A Framework for the Management of Information Security

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

Abstract

Information security is based on access control models and cryptographic techniques. These are well established areas of research in computer security, but are not capable of supporting development of comprehensive information security within organizations. There is a need to study upper level issues and to provide with organizational mechanisms to identify security enforcement mechanisms and specify policies that coordinate these mechanisms. This paper summarizes one such framework and identifies major components and critical success factors of the approach.

1 Introduction

Computer security is based on access control models and modern cryptography. Research in formal access control models started at early 1970's, when Bell and LaPadula published their model [3] that triggered significant amount of research leading to other similar models such as Biba model for integrity [4] and other lattice based security models [16] and other access control models, such as [6], and to models that used advanced languages to specify access control rules, such as [22]. A significant area of recent research are role based access control models [17]. Well established research in access control models also lead to the evaluation of secure systems according to different criteria, the most significant being the U.S. DoD Trusted Computer System Evaluation Criteria (TCSEC) [1], also known as "Orange Book".

In 1976, Diffie and Hellman published their article that introduced public key cryptography [7]. This, together with the increasing interest in secure communications over networks, lead to a quickly expanding area of research in cryptographic techniques. As access control models are the foundation for security in centralized systems, cryptography is the foundation for secure communications over insecure networks. Research in cryptography lead to several cryptographic models, employing both private keys, such as DES [9] and SPEED [24], and public key systems such as RSA [15] and ElGamal cryptosystem [8]. Also, several tools evolved for other applications of cryptography, such as provision of digital signatures and advanced authentication methods [18]. Recent research also suggests combination of encryption and digital signatures in order to improve efficiency of protection [23].

*Corresponding author

Access control and cryptographic models focus on provision of secure operation of a system based on certain operational criteria, known as security policy. Access control models enforce a formal access control policy and cryptographic models enforce security based on policy, usually expressed as one ore more cryptographic keys. From an organizational point of view, both foundations of computer security focus on lower layer activities and do not address issues that are critical in the organizational coordination of computer security, that is management of information security. Access control and cryptographic models provide security at layers 3 and 4 in the elaboration stack of information security [21] but do not address upper layer issues that are essential in the development of secure systems [11].

This paper provides a comprehensive framework for the management of information security, that is to study information security at higher layers in the elaboration stack. This is essential in order to provide with organizational coordination for the application of security models and to guarantee that specification and implementation of security enforcement measures are cost-effective, consistent and free of conflict, hence, to provide with adequate security.

The paper begins by the introduction of an architecture for the management of information security in section 2. After this, areas identified in the architecture shall be analyzed in detail in section 3. The approach shall be critically analyzed in section 4, and conclusions shall be drawn and directions highlighted for future work in section 5.

2 Management architecture

From a wide point of view, information security can be seen as a provision of protection measures up to ecological and social facets of information systems [10]. From a practical and research point of view, the scope needs to be narrowed. Within this paper, management of information security is seen as a specification and enforcement of information security meta policies that coordinate actual information security policies [12]. The upper and lower boundary of the duties of the managerial information security personnel need clearly defined boundaries, that can be specified as follows:

Upper boundary can be seen as the formulation of information security requirements based on information security objective set by the top management. Information security objectives are informal statements regarding to the desirable security of operations and are usually based on different national and international laws, agreements, standards and organizational business objectives.

Lower boundary is in the specification of different security policies based on the upper layer security requirements. From a managerial point of view, it is assumed that once identified and specified, security enforcement mechanisms can be implemented in a manner that enforces the desired security.

This is also illustrated in figure 1. Duties of the management include formulation of security requirements based on organizational security objectives, and harmonizing [13] these requirements in order to reduce their level of abstraction step by step, and to optimize them in order to improve cost-efficiency of protection. This includes specification of different harmonization, optimization, consistency and correctness criteria for information security requirements. Typically, security requirements originate from more than one source, and therefore it is essential to specify routines and procedures for resolving potential conflicts that may occur among different requirements. These operations lead to the specified technical protection measures that can be then implemented by security enforcement mechanisms, such as access control and cryptographic models.

