# 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 worrying situation, since insider attacks have a high probability of success because insiders have authorized access and legitimate privileges. 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 for identification and assessment of insider threat risks and of two supporting deliverables for awareness of insider threat. The deliverables are: (i) attack strategies structured in four decomposition trees, and (ii) a matrix which correlates defense strategies, attack strategies and control principles. The method output consists of goal-based requirements for the defense against insiders.

**Keywords:** Modeling of Security, Risk Assessment, Insider Threat

## 1 Introduction

According to recent surveys [1,2] and reports from studies [3,4] carried out by the U.S. Secret Services and the CERT (http://www.cert.org/insider_threat/), insiders are responsible for major financial losses, damages and disruptions to organizations. Worse, insider attacks are tending to rise and to become comparable in frequency to security events originated by outsiders. We consider an insider, as defined by Bishop [5], 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 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 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

* Supported by the research program Sentinels (www.sentinels.nl). Grateful to Roel Wieringa and Ben Elsinga for valuable comments on earlier draft of this paper.

insiders exists, and (ii) in more than half of the cases studied, insiders exploited vulnerabilities in applications, processes and procedures/policies, not necessarily known by outsiders. Thus, insiders do not only take advantage of technical expertise but they also take advantage of details specific to the organization and of social engineering in an environment based on trust. Additionally, insiders tend to have more opportunities, when compared to outsiders, caused e.g. by the deterioration of access and permission management which may cause accumulation of privileges. In summary, the combination of power, trust and knowledge turn insiders particularly dangerous and, as a consequence, their malicious actions have high probability to be successful and to remain undetected.

To reduce 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 e.g. step-wise or detailed approaches like attack trees [6], misuse cases [7] and defense trees [8] may become unusable due to the wide spectrum of insiders' goals. Yet another challenge is the lack of tool support for insider threat identification and assessment.

The contribution of this paper is a framework that addresses the first two challenges mentioned above. It consists of a method for identification and assessment of insider threat risks, and of two deliverables. The deliverables are: (i) insider attack strategies structured in four decomposition trees, and (ii) a matrix that relates control principles to attack and defense strategies. The purpose of these two 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. They take the perspective of control principles, which are exploited by attack strategies and enforced by defense strategies. This perspective enables us 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.

This paper is organized as follows. Section 2 briefly (i) introduces the notion of control principles, (ii) organizes insiders attack strategies in four decomposition trees, (iii) presents a matrix for matching defense strategies, attack strategies and control principles, and (iv) introduces the actual method, core of the framework. Section 3 describes an example application of the framework. In Section 4 the framework is discussed, in Sections 5 related work is reviewed, and finally, in Section 6, we conclude and point to future work.

## 2 A framework for gathering defense requirements

The proposed framework is composed of a method and of supporting deliverables. Its goal is to help organizations to identify requirements that enable defense against insiders.

Control principles are our starting point and this choice is twofold. First, insiders exploit vulnerabilities which can be achieved by exploiting control principles. Second, control principles provide mechanisms for organizations to pre-

vent and detect insiders activities. Thus, 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.

Cobit [9] 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 they are based on common control principles which apply to any organization.

The most relevant controls for this paper are: (i) Separation of Duties (SoD), (ii) Dual Control, (iii) Delegation and Revocation, (iv) Audit, (v) Least Privilege, (vi) Non-repudiation, (vii) Reconciliation, and (viii) Classification of Assets. Refer to our technical report [10] for a taxonomy of control principles.

### 2.1 Supporting deliverable: attack strategies decomposition trees

We structure attack strategies exploited by insiders in four attack strategy decomposition trees using two sources: literature [3,4,11] and our taxonomy of control principles [10]. Due to lack of space, we are only able to show in this paper the tree "Abuse permission", in Figure 1. The other trees ("Pre-attack", "Gain access", and "Abuse access") can be found in our report [10].

Decomposition trees permit the breakdown of a tree root and sub-nodes, in terms of AND/OR relations (in this paper, only OR relations are used in the decomposition trees). This kind of tree provides a structured way for the analysis of alternatives and has been used for goal-oriented analysis of requirements [12]. Towards its root, the tree allows for the abstraction of alternatives and, towards its leaves, the tree allows for precision of alternatives. The main idea of these trees is to provide a wide spectrum of strategies used by insiders to launch attacks.

