Four Approaches to Construction of Information Security Guidelines

Mikko T. Siponen
Mikko.T.Siponen@oulu.fi
University of Oulu, Department of Information Processing
Science, Linnanmaa, FIN-90401 Oulu, FINLAND.

Abstract

The field of information security encompasses various models and policies developed with different objectives lacking cohesion from the security management facet. This paper identifies a group of problems within these policies, including the challenges in applying these policies to the end-user. As a solution, four possible approaches, termed as conservative, liberal, prima facie and superegorative, to the construct information of security guidelines shall be outlined here, including the strengths and weaknesses of these approaches.

Keywords: Information security policy, end-user security, end-user guidelines

BRT Keywords: EK, EL, GA03

Introduction

Various information security policies and models have been introduced in order to satisfy very different information security requirements. A common feature of these security policies is the fact that their scope and nature of vary in many senses. For example, the scope can vary from having one particular security requirement (e.g. secrecy/confidentiality) to having many requirements, and as to whether these security policies can be expressed by formal or non-formal notation. One weakness that is a consequence of the unique objectives of security policies is their possible non-cohesive relation to each other. In the end, this weakness particularly affects the management facet of an organisation, and some attempts have been made to improve these weaknesses to some extent, e.g. Leiwo and Zheng (1997).

To understand this problem area which, unfortunately, has not been dealt with as of yet, the security policies are divided into two kinds as follows. Firstly, a lot of effort has been made in the area of "technical policies" (or security models), e.g. the terminology developed by Sterne (1991). However, interest in the second kind, non-technical policies has been unsubstantial. Different models and policies for access controls, for instance, are case in point in respect to the technical policies. Yet the issue of what principles and integration criteria should be followed in the case of non-technical policies is a matter of the latter category. The range of issues belonging to this second kind of policies is so broad, that we will not discuss them in this paper.

The issue of information security policies also concerns various end-users in an organisation. There are guidelines established for end-user computing and these fall into the category of non-technical policies according to the division made above. Although

this matter is indeed of crucial relevance in the consideration of security as a whole on any organisational level, e.g. Hale (1996), the end-user matters with respect to security polices have not received similar concern by researchers as other policy issues[1]. In this regard, only the omittance of guidelines has been often reported and some examples of good end-user guidelines or adequate criteria for different actions, such as passwords, have been presented by Conorich (1996) and Poore (1996).

Such guidelines, or chosen approaches to 'good guidelines,' may be good in a technical sense[2]. However, they are not modelled (to use the analogy with respect to technical policies/models) or discussed in enough detail to be considered adequate with respect to security policies, thus avoiding conflicts or inconsistencies within the guidelines[3]. Without this latter type of consideration there can be, for instance, conflicts within the guidelines themselves. In other words, two different rules of a guideline may conflict, i.e. in certain special circumstances the keeping of one rule within an information security guideline may violate another rule in those same guidelines. Alternatively, there is the case of guidelines to which conforming in a special circumstance would yield negative results with respect to security. Thus, in this latter case, in addition to the possibility that the result may be negative, there might also be a conflicting situation of another kind. For example, a literal following of the security guideline may be in conflict with higher level security polices, say, organisational information security policy.

The research questions of this paper include the following:

- Can there be a repertory of principles to organise end-user information security guidelines?
- What are the strengths and weaknesses of such principles?

Conceptual analysis is used as the primary research method to obtain results.

This paper is organised as follows. In the second section, the hierarchy of security policies is outlined. It should be noted that the second chapter might not add much to what has been contributed already. However, since the terms ‘information security policies’ and ‘models’ are used in rather indefinite manners by different authors, it is important to clarify the issue and particularly its relationship to the end-user guidelines that are considered under the next section. In section three, approaches for construction of security guidelines are discussed. The fourth section summarises the key issues of this paper.

2. Information security policies

It is may be sufficient, for the purpose of this paper, to explain that the information security policies presented here are aimed at fulfilling the requirements of confidentiality, availability and integrity of information. The universe of discourse of information security policies with respect to the management facet can be seen with the help of the following classification (Fig.1).

---

[1] Such as technical security policies or security models.

[2] Meaning that the adequacy criteria concerning passwords, for example, may be technically valid, i.e. has been proven to be such and it is difficult to break certain passwords, for instance.