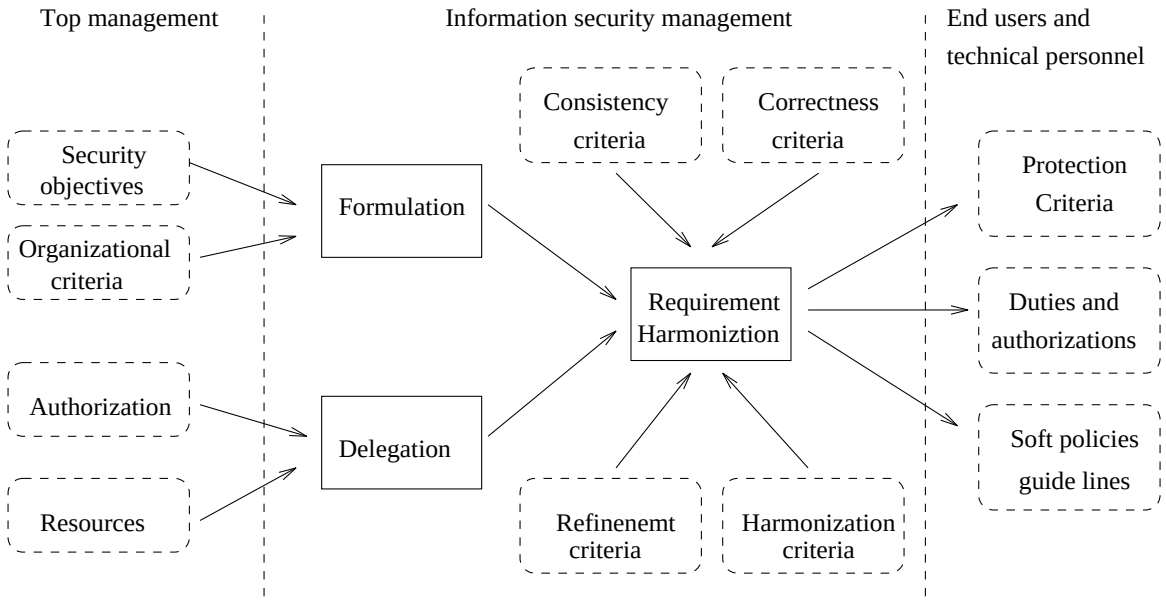

Figure 1: An architecture for the management of information security

Another track of duties of the management of information security is within the specification of duties and authorities for the secure operation of systems. Some source suggest that information security is mostly concerned with the specification of structures of responsibilities within organization [2] and therefore the importance of delegation of duties and authorities should not be underestimated. The top management is in charge of secure business operations, and has an authority to set policies that govern entire organization. This authority and responsibility is then delegated to the information security personnel that further designs different structures of responsibilities and different non-technical security enforcement functions, such as user education, to support technical protection measures. Even though essential, the issue shall not be further considered within this paper but the focus shall be on the determination of technical policies and mechanisms from high level security objectives.

3 Areas of consideration

This section provides with an analysis of critical factors identified in the previous section. The focus shall be on the specification of technical policies and mechanisms, questions of authority and "soft policies" such as user education shall ne be considered. First essential facet is the specification of the security organization. Then, specification of requirements based on security objectives shall be studied, and the criteria to process requirements shall be studied. Finally, the conflicts of requirements, and their resolving strategies shall be analyzed.

3.1 Specification of the organization

Typical organization for information security is hierarchical. The architecture assumed (figure 1) also assumes that information security is working under top management and structures and responsibilities within the organization can be clearly specified. A formal specification for the security development organization has been given in [13], and is based on two relationships between organizational units: Child and Parent -relationships. This approaches provides with flexibility to adapt the security development

model into changing environments, where non-traditional organizational structures may occur, such as matrix organizations and virtual organizations where hierarchies are flat and rapidly changing.

Relationships are based on the flow of requirement primitives within the process of harmonizing of requirements. In large organizations, there are several layers of units until security objectives are processed into technical security policies and specifications of security enforcement mechanisms. From a wide point of view, the security organization consists of also external entities, such as national and international operational environment, but as restricted in section 2, those issues are out of the scope of this paper.

