A Formal model to aid documenting and harmonizing of information security requirements

Jussipekka Leiwo and Yuliang Zheng
Monash University
Peninsula School of Computing and Information Technology
McMahons Road, Frankston, Vic 3199, Australia
Tel. +61-(0)3-9904 4287, Fax. +61-(0)3-9904 4124
E-mail: {skylark,yzheng}@fcit.monash.edu.au

Abstract

A formal top down model shall be presented to aid documentation and harmonization of information security requirements. The model formalizes layered development of information security, where top level abstract objectives, strategies and policies are step by step refined into concrete protection measure specifications. The model consists of static and dynamic parts, where static part refers to the organization, and dynamic part to the refinement of requirements. Major functions are horizontal and vertical harmonization functions used to transfer requirement into lower levels of abstraction, and to identify requirements of secure inter-operation of systems on each layer. Application of the model then consists of two parts: specification of the organization and specification of requirement harmonization functions.

Keywords

Information security development, harmonization of information security, organizational modeling

1 INTRODUCTION

A formal top down model to harmonize and document information security requirements shall be presented. Development of information security within an organization is seen

as a specification and enforcement of vertical and horizontal information security harmonization functions that are used to step by step refine abstract top level information security requirements and objectives into more concrete protection measure specifications. The model formalizes layered information security development, where the organization is divided into layers, each consisting of a set of administrative units. Based on upper layer requirements, unit specific requirements and layer specific requirements, total requirements on a given unit are specified by harmonization functions. Information security requirement here is any formal or informal statement about information security that the system should satisfy. The common approach shall be adopted, where information security refers to protection of three properties of information (ISO7498-2 1988, ITSEC 1992):

Confidentiality Information being accessible only to authorized entities.
Integrity Information being altered or removed only upon an authorized request.
Availability Information being accessible always when requested by an authorized entity

The fundamental goal of the model is to support specification and documentation of protection measures and operational procedures to enforce secure application of information systems. Components and functions of the model shall be specified formally to enable automated analysis of the target system. Formal specifications can be used to specify and verify each refinement to assure from the enforcement of higher level policies (Williams & Abrams 1995). Formal analysis is desirable also to follow the evolution of specification of protection measures from check lists to formal models (Backhouse & Dhillon 1996, Baskerville 1993). Formal presentation also supports the two major requirements of models in the development of trusted systems (Bell 1988): Faithful presentation of the situation of interest, and formal analysis of the model. Several formal access control models exist for database security (see, for example, (Castano, Fugini, Martella & Samarati 1995) for a summary) but the model presented in this paper attempts to adopt a wider perspective towards information security by considering any information security requirement as input for the model taking into account that real life security requirements originate from many different sources and are not always clarly structured. Also, no exact grammar is given to the specification of an information security requirement. At this stage, an assumption is made that any requirement, whether presented formally or informally, can be analyzed according to the model.

Due to the layered nature, the model is strongly related to hierarchies of information security policies. Layered information security policy concept shall be introduced in section 2. Based on layered security policies, the hierarchical development of information security, that the model formalizes, shall be discussed in section 3. This is also where an example is used to highlight the role of different layers. Formal specification for the model shall be given in section 4. Finally, conclusions shall be drawn and the directions for future research summarized in section 5.

2 LAYERS OF SECURITY POLICIES

The idea of establishing a harmonized framework for the development of information security within corporations started when studying the requirements that legislation should satisfy to provide an adequate protection against computer network crime (Leiwo 1995*a*, Leiwo 1995*b*). The need for a harmonized legislation in several nations, as for example the European Union is attempting to establish, lead to the identification of fundamental components of the hierarchical information security development. The model was first described by a case, where the development of information security is divided into five major layers, further divided into three categories, as illustrated in figure 1. Characteristics of categories are as follows:

Strategic Decision Category International and national objectives, standards, decisions, and guidelines establishing a harmonized framework for the information security development in several organizations. Requirements set at these layers are those that the operational environment sets to organization concerning protection of sensitive data and privacy of humans, or required or minimum level of security required in different transactions.