[3] e.g. Abrams & Moffett, 1995 see that security managers need to interpret formal/informal policies to avoid conflicts. As mentioned, such activities are not considered from the point of view of security guidelines.

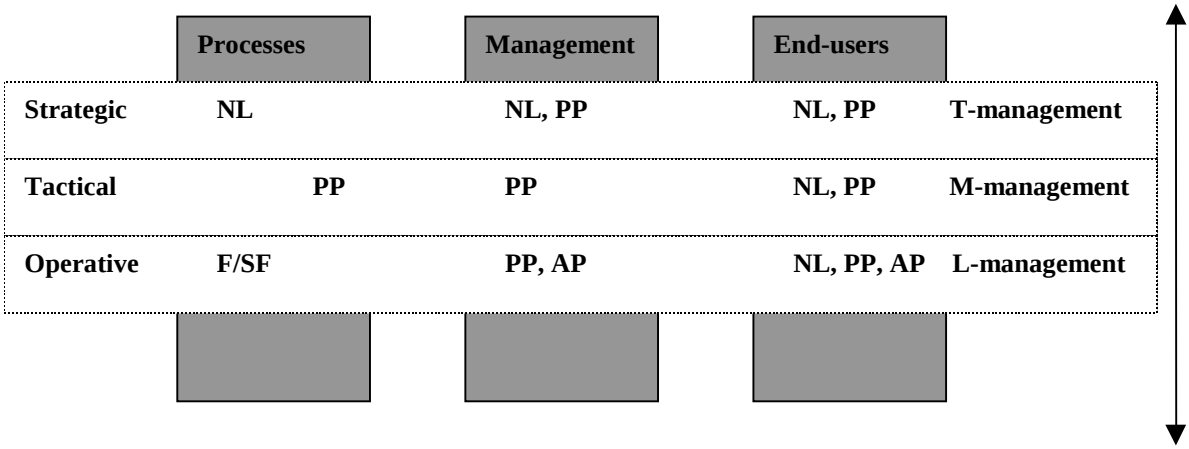

Figure 1. The universe of discourse of security policies according to the management facet.

The figure shown above has been modified from Abrams & Bailey (1995) to include different stages (strategic, tactical and operative) of management and the notation which is likely to be used in different levels or sections. NL denotes natural language, F stands for formal and SF is semi-formal. 'T-management' denotes the highest management, clarification of which depends on the chosen point of view. For example, T-management could be the president, security or information security manager of the organisation in question. M-management is the middle management and L-management is the lower level of management. AP stands for active policy and PP for passive policy, these terms where introduced by Abrams & Moffet (1995). In the case of active policy, the people concerned must be active (e.g. "Administrator of X domain is required to monitor that the password of each user is longer than 8 characters…"). Whereas in the case of passive policy, the people in question may not to be active in a similar sense (e.g. "The administrator is only allowed to…").

The objective of security models is to formulate or model how to achieve the protection enforced by a (technical security) policy. Policies (whatever security or other) are one type of standing plans while another include procedures (a set of related steps under recurring circumstances), rules expressing an action that should or should not be taken (Bartol & Martin, 1994) and/or principles. Security policies are generally seen to be mandatory by their nature (Wood, 1995). Those who views policies in this way are likely to be share the view that policies also have normative and prescriptive dimensions while security models, in turn, are descriptive i.e. non-prescriptive by their nature. In other words, an aim of the security model is to demonstrate (prescriptive) policies, i.e. they descriptively show the certain security requirements that are most likely wanted to be prescriptive[4].

The universe of discourse of security policies shall be considered next. The following scheme (Fig.2) indicates the relationships of various information security policies, to security policies and further their relation to information security guidelines.

As mentioned earlier, one problem related to different security policies was their non-cohesive relationship to each other. The need for policies to be cohesive can be

[4] The division between descriptive and prescriptive was first introduced by R.M. Hare (1952), further modified and used in the field of information security by the author (Siponen & Kajava, 1998), arguing that issues covered within information security guidelines should be regarded as prescriptive statements (i.e. statement including a kind of personal commitment towards the issues outlined by the guidelines) by end-user, not descriptive statements (i.e. statements that not include any kind of commitment towards security guidelines) by end-users.

illustrated with the help of the transitive relation following. The Relation R is transitive in set A = {Security Requirements, Organizational Security Policy, Information Security Requirements, Organizational Information Security Policy, Information Security Sub-Policies}; if SR, OSP, ISR, OISP, ISSP ∈ A. Relation (r for short) is transitive if SRrOSP and OSPrISR ⇒SRrISR. An epithet of transitive relation can be described by stating that:
OSP = SP + d2x
ISR = OSP +d3x, where d = df detailed attributive information of certain security requirements.

