Information Security Governance Analysis Using Probabilistic Relational Models

Waldo Rocha Flores and Mathias Ekstedt

Royal Institute of Technology, 100 44, Stockholm, Sweden

Abstract. This paper proposes the use of Probabilistic Relational Models (PRM) for analyzing dependencies between Information Security Governance (ISG) components and its impact on process capability of mitigating information security vulnerabilities. Using the PRM enables inference between different ISG components expressed in probabilities, and also inference on the process capability. A concrete PRM which exemplifies how to assess the capability of the access control process is further presented, and thus showing how the PRM can be adapted to fit the analysis of a specific process in an organizational environment.

1 Introduction

Information Security Governance (ISG) provides a holistic approach to information security, and considers management commitment and leadership, organizational structures, user awareness, policies, processes, and technologies, all working together to ensure information security of enterprise's assets is maintained at all times [1]. In order to increase the understanding of dependencies between different ISG mechanisms, the ISG structure can be modeled with architecture metamodels. Architecture metamodels support managers to effectively plan, design and communicate IT and business related issues, i.e. they provide decision support for managers [2][3]. Modeling ISG as architecture metamodels does not only keep track of important ISG mechanisms and their internal relationship, it also provides information about any dependencies in the structure. Therefore, the behavior and effect of changes to an ISG structure can be predicted, and the structure can be established in an enterprise without using trial and error. Conclusions can therefore been drawn on the consequences in the enterprise given that one ISG mechanism (e.g. process) is not well implemented or managed, that a certain organizational or human factor has not been considered, or that an important role has not been assigned. There are several best-practice guidelines targeted to support the assessment of an organization's current ISG. COBIT [4] for instance, has been suggested as a framework for ISG. COBIT includes security-related control objectives as *check points* to achieve security and a maturity model that can be used to assess the current state of security.

The ISO 27000 is the root for a number of series of international standards for the management of Information Security. For instance, ISO 27002 is a control-based framework using the widely known "Plan-Do-Act-Check" approach to ensure information security. Its related document, ISO 27004 includes several measures that can

Rocha Flores W. and Ekstedt M..
Information Security Governance Analysis Using Probabilistic Relational Models.
DOI: 10.5220/0003588001420150
In *Proceedings of the 8th International Workshop on Security in Information Systems* (WOSIS-2011), pages 142-150
ISBN: 978-989-8425-61-4

be used to evaluate the impact of implemented security controls and thus assess the effectiveness of the information security management in an organization [5].

Current architecture frameworks for Business/IT analysis do not provide a modeling language that supports assessments in general and for information security is particular [7]. There is also little research on the use of modeling languages to support quantitative assessment for information security. One example is the work presented in [8] where attack steps were defined as a part of a threat. The presented model was used for analyzing the effect of technical countermeasures and made it possible to predict quantified expected loss values from the suggested architecture model. However, technical countermeasures are not enough own its own. The purpose of the present paper is to propose a model that can be used for analyzing ISG in an organizational environment. The presented approach includes organizational and human factors of information security in an ISG structure, and aid assessments of their impact on security process capabilities, i.e., the effect of mitigating security vulnerabilities. To support assessments the model is coupled with an assessment and analysis mechanism and extended to a Probabilistic Relational Model (PRM) - specifying a template for a probability distribution over the architecture model. The classes in this PRM are abstract and cannot be directly instantiated into an architecture model. They can however be made concrete if they are specialized into subclasses according to a set of constraints. If architecture models are instantiations of such concrete classes, then the process capability to mitigate security vulnerabilities can be inferred from the architecture model. By applying an instantiated model on real enterprise ISG environments weaknesses and potential risks of security vulnerabilities in an organization can be highlighted, thus supporting decision making and planning. The remainder of the paper is structured as follows. In the next section PRM which severs as the assessment mechanism is presented. Section three is the locus of this paper's contribution and presents the PRM for ISG analysis, and an instantiation of the PRM to show how the PRM can be used to support capability assessment of the access control process. Section four concludes the paper.

