Proceedings of the 2005 workshop on New security paradigms, New York, NY, USA, ACM Press (2005) 77–78 http://doi.acm.org/10.1145/1146269.1146288.
7. Schneier, B.: Attack trees: Modeling security threats. Dr. Dobbs Journal (1999)
8. Sindre, G., Opdahl, A.L.: Eliciting Ssecurity Requirements by Misuse Cases. In: TOOLS-Pacific 2000: Proc. 37th Int. Conference on Technology of Object-Oriented Languages and Systems, Washington, DC, USA, IEEE Computer Society (2000) 120–131
9. Bistarelli, S., Fioravanti, F., Peretti, P.: Defense trees for economic evaluation of security investments. In: ARES 2006: Proc. 1st Int. Conference on Availability, Reliability and Security, Washington, DC, USA, IEEE Computer Society (2006) 8 pp http://ieeexplore.ieee.org/iel5/10823/34117/01625338.pdf?tp=&arnumber=1625338&isnumber=34117.
10. Stoneburner, G., Goguen, A., Feringa, A.: Risk Management Guide for Information Technology Systems. Technical Report NIST SP 800-30, National Institute Of Standards and Technology, US (2002)
11. Hayden, M.V.: The Insider Threat to U.S. Government Information Systems (1999) Advisory Memoranda NSTISSAM INFOSEC 1-99 www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf.
12. Brackney, R.C., Anderson, R.H.: Undersatanding the Insider Threat - Proceedings of a March 2004 Workshop. First edn. RAND Corporation, California, USA (2004)
13. IT Governance Institute: CobiT 4.0 - Control Objectives for Information and related Technology (2005) http://www.itgi.org.
14. Schaad, A.: A Framework for Organisational Control Principles. PhD thesis, University of York, Department of Computer Science (2003) http://www.cs.york.ac.uk/ftpdir/reports/YCST-2003-05.pdf.
15. COSO: Internal Control - Integrated Framework by Committee on Sponsoring Organizations of the Treadway Commission (1994) www.coso.org.

16. IT Governance Institute: IT Control Objectives for Sarbanes-Oxley, The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting - 2nd Edition (2006) www.itgi.org.
17. BS: ISO 17799: Information technology. Security techniques. Code of practice for information security management (2000) www.iso.org.
18. COSO: Internal Control over Financial Reporting - Guidance for Smaller Public Companies (2006) www.coso.org.
19. Schaad, A., Moffett, J.D.: A framework for organisational control principles. In: ACSAC '02: Proceedings of the 18th Annual Computer Security Applications Conference, Washington, DC, USA, IEEE Computer Society (2002) 229
20. Hayden, M.V.: The Insider Threat to U.S Government Information Systems) (1999) National Security Telecommunications and Information System Security Committee (NSTISSAM) INFOSEC 1-99 http://www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf.
21. Cappelli, D., Moore, A., Shimeall, T.: Common Sense Guide to Prevention and Detection of Insider Threat (2005) http://www.us-cert.gov/reading_room/prevent_detect_insiderthreat0504.pdf.
22. Moore, A.P., Ellison, R.J., Linger, R.C.: Attack Modeling for Informnation Security and Survivability. Technical Report CMU/SEI-2001-TN-001, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA, USA (2001)
23. Mylopoulos, J., Chung, L., Liao, S., Wang, H., Yu, E.: Exploring alternatives during requirements analysis. IEEE Software **18**(1) (2001) 92–96 citeseer.ist.psu.edu/mylopoulos01exploring.html.
24. Cappelli, D.M., Desai, A.G., Moore, A.P., Shimeall, T.J., Weaver, E.A., Willke, B.J.: Management and Education of the Risk of Insider Threat (MERIT). In: Proc. 24th Int. Conference of the System Dynamics Society, The Netherlands, Radboud University of Nijmegen (2006) www.systemdynamics.org/conferences/2006/proceed/papers/MOORE333.pdf.
25. Howard, J.D., Longstaff, T.A.: A Common Language for Computer Security Incidents. Technical Report SAND Sandia National Laboratories, US (1998)
26. Su, X., Bolzoni, D., van Eck, P.: A business goal driven approach for understanding and specifying information security requirements. In: 11th Int. Workshop on Exploring Modeling Methods in Systems Analysis and Design (EMMSAD2006), Presses Universitaries de Namur (2006) 465–472
27. Anton, A.I.: Goal-Based Requirements Analysis. In: ICRE '96: Proc. 2nd Int. Conference on Requirements Engineering (ICRE '96), Washington, DC, USA, IEEE Computer Society (1996) 136–144
28. Dardenne, A., van Lamsweerde, A., Fickas, S.: Goal-directed requirements acquisition. Science of Computer Programming **20**(1-2) (1993) 3–50 http://citeseer.ist.psu.edu/dardenne93goaldirected.html.
29. Mylopoulos, J., Chung, L., Yu, E.: From object-oriented to goal-oriented requirements analysis. Commun. ACM **42**(1) (1999) 31–37
30. Chinchani, R., Iyer, A., Ngo, H.Q., Upadhyaya, S.: Towards a Theory of Insider Threat Assessment. In: DSN 2005: Int. Conference on Dependable Systems and Networks, IEEE Publishing (2005) 108–117 http://ieeexplore.ieee.org/iel5/9904/31476/01467785.pdf.
31. Damianou, N., Bandara, A., Sloman, M., Lupu, E.: A survey of policy specification approaches. Technical report, Department of Computing, Imperial College of Science Technology and Medicine, London (2002) citeseer.ist.psu.edu/damianou02survey.html.