Decomposition trees extend the idea of attack trees (introduced by Schneier [6]). Attack trees permit the modeling of security threats represented as the root of the tree. This threat is successively refined through AND and OR joints, indicating conjunction and disjunction between pairs of nodes for the achievement of their parent node. Thus, attack trees allow the exploration of deepness while decomposition trees allow the exploration of broadness.

### 2.2 Supporting deliverable: a matrix of attack versus defense strategies

A concise version of defense strategies, extracted from a more complete list available in our report [10], is organized in a matrix with the attack strategies.

Table 1 shows an extract (the full matrix has 15 columns and 17 rows) of such a matrix, where (i) the horizontal axis contains a list of defense strategies, (ii) the vertical axis contains the first level of nodes from the attack decomposition

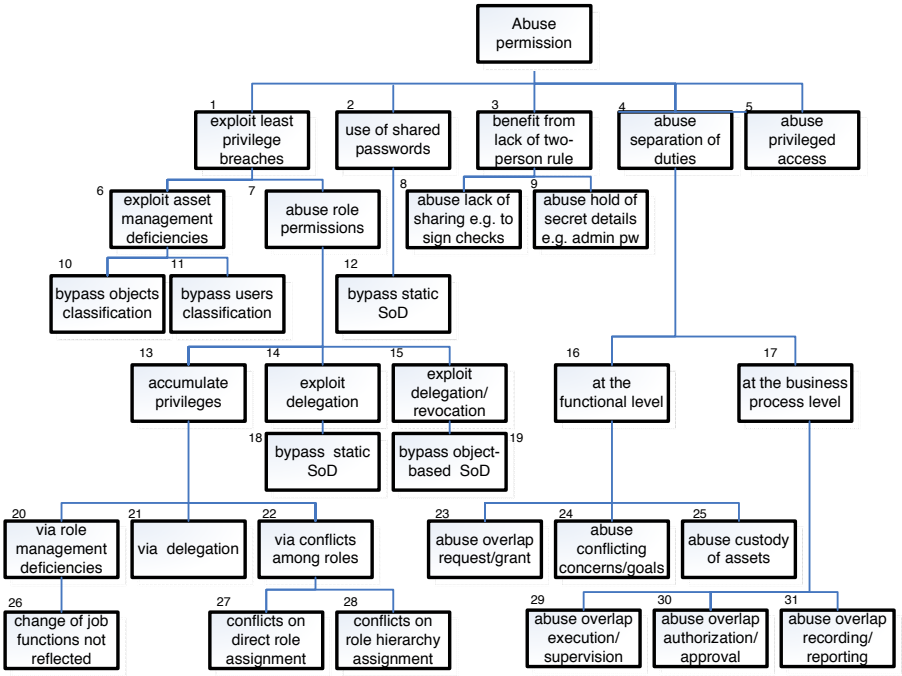


**Fig. 1.** Attack strategies involved with "Abuse permission"

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 uni… |
|---|---|---|---|---|---|---|
| Review periodically actual access paths against expected paths | AU RC LP | | AU RC LP | | AU RC LP | |
| Ensure only paths needed for job function are activated for an individual | LP | | AU RC LP | | AU RC LP | |
| Ensure deactivation of paths upon job termination | | | AU RC NR | | AU RC LP | |
| Enforce tight password management: (i) strong password, (ii) periodic changes, (iii) none out-of-box passwords | AU | AU NR | AU NR | | | |

**Table 1.** Extract from a matrix which correlates attack strategies, defense strategies and control principles

trees (where e.g. PA refers to "Pre-attack", GA to "Gain access" and so on), and (iii) the intersections 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. Defense strategies, derived from the literature [3,4,11] and from control principles, have been composed with the same objective of broadness instead of deepness as we did for the attack strategies. 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. Thus, the matrix is useful when deriving requirements for the defense against insiders.

### 2.3 Method for gathering defense requirements

The method, shown in IDEF0 notation in Figure 2, consists of 5 steps. The boxes represent steps of the method. Horizontal arrows coming into the boxes are inputs which are transformed by the steps into outputs and vertical arrows are inputs not transformed by the steps. Outputs are represented by horizontal arrows coming out of the boxes. Due to space constraints it is not possible to describe the steps of the method in this paper. Refer to our report [10] for details.