Organization Administrative Category Strategies and policies specific to each organization, adapting international and national framework for the organization specific needs and establishing a systematic approach for the development of information security within the organization. Requirements at this level are organization specific and contain all requirements that are concerned with storage, processing and transmission of information within the organization or to external parties.

Implementation Category Specifying and implementing mechanisms to guarantee the adequate level of protection for systems to satisfy the corporation information security objectives. This is where required protection measures are implemented and operated. Requirements include requirements on implementation methods and tools and may require changes on upper level requirements in order to improve cost efficiency of protection and to ensure secure interoperation of different systems.

The division into categories is influenced by the layered security policy concept (Abrams & Bailey 1995, Olson & Abrams 1995, Sterne 1991) where information security policy consists of three layers each representing different views to the system: Corporate Security Policy, Organizational Security Policy, and Technical Security Policy that can be further divided into sub policies according to the organization. Fundamental layers of policies can be described as follows:

Corporate Security Policy Laws, rules, and practices that regulate how assets including sensitive information are managed, protected, and distributed within a user organization. This level represents top management's view of the system.

Organizational Security Policy Laws, rules and practices that regulate how an organization manages, protects, and distributes resources to achieve specifies security policy objectives. At this level, criteria should be defined for conditions under which entities are allowed to access resources. This level represents system users view on the system.

Technical Security Policy Laws, rules, and practices regulating the processing of sensitive information and the use of resources by the hardware and software on an IT system or product. This level represents system builders view of the system.

This layer security policy approach is then considered in association with the conceptual information system meta model, named PIOCO (Iivari 1983). The meta model divides development of an information system into three levels that are used to analyze different levels of abstraction of the becoming system. The three levels of the meta model are pragmatic level (P), info-logical/organizational level (IO) and constructive/operational level (CO). Within this paper, these levels of abstraction have been adapted into the development of information security by roughly mapping them to fit the categories where requirements of different abstractions of information security requirements are created, so that pragmatic level refers to strategic decision category, info-logical/organizational level refers to organization administrative category, and constructive level refers to implementation category.

As establishment and enforcement of layered security policies refers mostly to the vertical harmonization within our terminology, the justification of horizontal harmonization is still open. Assume two separate secure systems, that need to inter-operate in a secure manner. As studied by, for example, (Gong & Qian 1994), decision about security of interoperation is a computationally complex task. Due to this complexity, assurance of the security of interoperation shall be provided by enforcing harmonized refinements of security requirements at each layer of different systems security development by horizontal harmonization functions. Secure interoperation is approached by analyzing interoperability at each level of abstraction, and then harmonizing requirements between different units that need to inter-operate.

3 HARMONIZED DEVELOPMENT OF INFORMATION SECURITY

Within this section, the harmonized development of information security shall be described. Figure 1 illustrates a five-layer case, that this analysis is based on. First two layers provide an external coordination, that shall be studied in section 3.1. Next two layers, Organization Layer and Business Unit Layer, are where the security management