32. Butts, J.W., Mills, R.F., Baldwin, R.O.: Developing an insider threat model using functional decomposition. In: MMM-ACNS: 3rd Int. Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security. Volume 3685 of LNCS., Springer (2005) 412–417
33. Alberts, C., Dorofee, A.: Managing Information Security Risks: The OCTAVE Approach. First edn. Addison-Wesley, Boston, MA, USA (2002)

Appendix A - Tree structures of attack strategies

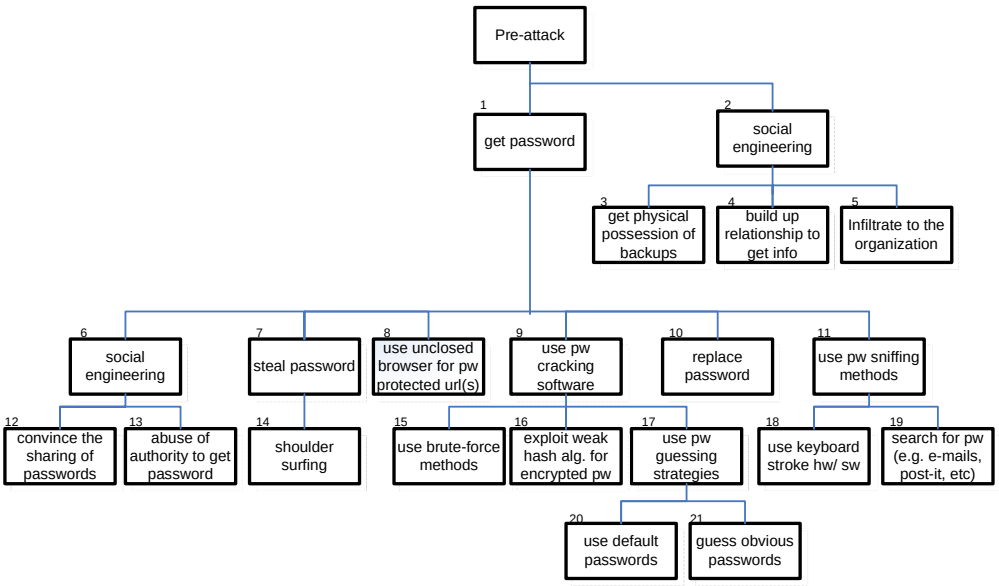

Fig. 5. Tree structure of attack strategies involved with "Pre-attack"

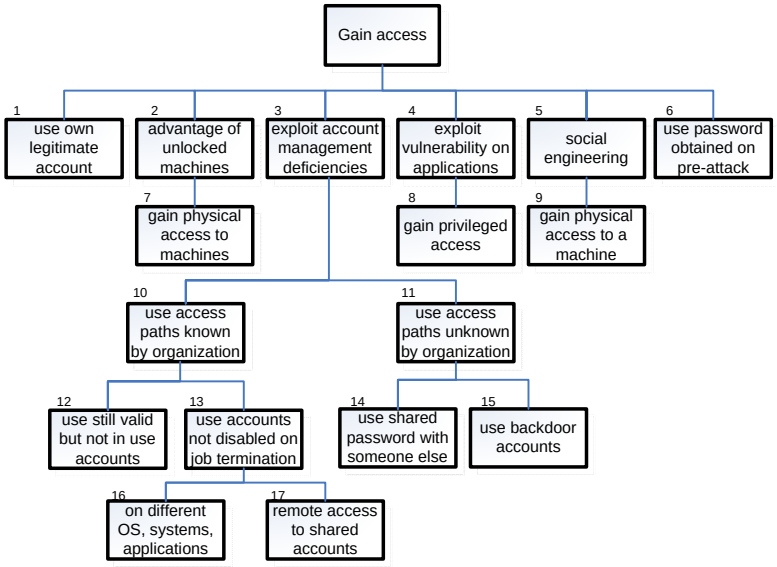

Fig. 6. Tree structure for attack strategies involved with "Gain access"