Typically, information security policies come on layers [20], and therefore a hierarchy is a logical model of security organization. Anyhow, as the relationships between units are specified based on flows of requirement primitives within the organization, flexibility can be achieved and the model can be applied to different types of organizations. As the hierarchy changes, the requirements of a given organizational unit may originate from a varying amount of different sources, and approaches towards solving potential conflicts of these requirements emerge.

3.2 Specification of requirements

To support automated analysis of requirements as suggested by [13], information security requirements should be exactly formulated. Also other models, such as [5] assume that security requirements can be identified and formulated for analysis. Therefore, it is essential to specify a language for formulation of security objectives into information security requirements. Information security requirements can be roughly classified into three [14]: specific, pervasive and non-technical requirements. Specific requirements are those of the major concern here. They are requirements that can be pointed to any specific computer system or an association within the system. Pervasive and non-technical requirements set, for example, requirements regarding to the trusted implementation of security mechanisms or non-technical issues such as user education. As implementation of security enforcement mechanisms is not within the scope of the management of information security, and as non-technical requirements are not within the scope of this paper, they shall not be further considered herein.

Communications security is usually seen as a specification of secure association within the system [19]. Distributed processes share data over an association, that is an abstraction of a communication channel, and communications security is concerned with the provision of security enforcement for this association. Typically, security is provided by specification of processing rules of data, such as encryption, based on certain possessions of processes, such as keys. Also, criteria can be set for these possessions or processing rules in order to enforce security, for example by determination of key lengths.

A security requirement can den roughly be seen as a set of associations between processes, and security specification of this association based on attributes of processes or the association itself. In addition to the security specification, security requirement should also include specification of accepted content of that association. Different media may, for example, have different clearance and as different types of data have different classification, it may be that not all data can be transmitted over different associations. Therefore, it must be that either the specification includes the restriction of content of an association or the security specification is conditional based on different attributes.

3.3 Specification of criteria to process requirements

The major function the the management of information security is the processing of security requirements in order to harmonize and optimize them, and in order to assure from correctness, consistency

and other properties of the requirement base. To be independent from the notation for specifying requirements, processing should be carried out by different means. Requirement processing should be implemented by specifying criteria that can be implemented as functions that map requirements to modified requirements. The two major types of processing are requirement refining processing and requirement generating processing:

Requirement refining processing is to refine individual requirements in order to optimize them by changing the requirement or by adding detail into incomplete requirement primitives. These criteria are used to harmonize and optimize requirements.

Requirement generating processing is where criteria are used to generate new requirements into the requirement base. This is mostly used to specify dependencies of requirements, and to specify dependent requirements that can then be further processed by other processing rules.

Requirement processing can be used to assure from internal or external properties of a requirement base. Internal properties, such as consistency and optimization, are mostly carried out by requirement refining processing, whereas external properties, such as dependencies and comprehensiveness of requirements, are carried out by requirement generating processing.

3.4 Resolving conflicts of requirements

Information security requirements typically originate from several sources, depending on the organization. Also, different requirements may have different priorities. For example, requirements originating from a national legislation regarding security enforcement should override the organizational requirements. Laws and regulations may set minimum or maximum levels of security for certain security enforcement mechanisms, and no parameter within the organization should violate these requirements. Within organization, the organizational structure may lead one business unit to get requirements from more than one upper layer unit. Therefore, it is essential to develop mechanisms to analyze the security enforcement level of a requirement and to solve potential conflicts in the level enforced by different requirements.

The process consists of two phases. Assume two requirements that are in potential conflict. First is the determination of the security level to be enforced by both requirements. Second phase is the modification of one or both of these requirements to meet the conflict solving strategy. Conflict solving strategy specifies the principles for resolving conflicts by determining acceptable modification of requirements.