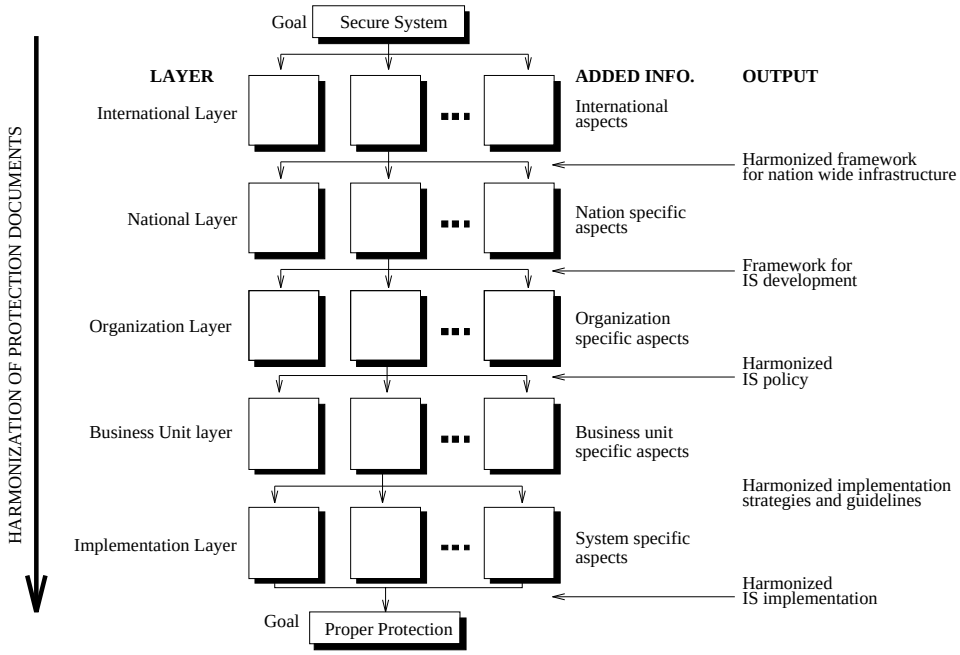

Figure 1 Harmonized development of information security

within an organization is enforced and shall be studied in section 3.2. Lowest layer, implementation of protection measures shall be studied in section 3.3. During the analysis, an example shall be given on the application of the approach into the European Union Directive concerning the protection of individuals in relation to the processing of personal data (EC-C277 1990). Requirements of the directive shall be transferred throughout the development organization to highlight different tasks at each layer.

3.1 External coordination

Most information systems get their security requirements from outside, from, for example, laws and governmental decisions. These documents also provide organizations a base for security work. When developing information security within an organization, international and national standards, strategies, laws and other decisions must be taken as a starting point. They are needed to establish a framework for the corporation information security management. International strategies, for example, set components of information security, classification and evaluation of information security, general guidelines on the goals and requirements of security work and so on. When the security of global systems, where physically distributed components are located across national borders, the importance of international coordination of law increases. International coordination is required to avoid situations, where weaknesses and inconsistencies of nationally different juridical environ-

ments can be exploited either to use logical connectivity to commit a criminal act from a country having a weak legislation or use logical connectivity and target a system in a country having inadequate legislation.

The example directive specifies contents of law that each member nation should implement according to nation specific characteristics. A generic specification is given on the contents of the required law with regard to acceptable processing and storage and required protection of personal data. Upper level requirements for nations are here the requirements set by the directive, that provides each country a harmonized base to establish their national law based on country specific special features. Each of the high level requirements set by the directive must be considered nationally within each member country. This provides international organizations with the assurance of the critical topics being addressed by each member nation.

3.2 Organizational coordination

The management level, Organization Layer and Business Unit Layer within figure 1, is where the corporation information security work is coordinated. Based on the operating environment, the top management of the organization is responsible for specifying corporation security policies and strategies. Top management is responsible of the organization information security violations but is also authorized to establish policies and procedures that concern the entire organization. Management has to face two factors (Anderson, Longley & Kwok 1994): The probability that the threat will eventuate, and the potential financial outcome of the business impact. As it is not the responsibility of the security staff to make business decisions in the risk environment, it is essential that the management contributes actively to the security work.

Information security management within organization operates between those who set responsibilities and those who fulfill these requirements. Requirements are set by corporation (or business unit) management and fulfilled by system users and developers. Two major obligations of the security management to the general management are to ensure that security requirements imposed on the system will adequately protect the organization's resources and data, and to ensure that the system is operated in a manner that satisfies its security requirements (Bailey 1995).