2 Probabilistic Relational Models

A Probabilistic Relational Model (PRM) specifies a template for a probability distribution over an architecture model [9]. An architecture metamodel *M* describes a set of classes, $X_1, \ldots, X_n$. Each class is associated with a set of descriptive attributes and a set of *reference slots* (relationships). The set of descriptive attributes of a class *X* is denoted *At(X)*. Attribute *A* of class *X* is denoted *X.A* and its domain of values is denoted *V(X.A)*. The set of reference slots of a class *X* is denoted *R(X)*. We use *X.v* to denote the reference slot v of *X*. A reference slot v denotes a function from X_i to X_j, and its inverse v^{-1}denotes a function from X_j to X_i. Thus, the fundamental modeling constructs are the same as in general conceptual modeling techniques. An architecture instantiation *I* (or an architecture model) specifies the set of objects of each class, the values for the attributes, and the references of the objects. It specifies a particular set of process, activities, roles, etc. A PRM template describes the metamodel for the architecture model, and the probabilistic dependencies between attributes of the architecture objects. A PRM Π, together with an instantiated architecture model of specific

objects and relations, defines a probability distribution over the attributes of the objects. This probability distribution is specified similar to a Bayesian network [10] which consists of a qualitative dependency structure and associated quantitative parameters. The probability distribution can be used to infer the values of unknown attributes, given evidence of the values of a set of known attributes.

The qualitative dependency structure of a PRM is defined by associating attributes *X.A* with a set of parents *Pa(X.A)*. Each parent of *X.A* has the form $X.\tau.B$ where $B \in A(X.\tau)$ and τ is either empty, a single reference slot υ or a sequence of reference slots $\upsilon_1,\ldots,\upsilon_k$ such that for all *i*, $Range[\upsilon_i] = Dom[\upsilon_{i+1}]$. We call τ a slot chain. Note that when $X.\tau.B$ reference attributes external to the class *X*, it might be referencing a set of attributes rather than a single one since there multiple instantiated objects of one class may exist. In these cases, we let *X.A* depend probabilistically on an *aggregated* property over those attributes constructed using operations such as *AND*, *OR*, *MEAN* etc. Considering the quantitative part of PRMs, given a set of parents for an attribute, we can define a local probability model by associating a Conditional Probability Distribution (CPD) with the attribute, *P(X.A|Pa(X.A))*. In Fig. 3, fictive numbers are included to illustrate the CPD table for the instantiated metamodel of the access control process. Using the fictive numbers gives a value that specifies the probability that the security process has high capability given that for instance the security culture in the organization is developed and that the risk awareness is high. We can now define a PRM Π for a metamodel *M* as follows. For each class *X* and each descriptive attribute $A \in At(X)$, we have a set of parents *Pa(X.A)*, and a CPD that represents $P_{\Pi}(X.A|Pa(X.A))$. Given a relational skeleton, σ_r (i.e. an instantiated metamodel without attribute values), a PRM Π specifies a probability distribution over a set of instantiations *I* consistent with σ_r:

$$P(I|\sigma_r, \Pi) = \Pi_{x\epsilon\sigma_r(X)}\Pi_{A\epsilon At(X)}. \quad (1)$$

where $\sigma_r(X)$ are the objects of each class in the instantiated metamodel. Hence, the attribute values can be inferred. A PRM thus constitutes a machinery for calculating the probabilities of various architecture instantiations. This allows us to infer the probability that a certain attribute assumes a specific value, given some (possibly incomplete) evidence of the rest of the architecture instantiation.

3 A Probabilistic Relational Model for Information Security Governance Analysis

Several definitions to the concept of ISG have been proposed by international associations, public institutions, and researchers [1][4][5][11][12][13][14]. [4] argues that ISG is about management commitment and leadership, organizational structures, user awareness and commitment, policies, processes, and technologies, all working together to ensure information security of enterprise's assets is maintained at all times [1]. [11] and [14] further emphasize assignment of responsibilities and segregation of duties as important components of ISG. Internal dependencies between ISG components such as organizational structure, and security process capabilities has been iden-

tified and validated by [15][16]. Adopting these definitions and findings, the proposed PRM for ISG analysis (Cf. Fig. 1) focuses on how a structure of ISG in an organizational environment impacts the capability of a process in terms of mitigating vulnerabilities. Therefore, a high process capability leads to fewer flaws in an organization's security mechanisms, i.e. vulnerabilities that can be exploited by an attacker.