For the determination of the security level to be enforced, it is essential to specify security interpretation functions that map requirements into measurable and comparable values, such as security levels. Based on these security levels, a conflict solving strategies may be specified and criteria set to modify one or both of conflicting requirements to be consistent. Three fundamental conflict solving strategies can be identified: lower level wins, higher level wins, or hybrid strategies. Lower level wins -strategy can be used, for example, to meet the requirements set by different laws to restrict applications of cryptography. Each requirement with the restricted security enforcement mechanism is analyzed with a requirement that sets the maximum key length, and if higher key length is identified, it is returned to the maximum length allowed by law.

Maximum level enforcement can be used, for example, in the opposite case. Assume that there is a minimum level of security by encryption, set by key length, that each association must satisfy. This can be set as a basic requirement, and each requirement where an association is protected by that

mechanism is compared to the basic requirement and if shorter keys are found, the attributes specifying the minimum key length are updated to meet the minimum requirement. To provide with flexibility, different hybrid criteria can be based on different logics to set processing principles.

4 Analysis of the approach

If successfully implemented, the framework presented in this paper has application in several areas of information security. The direct applications are in the development of comprehensive information security in organizations, and due to formal approach taken in [13] the requirement processing can be at least partially automated. Further applications are in the comparison of a given organization to a predefined security criteria. Typically, information security has been based on risk analysis [2] but this would enable evaluation of the security of complete information systems, hence improving the level of security management. This might also be of interest of, for example, organizations that are analyzing security of different providers of outsourcing services, or by insurance companies willing to estimate whether the security level of their client is acceptable for insurance purposes.

There are, though, several critical success factors for the framework that need to be considered before extensive applications. First is flexibility. Typically, organizations vary from structure and from the nature of information security requirements. Therefore, it is essential the organizational security models based on this framework can reach the adequate flexibility to meet different needs. The formulation of requirement harmonization [13] sets only minimum restrictions for the organizational structure, and later research suggests that requirements and requirement processing criteria can be set to be flexible enough to meet needs of different organizations.

Another essential success factor is the feasibility of the model. As any formal approach, this framework also restricts the scope of setting and processing information security requirements. As analyzed earlier, the focus is mostly on specific requirements and different tools are needed for analysis of pervasive and non-technical requirements. Such requirements can be set as attributes of processes and hence included in the framework, but automated analysis of their properties may not be easily applicable. As these requirements are supporting requirements for specific security requirements, it is believed that this restriction is not too strong for the application for the model.

Third success factor is the development of top-down tools to support application of the framework. Development of information security is typically a top-down process, and not fully carried out by information security specialists, but communication among different peer groups is needed. Therefore, success application of the framework presented here need supporting graphical top-down tools. Similarly than in system engineering, there is a need to tools that can be used and understood by different technical and non-technical personnel groups, and that support the framework presented herein. Also, it is essential to identify the parts that can be automated, and develop tools that support automated analysis of requirements. As the process-association -model suggests, traditional structured, data-flow based system development tools might be applicable also in the development of secure systems. Further, recent trends suggest that Object oriented modeling tools are taking over structured analysis tools, and should also be considered in the security context.

5 Conclusions and areas for further research

A framework has been proposed for the development of comprehensive information security in organizations, that is to support management of information security. The focus has been on the formulation

and processing of information security requirements, based on high level security objectives, in order to reduce abstraction, improve cost-efficiency, consistency and other properties of the requirement base, and in order to solve conflicts of different requirements. This framework consists of several major areas that each need to be considered. The success of the approach is based on the several issues analyzed within this paper.

The paper also identifies several areas for further research. Each component analyzed can be analyzed in detail, and preliminary solutions provided can be further developed and interfaces between different components can be analyzed in detail. Management of information security as a whole is a large subject, and models such as [10] suggest a very wide point of view, where the areas of research expand widely also to non-traditional areas of research in computer science. Therefore, it has been an intentional choice within this paper to restrict on issues that have direct relationship to the specification of meta policies that coordinate actual technical security policies. From the layered security policy model [20] point of view, this means that focus is on administrative security policies, and in their relationships to upper and lower layer policies.