Corporations dealing with personal data must then set their security strategies and policies to take into account the requirements set by national laws concerning protection of personal data. As required by example directive, protection measures must be implemented against different threats against the data and guidelines must be established and enforced to control the flows of the information under the law. The protection requirements by law are the minimum requirements. It may be, that at some level, other measures required are stronger than those required by law. In this case, layer or unit specific requirements over ride the upper level requirements, and a stronger security results. In the

case of stronger requirements set by a specific unit, horizontal harmonization is required to identify other units that co-operate with the unit with higher requirements. Requirements at these units must then be aligned with the unit having highest requirements to guarantee secure interoperability.

3.3 Implementation of protection measures

To guarantee consistent approach to the information security development, security mechanisms must be aligned with the corporation policies. Mechanisms must guarantee satisfaction of corporation general goals as well as satisfaction of the specific information security requirements of different systems. Implementation layer is the final step in the development of information security. It includes definition, implementation and monitoring of the information security mechanisms. Two major requirements can be set for implemented controls and protection measures. They should be selected so that they can adequately counter the threats found during risk assessment, that means they enforce the security policy, and they should be implemented in a cost-effective manner. Important factor is to not overestimate protection measures, security measure is efficient when it costs less than alternatives, including doing nothing.

Combination of several factors affecting cost of protection results as a graph where costs are high now and in the far future, but as minimized as possible during the optimal time frame (Cohen 1995). An important factor reducing security of information systems is the lack of integration of security measures from the very early stages. No single design element, that may be operating system, application, or network, alone is capable of providing adequate security. Another controversial issue in the implementation layer is how to guarantee, that all informal requirements set at higher layers of the model, shall be transformed into the actual implementation of information security measures, that is enforcement of corporate information security policy.

When different requirements are harmonized at upper levels, different domains can be identified. Once implemented, the cost-effectiveness can be improved by identification of similar functionalities and using same design and implementation documents in each case. Also, at this point similar requirements between different units can be horizontally harmonized to simplify the implementation, and hence improve cost efficiency.

4 THE MODEL

The harmonized development model for information security shall be studied in detail in this section. Static components of the model shall first be specified in section 4.1. Based on these components, harmonization functions can be specified to provide comprehensive re-

quirements of each unit. Section 4.2 studies harmonization functions in detail. Situations, where the model needs to be refined, shall be studied in summarized 4.3.

4.1 Components of the model

The model can be presented as a 4-tuple (L, U, I, S) where L refers to layers, U to units, I to layer specific requirements and S to unit specific requirements. $L = \{L_i | i = 1, 2, \ldots N\}$ is layers L_1 to L_N, L_1 being the top layer. Each layer L_i consists of $count(i)$ units $U = \{u_{i,j} | i = 1, 2, \ldots, N; j = 1, 2, \ldots, count(i)\}$, where function $count$ refers to the number of units on a given layer. $I = \{I_i | i = 1, 2, \ldots, N\}$ are the layer specific requirements of a layer L_i. Unit specific requirements are the set $S = \{s_{i,j} | i = 1, 2, \ldots, N; j = 1, 2, \ldots, count(i)\}$. All these components, L, U, I, and S are static, whereas other components of the model, requirements R, and harmonization functions τ and ρ are dynamic.

Each unit $u_{i,j} \in U$ on a given layer has its total requirements $R_{i,j} \in R$ that are based on the previous layers' output, layer-specific requirements, and unit-specific requirements. An exact specification shall be given in equation 5, in section 4.2. The output from upper layers and identification of similar requirements within each layer establishes the harmonized approach for the information security development.

Vertical harmonization within each unit $u_{i,j}$ is enforced by two related sets, $Parent \subset U$ and $Child \subset U$. They are specified so that the set $Parent(u_{i,j}) = \{u_{i-1,j'}\}$ is the set of all those units $\{u_{i-1,j'}\}$ that set requirements for the unit $u_{i,j}$. Similarly, $Child(u_{i,j}) = \{u_{i+1,j''}\}$ where the unit $u_{i,j}$ sets requirements for each unit in $\{u_{i+1,j''}\}$. For each layer L_i, layer-specific requirements, I_i, can be specified to set requirements for each unit at that layer.