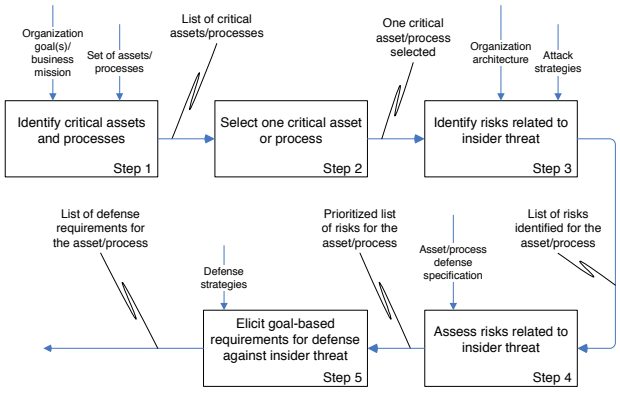


**Fig. 2.** Method for gathering requirements for defense against insiders

## 3 The framework applied: an example

Figure 3 shows an example, collected from Chinchani et al. [13], based on a fictitious financial institution. In the example, a teller can complete any personal account transaction involving up to $5,000, through the *personal account*

*database*, but only a manager can complete transactions, above this limit. Transactions on business accounts are limited to managers upon the presentation of credentials to a PKI server. Successful authentication generates a session key to access the *business account database*. Both databases are protected by firewalls to prevent external attacks.

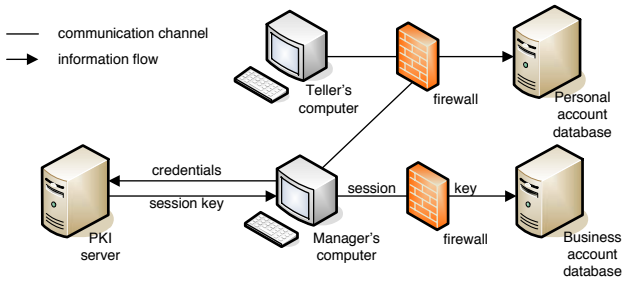


**Fig. 3.** Example from a fictitious financial institution(from Chinchani et al. [13])

### 3.1 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. In step 1, management identifies the critical assets/processes. In this very simple example, we assume that this results in the following list: (i) asset: personal account database, (ii) process: endorsement of personal account transactions over $5,000, (iii) asset: business account database, and (iv) process: business account transactions.

### 3.2 Example - step 2

We select the process "business account transactions" because, although this process seems already well protected, the board of directors wants re-assurance.

### 3.3 Example - step 3 and 4

We simulate the role of stakeholders to identify risks using as reference the four attack strategy trees. They look at each branch of the trees and decide if the risk reported is relevant for the process or if it suggests another relevant situation (i.e. sequence of steps). Table 2 shows the risks identified and assessed.

| | Risk | Defense level | Risk level |
|---|---|---|---|
| R1 | terminated manager uses his account/credentials 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** | teller *learns* a vulnerability specific to the organization, e.g. the manager does not apply security patches on a regular basis, to acquire credentials to 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, e.g., wife or boyfriend accounts (as beneficiaries) | high | low |
| **R7** | insider discloses information about business transactions to competitors or press | low | high |
| **R8** | member of application X developers team inserts a trap door in the application code which enables business transactions | low | high |
| R9 | manager shares password/credentials with a teller or another manager (e.g. in case of emergency), enabling them to impersonate the manager to perform business transactions | high | low |

**Table 2.** Risks for the critical process "business account transactions"

### 3.4 Example - step 5

In this step we identify the defense strategies which seem appropriate as countermeasures for the five risks marked in bold in Table 2. 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.

This 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.

## 4 Discussion

In this section, we discuss the proposed framework around three topics which, we believe, turn it interesting: (i) merging of access-oriented with permission-oriented approaches, (ii) abstraction from attacker *goals* and focus on attacker *means*, and (iii) shift from risk-based to defense-based assessment of insider threat risks.

The management of access control may deteriorate over time, opening security breaches for abuse from insiders. These breaches are related not only to the

| | 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.** Defense goals for the critical process "business account transactions"

authorization of access to assets but also to more subtle permissions and control principles, such as prohibition of access, delegation of authorization, separation of duties, membership to roles, etc. In the case of insiders, it is important to consider all these aspects when assessing risks.