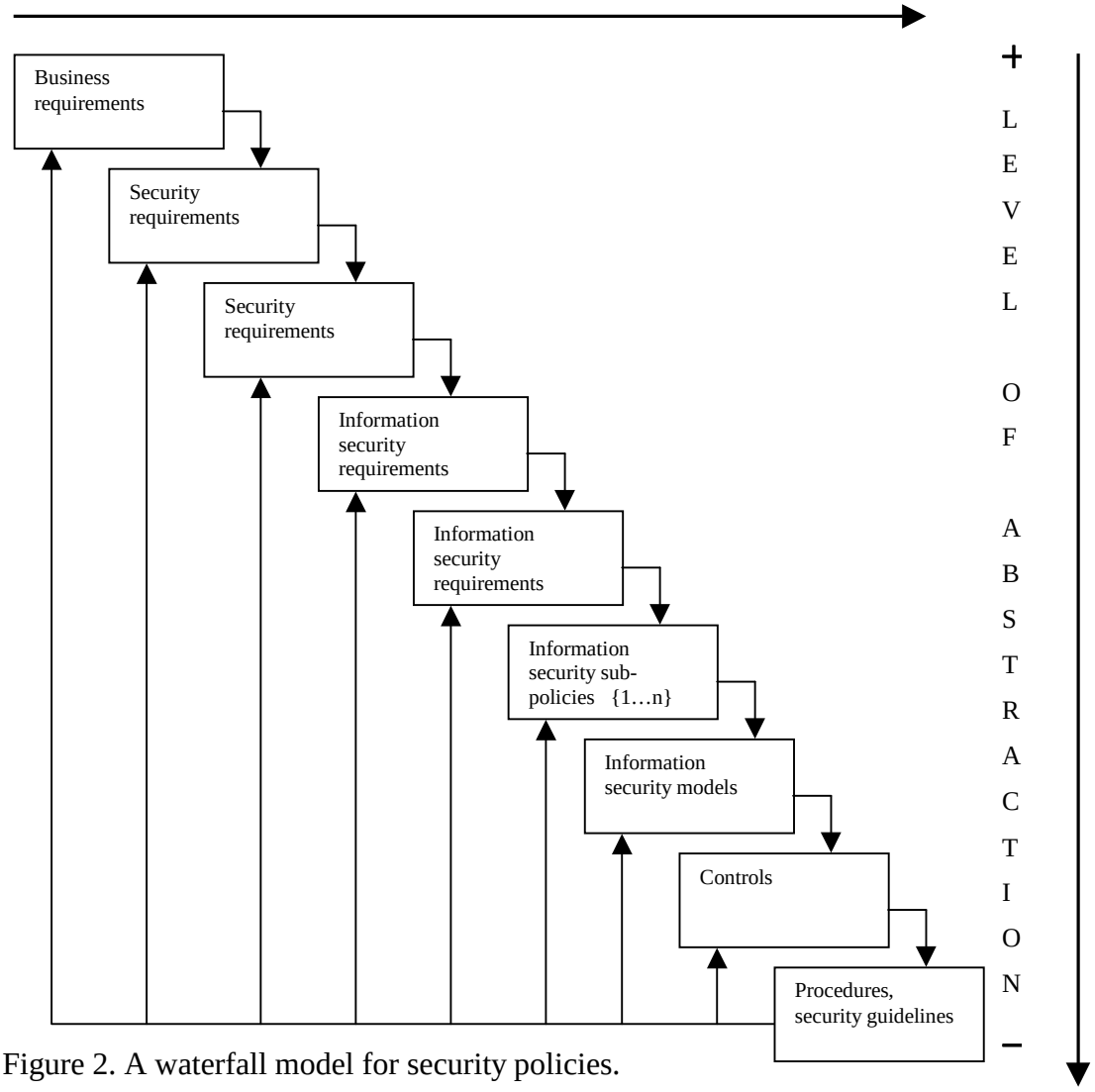

Figure 2. A waterfall model for security policies.