To be adequately established, the model should satisfy three conditions: First, the division into layers should be complete, as specified in "Completeness of Layers" condition 1. Intuitively, this means that each unit $u_{i,j} \in U$ should belong to a layer. Second, each layer should be unique, that means no unit can belong to more than one layer. This is determined by condition 2, "Uniqueness of Layers". The model should also satisfy is the "Uniqueness of Units" (condition 3) that says, that the the forming of units should be unique.

Condition 1 (Completeness of Layers) $\forall u_{i,j} \in U | u_{i,j} \in \bigcup_{n=1}^{N} L_n$

Condition 2 (Uniqueness of Layers) $\bigcap_{n=1}^{N} L_n = \emptyset$

Condition 3 (Uniqueness of units) $\forall u_{i_1,j_1}, u_{i_2,j_2} \in U | (u_{i_1,j_1} = u_{i_2,j_2}) \Rightarrow ((i_1 = i_2) \wedge (j_1 = j_2))$

4.2 Harmonization functions

The two major functions within the model are vertical and horizontal harmonization of requirements. In the very essence, vertical harmonization means transformation of abstract upper layer requirements into more concrete lower layer requirements. Horizontal harmonization refers to the identification and harmonization of requirements that need to be similar within each unit on a given layer. The nature of vertical harmonization is interaction between units at different layers, whereas horizontal harmonization is interaction between units at same layer. Vertical harmonization, therefore, is the enforcement of the hierarchical development of information security, whereas horizontal harmonization is the enforcement of secure inter-operation of systems.

Each unit $u_{i,j} \in U$ gets requirements $R_{i,j} \in R$ as a result of requirements originating from upper layers $\{R'_{i-1,j'} | u_{i-1,j'} \in Parent(u_{i,j})\}$, from unit-specific requirements $S_{i,j} \in S$, and from layer-specific requirement $I_i \in I$ (see equation 5). Let $\tau : \{R \times S \times I\} \rightarrow R$ be a set of vertical harmonization functions, specified in equation 1. Function $\tau_{i,j}$ specifies the harmonization of requirements from unit $u_{i,j}$ to all units $u_{i+1,j'} \in Child(u_{i,j})$. Vertical harmonization within the model refers to the identification of functions τ in a top-down fashion. The top down approach is required to provide an integral and formal approach to the specification or high level abstractions of requirements that can then be formally refined.

$$\tau_{i,j}(R_{i,j}, S_{i,j}, I_i) = R'_{i+1,j'} | u_{i+1,j'} \in Child(u_{i,j}) \tag{1}$$

As each unit may have more than one parent-units, and each unit may have several child-units, some of the requirements within each layer must be similar. Horizontal harmonization within the model is required to guarantee secure interoperability between units at same layer. Typically, different systems need to communicate between each other. Horizontal harmonization is required to guarantee that none of the links in the communication flow weakens the level of security under requirements set at the upper level. The basic form of horizontal harmonization is specification of layer-specific requirements I, but in addition to that, identification of similar requirements originating from upper layers within a given layer may be required. A simple example of horizontal harmonization is specification of password protection of systems. The requirement to have password protection (if considered adequate) is a reasonable high level decision. Anyhow, it is not the duty of high level management to specify requirements on length, expiration, required structure, storage method, and other properties of passwords. For example, let us assume, that two different systems S_1 and S_2 need to inter-operate, and they have got a top level requirement of password based protection. If, for example, required length of a password in system S_1 is greater than required length at system S_2, the communication requirement may violate the security level of S_1.