The qualitative part of the PRM consists of classes, reference slots, attributes and their parents. A total of six classed were identified *Organizational Unit, Process, Activity, Artifact, Role*, and *Actor.* The main class in the PRM is *OrganizationalUnit* that represents an organization. An organization consists of processes and in our case; processes to mitigate security vulnerabilities. The *OrganizationalUnit* has therefore the reference slot *ConsistOf* whose range is the class *Process.* Each *Process* further consists of a set of activities that defines a process and takes and creates artifacts such as security policies, back-up storage, etc. This is represented by the two classes *Activity* and *Artifact* with an *IsapartOf* reference slot for the *Activity* class and an *ExistsIn* reference slot for the *Artifact* class. In a PRM, classes can further be specialized through inheritance relationships. The classes are related to each other using subclass relation. For instance, the *AccessControlProcess* is a subclass of *Process* (**AccessControlProcess << Process)** and then *Process* class is a superclass of *AccessControlProcess*. In the PRM this inheritance relationships is represented by an *IsakindOf* reference slot.

A role (e.g. a security manager) is assigned to a process. This relation is illustrated by the class *Role* with an *IsResponsibleFor/IsAccountableFor* reference slot whose range is the class *Process*. This *Role* class has further an *IsakindOf* reference slot illustrating that there exist several specializations of a *role*. The *SecurityManageRole* is for instance a subclass of the class *Role* (**SecurityManagerRole << Role)**, and *Role* is then a superclass of *SecurityManagerRole.* A *role* is further a resource in the organization; this relation is represented by the class *Role* with an Is*aResourceIn* reference slot whose range is the *OrganizationalUnit.* Finally, an actor fills the role, and is illustrated in the PRM with the class *Actor* and a *FillsA* reference slot with the range *Role*.

Regarding the attributes in the PRM, The *Process capability* attributes is first and foremost influenced if formal processes are effectively implemented. Further, the capability of a process is influenced by an organization's *security culture*, i.e. shared attitudes, values, goals, and practices related to information security. The organization further need to promote and communicate *security awareness*, establish security awareness programs, provide education of employees about security policies, etc. [11][13][14][15][18].

Internal efficiency in terms of the execution of activities, production of artifacts and the capability of roles has earlier been identified to influence process capability in [3][19]. We therefore, include an attribute considering if the process is *efficiently managed*. The *effective implementation* of security processes in organizations is strongly influenced by organizational factors such as *top management support, organizational size*, how reliant the organization is on information technology, i.e. *IT reliance,* and the *environmental uncertainty* [15][16][18]. Top management support may take the form of guidance during planning, participation during design or involvement during deployment. Besides the ability to secure adequate resources, top management can also encourage positive user attitude towards the use of information security. The size of the organization matters as smaller organizations suffer from a

lack of human and financial resources. With the lack of funds, smaller organizations often implement their security processes throughout the organization in a less optimal way. Depending on the type of industry the organization is active in, the requirements for security differ. For instance, information security plays a more strategic and critical role in the financial industry were the environment is highly competitive and volatile [18].

Competence is another critical factor for the effectiveness of implementing information security [18]. However, [3] argues that *competence* influences an actor's *decision making ability*, and as competence is defined as *experience* and how often an actor works with a subject by [15], these variables are included as attributes in the *Actor* class and *Role* class, which in turn influence if the process is efficiently managed in the *process* class.

In Table 1, the attributes for the abstract PRM are shown in this form, i.e. attributes together with the slot chains defining their parents. In Fig. 1, the complete abstract PRM is presented including classes, reference slots between classes, the attributes of each class and the attribute relations. The attributes of the PRM are all defined with scales. Excerpts of five attribute scales are presented in Fig. 2.

Table 1. Attributes for the abstract PRM shown together with the slot chains defining their parents.