Of course, the nature of different levels of security policies is a controversial issue. It is clear that the security policy objective is of very informal nature, and technical security policies are formal in order to automate their enforcement, and to enable analysis of security. The major contribution of this paper has been identification of components that have a major impact on the formulation of security requirements to satisfy security policy objectives, and to identify components needed in the automated analysis of security at organizational level.

References

[1] Trusted computer systems evaluation criteria. U.S. Department of Defence, 1983.

[2] J. Backhouse and G. Dhillon. Structures of responsibility and security of information systems. *European Journal of Information Systems*, 5:2–9, 1996.

[3] D. E. Bell and L. J. LaPadula. Secure computer systems: Mathematical foundations and model. Technical Report M74-244, MITRE Corporation, Bedford, MA,USA, 1975.

[4] K. Biba. Integrity considerations for secure computer systems. Technical Report TR-3153, MITRE Corporation, Bedford, Massachusetts, USA, 1977.

[5] H. Booysen and J. Eloff. A methodology for the development of secure application systems. In *Proceedings of the IFIP TC11 11th International Conference on Information Security*, 1995.

[6] D. D. Clark and D. R. Wilson. A comparison of commercial and military security policies. In *1987 IEEE Symposium on Security and Privacy*, 1987.

[7] W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT–22(6):644–654, Nov 1976.

[8] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[9] Federal Information Processing Standards Publications (FIPS PUB) 46. *Data Encryption Standard.* National Bureau of Standards, Jan 1977.

[10] A. Hartmann. Comprehensive information technology security: A new approach to respond ethical and social issues surrounding information security in the 21st century. In *Proceedings of the IFIP TC11 11th international conference of Information Security*, Cape Town, South Africa, May 1995.

[11] L. J. LaPadula. Foreword for republishing of the Bell-LaPadula model. *Journal of Computer Security*, 4:233–238, 1996.

[12] J. Leiwo and S. Heikkuri. Clarifying concepts of information security management. In *Proceedings of the 2nd International Baltic Workshop on DB and IS*, Tallinn, Estonia, June 12-14 1996.

[13] J. Leiwo and Y. Zheng. A formal model to aid in documenting and harmonization of information security requirements. In *Proceedings of the IFIP TC11 13th International Conference on Information Systems Security*, 1997.

[14] S. Muftic, A. Patel, P. Sanders, R. Colon, J. Heijnsdijk, and U. Pulkkinen. *Security Architecture for Open Distributed Systems.* John Wiley & Sons, 1994.

[15] R. L. Rivest, A. Shamir, and L. M. Adleman. A Method for Obtaining Digital Signatures and Public–Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, Feb 1978.

[16] R. S. Sandhu. Lattice-based access control models. *IEEE Computer*, pages 9–19, November 1993.

[17] R. S. Sandhu, E. J. Coyne, H. J. Feinstein, and C. E. Youman. Role-based access control models. *IEEE Computer*, 29(2):38–47, February 1996.

[18] B. Schneier. *Applied Cryptography.* John Wiley & Sons, New York, second edition, 1996.

[19] W. Stallings. *Network and Internetwork Security: Principles and Practise.* Prentice Hall, Inc., Englewood Cliffs, NJ, USA, 1995.

[20] D. F. Sterne. On the buzzword Security Policy. In *IEEE Symposium on Security and Privacy*, 1991.

[21] J. G. Williams and M. D. Abrams. Formal methods and models. In M. D. Abrams, S. Jajodia, and H. J. Podell, editors, *Information Security - An Integrated Collection of Essays.* IEEE Computer Society Press, Los Alamitos, CA, USA, 1995.

[22] T. Y. Woo and S. S. Lam. Authorization in distributed systems: A formal approach. In *Proceedings of 1992 IEEE Symposium on Research in Security and Privacy*, 1992.

[23] Y. Zheng. Digital signcryption or how to achieve cost(signature & encryption) $\leq$ cost (signature) + cost(encryption). In *Advances in Cryptology – Crypto'97*, number 12xx in Lecture Notes in Computer Science. Springer-Verlag, 1997.

[24] Y. Zheng. The SPEED cipher. In *Proceedings of the Financial Cryptography'97*, 1997.