To prevent such a violation, horizontal harmonization is a function to identify all requirements providing with requirements on same properties, like password length in the previous example and provision of horizontal harmonization function ρ_i at each layer L_i. As the requirement is not specified, an assumption is made, that a requirement consists of two parts: identity and the actual requirement. Let the notation $R_{i,j}^{id}$ be used to indicate the identity of a requirement $R_{i,j}$. Also, let the set $ID_i = \{id_n\}$ be a set of n different identities of requirements at a given layer L_i. Horizontal harmonization on a given layer L_i is identification of sets $\{H_i^{id} | id \in ID_i\}$, where $\forall id \in ID_i | H_i^{id} = \{R_{i,j} | R_{i,j}^{id} = id\}$. Function $\rho_i : R \rightarrow R$ on a given layer and id can be specified as in equation 2, where $R'_{i,j}$ is specified as in equation 1.

$$\rho_i(R'_{i,j}) = R_{i,j} | R'_{i,j} \in H_i^{id} \tag{2}$$

Each unit $u_{i,j} \in L_i, i > 1$ has specific security requirements $R_{i,j}$ that are combination of requirements from parents of that unit $\{R_{i-1,j'} | u_{i-1,j'} \in Parent(u_{i,j})\}$, layer-specific requirements I_i and requirements specific for the unit, $S_{i,j}$ when harmonized by a vertical and horizontal harmonization functions $\tau_{i,j}$ and ρ_i. Function $\tau_{i,j}$ generates vertically harmonized requirements $R'_{i,j}$ as illustrated in equation 3. These vertically harmonized requirements are then harmonized horizontally by ρ_i function. It should be noted, that in the case $i = 1$, requirements, $R_{i-1,j'} = \emptyset$.

$$R'_{i,j} = \bigcup_{u_{i-1,j'} \in Parent(u_{i,j})} \tau_{i-1,j'}(R_{i-1,j'}, I_{i-1}, S_{i-1,j'}) \tag{3}$$

Horizontal harmonization is harmonization of requirements $R'_{i,j}$ that are similar at all units within a given layer to guarantee secure interoperability between units. Similar requirements can be identified based on the identity of requirements. An assumption is made, that each requirement $R'_{i,j}$ can be uniquely identified by the requirement identity $R_{i,j}^{'id}$. Horizontal harmonization on a given layer L_i is identification of sets H_i^{id} for each $id \in ID_i$, where $H_i^{id} = \{R'_{i,j} | R_{i,j}^{'id} = id\}$ and specification of horizontal harmonization functions $\rho_i : R' \rightarrow R$ that harmonize vertically harmonized requirements $R'_{i,j}$ to actual requirements $R_{i,j}$ as specified in equation 4. ID_i refers to a set of different identities on a given layer L_i.

$$R_{i,j} = \rho_i(R'_{i,j}) \tag{4}$$

Comprehensive harmonization, where total requirements R are specified, is done in two phases. First, vertical harmonization of upper layer requirements is carried out, and the