Attribute
Process.Capability
OrganizationalUnit.SecurityCulture
OrganizationalUnit.SecurityAwareness
Process.IsEffectivelyImplemented
Process.IsEfficientlyManaged
Process.IsEffectivelyImplemented
Process.HasTopManagementSupport
OrganizationalUnit.DegreeOfITReliance
OrganizationalUnit.EnvironmentalUncertainty
OrganizationalUnit.Size
Process.IsEfficientlyManaged
Artifact.Existence
Activity.IsExecuted
Role.HasRoleCapability
Role.HasRoleCapability
Role.IsAssigned
Actor.HasDecisionMakingAbilities
Actor.HasDecisionMakingAbilities
Actor.Competence
ActorIsAwareOfRisks
Actor.Competence
Actor.DegreeOfExperience
Actor.Frequency

Regarding the quantitative part of the PRM, for each attribute local probabilities are presented using CPDs tables. Fictive numbers are used in Fig. 3 to demonstrate how

an instantiated PRM (combined with the proposed dependency model) allows inference of the process capability.

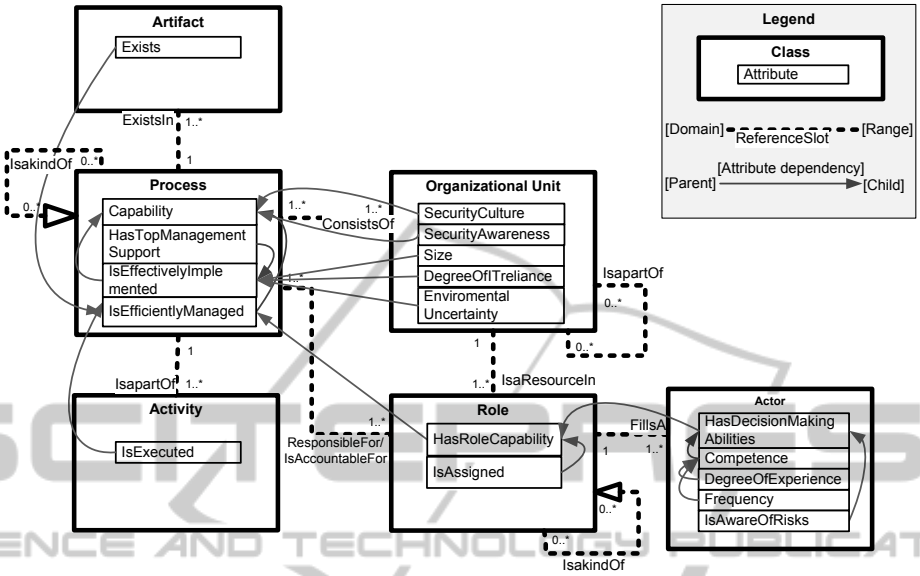

Fig. 1. The proposed PRM presenting classes, reference slots, attributes and their parents.

Class	Attribute	Definition	Model scale
Process	Has Top Management Support	The degree of Top management support for information security. Subjectively evaluated using perceptual responses	{True, False}
	Is Efficiently managed	If more than 50% of the activities related to a process is executed	{True, False}
		If more than 50% of the artifacts related to a process exists	{True, False}
		If the role is capable of managing the process or is accountable for the process	{True, False}
Organisational Unit	Security Culture	The degree of security culture in the organization Subjectively evaluated using perceptual responses	{Not developed, Developed, Highly developed}
	Security Awareness	The degree of security awareness in the Subjectively evaluated using perceptual responses	{Low, Medium, High}

Fig. 2. Examples of attribute definitions, and model calculation scales for the two classes *Process* and *Organizational Unit.*

3.1 Application to the Access Control Process

A simplified demonstration of how a modeler can use the PRM for ISG analysis applied to the access control process is presented in Fig 3. The access control process consists of 6 activities that are needed to be *executed*, 4 artifacts that should *exist*, and 2 roles that should be *assigned* in the process. In the evaluation of the fictive medium-