Our approach to the modeling of insider threat concentrates not on the goals of an insider but on the spectrum of alternatives he can exploit to reach these goals. The decomposition trees ("Pre-attack", "Gain access", "Abuse access" and "Abuse permission") we propose reflect this approach of focus on means, allowing the combination of these means in countless ways to reach whatever goals. Other researchers (e.g. [11,14]) have modeled insider threat differently.

The most used approach to prioritize risks related to attacks rely on measures of attack likelihood or impact. However, it is difficult to determine probability measures for the likelihood of an insider attack in a meaningful way. It is also difficult to evaluate the impact of an insider attack since it depends on the insider intents and goals. We prioritize risks represented by insiders using the level of defense of the asset/process under analysis for a specific risk. This shift allows the classification of a same risk differently according to the level of defense or degree of resistance of the asset/process under this risk.

The deliverables of our framework aim to decrease the dependency on expert judgment for the assessment of insiders risks. We believe that stakeholders can participate more effectively and efficiently in the process of identification and assessment of risks if they have knowledge about means exploitable by insiders and defenses useful against them. However, we are aware of the subjectivity implied in the assessment of the defense level of an asset/process in our framework.

## 5 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 briefly two risk management frameworks, OCTAVE [15] and NIST SP 800-30 [16], as well as risk assessment patterns [17], considered of relevance for our work. With respect to the former, we already reviewed, along the paper, relevant related work [7,8,11,14,6].

Three points from OCTAVE are of interest for our work: (i) threats are gathered from enterprise knowledge. We believe our deliverables decrease this dependence; (ii) assets are prioritized based on threats, opposed to our approach where prioritization is aligned to organization goal(s)/business mission; (iii) vulnerabilities are identified based on catalogs of known attacks, however threats related to "accumulation of privileges" (AP-13) e.g. are hardly found in catalogs.

Two points from the NIST SP 800-30 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.

Risk assessment patterns provide the basics of the method proposed in this paper. However, two points are worth mentioning. First, the proposed framework applies the general pattern specifically to the Insider Threat domain, by means of supporting deliverables. Thus, it adds value to the patters in that sense. Second, it fills some gaps left to the implementer of the risk assessment pattern. For example, we define a simple rationale for the qualitative prioritization of risks based on the protection level in place for an asset/process.

## 6 Conclusion

We address the assessment of risks represented by insiders by proposing a framework that consists of (i) a method for gathering goal-based requirements for defense against insiders, and of (ii) two deliverables: insider attack strategies organized in four decomposition trees, and a matrix structure for matching attack and defense strategies with control principles. We do not claim that the method itself is specific for insiders and not applicable to outsiders threat. However, the framework as a whole is tailored to provide awareness to organizations towards e.g. abuse of permissions related to SoD and accumulation of roles, specific to insiders.

As a short-term plan we aim to validate and calibrate the framework through action research. As a long-term plan we aim to develop tools e.g. for the evaluation of the defense level of an asset, to make the process of defense level assessment of our framework more sistematic.

## 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. 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.
4. 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.
5. 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.
6. Schneier, B.: Attack trees: Modeling security threats. Dr. Dobbs Journal (1999)
7. 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
8. 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.
9. IT Governance Institute: CobiT 4.0 - Control Objectives for Information and related Technology (2005) http://www.itgi.org.
10. Franqueira, V.N.L., van Eck, P.: Defense against insider threat: a framework for gathering goal-based requirements. Technical Report TR-CTIT-06-75, University of Twente (2006) http://eprints.eemcs.utwente.nl/9615/.
11. Brackney, R.C., Anderson, R.H.: Undersatanding the Insider Threat - Proceedings of a March 2004 Workshop. First edn. RAND Corporation, California, USA (2004)
12. 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.
13. 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.
14. 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
15. Alberts, C., Dorofee, A.: Managing Information Security Risks: The OCTAVE Approach. First edn. Addison-Wesley, Boston, MA, USA (2002)
16. 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)
17. Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., Sommerlad, P.: Security Patterns: integrating security and systems engineering. First edn. John Wiley & Sons, Ltd, Wiltshire, GB (2006)