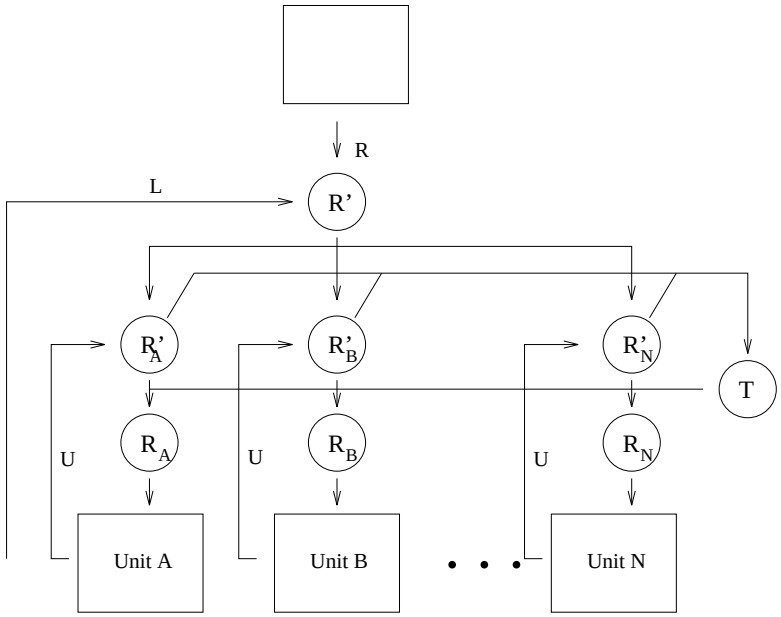

Figure 2 Harmonization of requirements

output is then horizontally harmonized layer wise. The specification is given in equation 5. This is also illustrated in figure 2.

$$R_{i,j} = \rho_i(\tau_{i-1,j'}(R_{i-1,j'}, I_{i-1}, S_{i-1,j'})|R_{i-1,j'} \in Parent(u_{i,j})) \quad (5)$$

4.3 Refinement of the model

Application of the model includes two tasks: modeling the organization, and specification and enforcement of harmonization functions. The organization is expected to be static whereas harmonization functions change more often. The following cases, are where the model should be refined in order to maintain its validity:

1. Organizational change, for example appearance or disappearance of some units in organizational restructuring.
2. A change has occurred in some layer specific requirements, requiring refinement of harmonization functions from that layer downwards.
3. A change has occurred in unit specific requirements, requiring refinement of harmonization functions from that unit downwards.
4. Within the periodical refinement of information security within the organization.

The cost of change can easily be calculated according to the amount of changes needed to maintain the model. Obviously, organizational changes cost most since most factors of the model need to be refined. Major refinements, like within periodical refinement of information security within organizations, the cost may be reasonable small but the frequency may increase the total cost. Again, automation can be used to reduce the cost of chances in static parts of the model.

5 CONCLUSIONS AND FUTURE WORK

A formal model has been presented to aid in documentation and harmonization of information security requirements. The model assumes a hierarchical, layered, information security development organization and specifies vertical and horizontal harmonization functions in order the establish cost effective protection. Information security requirements originate from many different sources, and may be fragmented. Vertical harmonization provides each layer a common view of requirements established at upper layers, so protection measures can be as identical as possible. Horizontal harmonization identifies similar requirements at each layer to provide a common approach towards them to simplify the implementation and maintenance, and to guarantee secure interoperability of different units within that layer.

The model itself acts as a starting point for further work. Once the formal model is established, different automation of specification and verification of requirements is enabled. There is a need to specify tools and methods to support harmonization, and to test the strength of the model in real life environments. Even though not done here, the model also enables formal analysis of different properties of the information security management itself, like the security of security management. If the organization can be modeled, then established access control and information flow models can be applied to give a formal specification for security properties of the organization.

Another essential topic of research is analysis of requirements. At this stage, no exact specification is given to the contents of requirements, rather the focus has been on the harmonization tasks. To get the most out of the formalism, an exact specification should be given to an information security requirement and refinement and dependencies should be analyzed according to the specification.

REFERENCES

Abrams, M. D. & Bailey, D. (1995), Abstraction and refinement of layered security policy, *in* M. D. Abrams, S. Jajodia & H. J. Podell, eds, 'Information Security - An Integrated Collection of Essays', IEEE Computer Society Press, Los Alamitos, CA, USA.

Anderson, A., Longley, D. & Kwok, L. F. (1994), Security modelling for organisations, *in* '2nd ACM Conference on Computer and Communications Security', Fairfax, Virginia, USA.

Backhouse, J. & Dhillon, G. (1996), 'Structures of responsibility and security of information systems', *European Journal of Information Systems* **5**, 2–9.

Bailey, D. (1995), A philosophy of security management, *in* M. D. Abrams, S. Jajodia & H. J. Podell, eds, 'Information Security - An Integrated Collection of Essays', IEEE Computer Society Press, Los Alamitos, CA, USA.