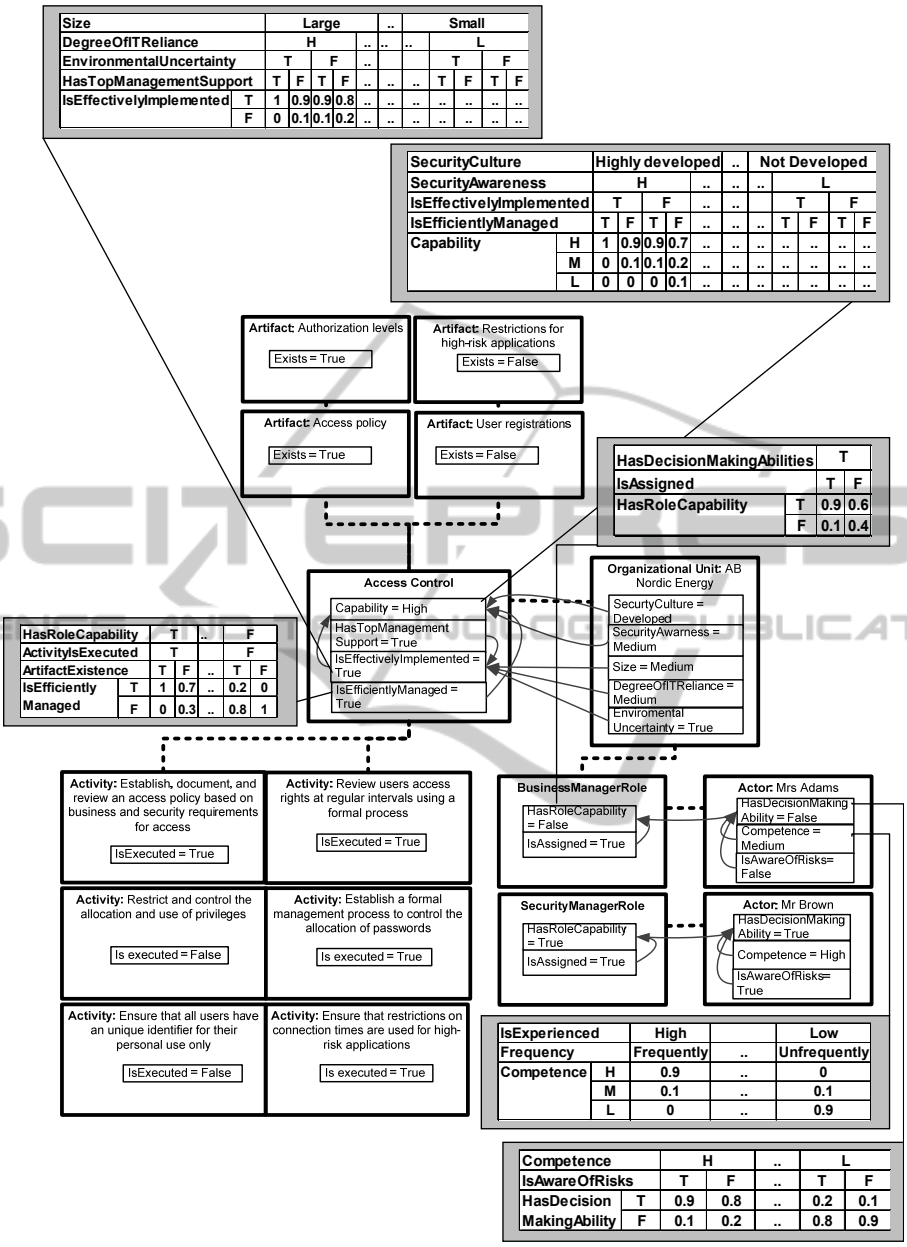

Fig. 3. The instantiated PRM for access control with CPD tables and fictive numbers.

sized company AB Nordic Energy, the modeler found that 4 out of 6 activities were executed, and 2 out of 4 artifacts existed in the process. Thus, 67% of the suggested process activities were executed and 50 % of the artifacts existed. As both values are more than 50%, these two values yield a **True** state for activities and a **False** for artifacts. Further, at least one of the business manager (Mrs. Adams) and security

manager (Mr. Brown) is responsible for managing the process. The *decision making ability* (based on their *competence* and *awareness of risks*) of the two actors was assessed to **False** and **True**. Therefore, by combining the fictive probabilistic values in the local CPD table, the attribute *IsEfficientlyManaged* yielded a **True** state.

As AB Nordic Energy is a medium-sized company active in an *uncertain environment* and at the same time is **Medium** *reliant on IT*, but have *top management support* for security endeavors, the attribute *IsEffectivelyImplemented* yielded a **True** value based on the local CPD table for the attribute. Finally, by collecting data for the last two organizational factors (*security culture and security awareness*) and combining these with the already collected data in the CPD table for the attribute *process capability,* a state of **High** was yielded.