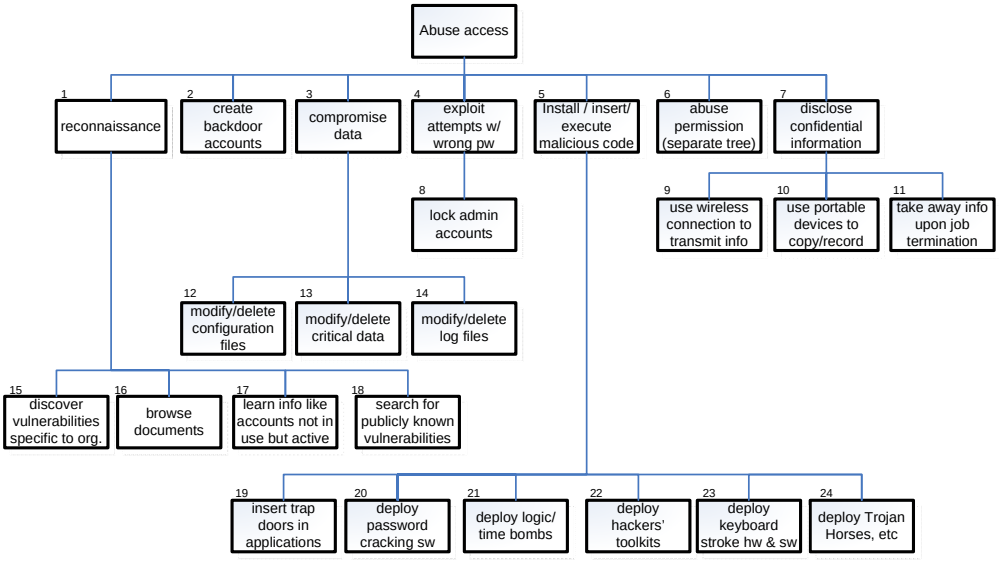

Fig. 7. Tree structure for attack strategies involved with "Abuse access"

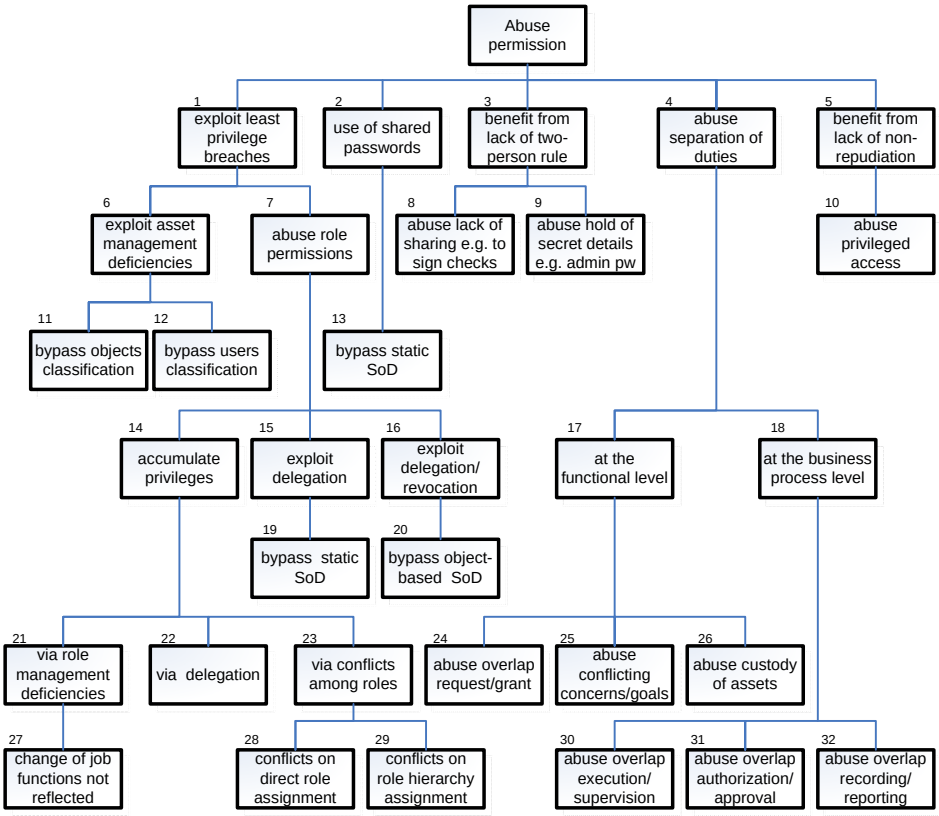

Fig. 8. Tree structure for attack strategies involved with "Abuse permission"