Baskerville, R. (1993), 'Information systems security design methods: Implications for information systems development', *ACM Computing Surveys* **25**(4), 375–414.

Bell, D. E. (1988), Concerning "modeling" of computer security, *in* 'IEEE Symposium on Security and Privacy'.

Castano, S., Fugini, M., Martella, G. & Samarati, P. (1995), *Database Security*, ACM Press.

Cohen, F. B. (1995), *Protection and Security on the Information Superhighway*, John Wiley & Sons, inc.

EC-C277 (1990), 'Proposal for a council directive concerning the protection of individuals in relation to the processing of personal data', Official Journal of the European Communities No C277.

Gong, L. & Qian, X. (1994), The complexity and composability of secure interoperation, *in* '1994 IEEE Symposium on Research on Security and Privacy'.

Iivari, J. (1983), Contributions to the theoretical foundations of systemeering research and the PIOCO model, Acta Universitatis Ouluensis A150, University of Oulu, Oulu,Finland.

ISO7498-2 (1988), 'International standard ISO 7498-2. information processing systems - Open systems interconnection - Basic reference model - Part 2: Security architecture'.

ITSEC (1992), 'Information technology security evaluation criteria (ITSEC). Provisional harmonized criteria, version 1.2', Commission of the European Communities COM(92) 298 final, Brussels, Belgium.

Leiwo, J. (1995*a*), Deterrence of computer network crime: The international coordinative level approach towards legislation, Working Papers Series B 35, University of Oulu, Department of Information Processing Science, Oulu, Finland.

Leiwo, J. (1995*b*), Deterring computer network criminals with legislative methods: The need for international harmonization, *in* 'GRONICS'95 International Information Technology Conference for Students', University of Groningen, Groningen, the Netherlands.

Olson, I. M. & Abrams, M. D. (1995), Information security policy, *in* M. D. Abrams, S. Jajodia & H. J. Podell, eds, 'Information Security - An Integrated Collection of Essays', IEEE Computer Society Press, Los Alamitos, CA, USA.

Sterne, D. F. (1991), On the buzzword Security Policy, *in* 'IEEE Symposium on Security and Privacy'.

Williams, J. G. & Abrams, M. D. (1995), Formal methods and models, *in* M. D. Abrams,

S. Jajodia & H. J. Podell, eds, 'Information Security - An Integrated Collection of Essays', IEEE Computer Society Press, Los Alamitos, CA, USA.

BIOGRAPHIES

Jussipekka Leiwo received his M.Sc. in computer science from the University of Oulu, Finland, in 1995. From March 1995 to April 1996 he was employed by Nokia Telecommunications in Helsinki, Finland. Since April 1996, he has been enrolled in Ph.D. studies at Monash University, Peninsula School of Computing and Information Technology, focusing on information security management.

Yuliang Zheng received his B.Sc. degree in computer science from Southeast University (formerly Nanjing Institute of Technology), Nanjing, China, in 1982, and the M.E. and Ph.D. degrees, both in electrical and computer engineering, from Yokohama National University, Yokohama, Japan, in 1988 and 1991 respectively. From 1982 to 1984 he was with the Guangzhou Research Institute for Communications, Guangzhou (Canton), China, and from February 1991 to January 1992 he was a Post-Doctoral Fellow at the Computer Science Department, University College, University of New South Wales, in Canberra, Australia. From February 1992 to January 1995 he was a Lecturer of the Computer Science Department, University of Wollongong. Since February 1995 he has been a Senior Lecturer at the Peninsula School of Computing and Information Technology, Monash University, in Melbourne. His current research interests include information security, cryptography, computational complexity theory and information theory. Dr. Zheng is a member of IACR, ACM and IEEE. He has a homepage at http://pscit-www.fcit.monash.edu.au:/~yuliang/.