This simplified example of how the PRM can be put into practice has shown that by collecting data from an enterprise ISG structure, using constraint such as those presented in Fig 2., a value of process capability can be inferred. Further, different components in the ISG PRM structure can be analyzed and their dependency can be calculated.

4 Concluding Remarks and Future Work

A literature review was conducted to extract important variables for the governance of information security, their relation to organizational and human factors and impact on security process capability. The main contribution with this paper is that we have argued and demonstrated the general feasibility of performing ISG analysis using PRMs. We have also provided an instantiated PRM of the access control process and thus shown how this analysis can be adapted to fit the analysis of a specific process in an organizational environment. Of interest for future work, and parts of ongoing research, is the enhancement of the PRM; focusing on more specialization of security processes to provide a PRM that can be used to analysis and calculate the aggregated capability value of several processes combined such as the risk management process, patch management process, incidents management process etc. The greatest part of future research is however to validate the qualitative structure and the attribute relations in the PRM so that the CPDs can be set with real empirical data. The data will be collected from case studies combined with surveys with the aim to improve the accuracy of the predictive function that the PRM can provide.

References

1. Von Solms, S H. Information Security Governance - Compliance Management vs. Operational Management. Computer & Security. September 2005, pp. 443-447.
2. Winter, R and Fischer, R. Essential layers, artifacts, and dependencies of enterprise architecture. Journal of Enterprise Architecture, volume 3. 2007, pp. 7-18.
3. Lagerström, Robert, et al., et al. A Method for Creating Enterprise Architecture Metamodels - Applied to System Modifiabiltiy Analysis. International Journal of Computer Science and Applications, Vol. 6, No. 5. 2009, pp. 89-120.
4. ISACA. Control Objectives for Information and related Technology: ISACA, 2007.

5. ISO/IEC. ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management. Switzerland : ISO/IEC, 2005.
6. ISO/IEC, JTC1/SC27. Common criteria for information technology security evaluation – part 1: introduction and general model: ISO/IEC, 2006.
7. A Modeling Language for Interoperability Assessments. Ullberg, J, Johnson, P and Buschle, M. Stockholm : Springer, 2011. IWEI, Lecture Notes in Business Information Processing. pp. 61-74.
8. Sommestad, Teodor, Ekstedt, Mathias and Johnson, Pontus. A probabilistic relational model for security risk analysis. Computers & Security 29. 2010, pp. 659-679.
9. Learning probabilistic relational models. Friedman, N, et al., et al. 1999. Proceeding of the 16th International Joint Conference on Artificial Interlligence. pp. 1300-1309.
10. Jensen, Finn V. An introduction to Bayesian networks. New York : Springer-Verlag, 1996.
11. ISACA. Information Security Governance: Guidance for Board of directors and Executive management 2nd Edition: ISACA, 2006.
12. ISF. The standard of Good Practice for Information Security: Information Security Forum, 2007.
13. NIST. Special Publication 800-100 Information Security Handbook: A Guide for Managers: NIST, 2006.
14. US-CERT. Governing for Enterprise Security (GES) Implementation Guide: US-CERT, 2007.
15. Chang, Shuchih E and Ho, Chienta B. Organizational factors to the effectiveness of implementing information security management. Industrial Management and Data Systems, Vol. 3 No 3. 2006, pp. 345-361.
16. Kankanhalli, Atreyi, et al., et al. An integrative study of information systems security effective-ness. Journal of International Journal of Information Management 23. 2003, pp. 139-154.
17. Knapp, Kenneth, et al., et al. Information Security Effectiveness: Conceptualization and Validation of a Theory. International Journal of Information Security and Privacy, Volume 1 Issue 2. 2007, pp. 37-60.
18. Chang, Shuchih and Lin, Chin-Shien. Exploring organizational culture for information security management. Industrial Management and Data Systems, Vol. 107 No 3. 2007, pp. 438-458.
19. Simonsson, M, Johnson, P and Ekstedt, M. The effect of IT Governance Maturity on IT Governance Performance. Information Systems Management. December 2010, pp. 10-24.