According to the schema outlined above, security politics are cohesive only if they satisfy the conditions SP<OSP and OSP<ISR ⇒ SP < OSP ∀ SP, OSP, ISR ∈ A. The relation outlined above seems to have certain affiliations with the supervenience relation, as a universe of security policies can perhaps be described as a set of pairs of upper level and lower level policies, where there is a supervenience relation between each pair. Thus a local/weak (and a kind of logical) supervenience relation between sets of security properties (or requirements) can be seen in a sense that upper lever policy supersedes lower lever policy. The outlined schema favours a top down approach in the sense that there cannot be such modifications on a lower level that are not supported by a higher level (policy). This does not logically prevent a bottom up approach, but the top down approach is advocated herein due to rational reasons (the detailed discussion of

which is beyond the scope of this paper), namely security and security policies are easier to develop in a top down manner. For example, it may be better to develop an upper level part before its lower level counterpart as modification of a lower level procedure may cause changes in the upper level, all the way to the organisational security policies. It should be noted that this does not obstruct ongoing iterative development in terms of security (policies), but rather such a development, if adopted, should be executed in a top down manner.

3. Four principles behind end-user guidelines

Different end-users form an important component from the security point of view simply because many uses or abuses of a system (in terms of security) directly or indirectly involve end-users. Regarding the end-user facet, security guidelines are an object of discussion with respect to security policies. In this respect, security guidelines simply reflect security requirements captured by security policies as they enforce (in certain ways that will be considered later) end-users compliance to the security policy of the organisation in question. Security guidelines are mainly expressed by a natural language, as they need to be easily understandable for any end-user.

As mentioned earlier, the political issue of how to approach (or what principle should be used to approach) security guidelines generally, or especially in cases where rules of a guideline may be not applicable (or may not give the best possible results), shall be tackled next. Principles behind end-user guidelines, in the mentioned respect, can be divided, for example into conservative, liberal, prima-facie and superegorative. These approaches will be discussed next.

The first is a standard approach often seen in the military environment stating that what are not allowed by information security guidelines is strictly denied irrespective of the situation in question or consequences it may raise, in other words and order is an order, to be followed no matter what.

The second is called a liberal approach. According to this, those actions (in terms of security) which are not prohibited are acceptable, per se. Security guidelines are to be followed literally, but if the user is faced with an issue that is not addressed by the guidelines, it follows that some appropriate action to deal with the situation is acceptable. The liberal approach is not likely to be favoured by any (information) security policies, but it may be an approach in which people may be easily caught up (especially if control concerning those guidelines is loose). This is the attitude one often finds toward the law; if something is not expressly forbidden, it is allowed.

The third form shall be called as prima-facie approach, and is modified from Ross (1930) (his use of prima facie is in the area of moral philosophy). According to this view, the requirements of security guidelines should be met generally. Yet they can be formally violated inasmuch as 1) the situation involves two or more conflicting requirements; or 2) the benefits of compromising those guidelines (excluding a person's egoistic benefits) clearly outweigh the benefits of complying with the security guidelines.

The final approach is superegorative by its nature. In this case, the guidelines are interpreted as a) descriptive or b) prescriptive. However, in the sense that prescriptivity is not a logical demand, rather the guidelines prescribe an ideal or a virtuous state-of-affair that is good or courteous for the end-user to follow. This approach differs from the others, as the actions against codes are not ultimately bad, required nor punishable. It is therefore a similar approach to that often used in superegoration of virtue ethics in the

area of moral philosophy.

The analysis of strengths and weaknesses concerning these approaches of security guidelines shall be presented. The conservative approach, albeit it is commonly enamoured by the security community, is impractical, at least in the sense that is rigid, inflexible (more than the other approaches) and therefore mostly likely to be inapt in a dynamic environment. To be more precise, the more dynamic the environment and changing the workers assignments are, the more inadequate the conservative viewpoint is likely to be. For example, in the case of dynamic environment, it is very difficult to formulate all-inclusive guidelines, with the result that there might be situations in which certain actions not covered by guidelines are desirable, whether in terms of the mission statement or security. This kind of hard-and-fast approach, as the conservative one is likely to be, might also be invidious as it may neglect the motivational aspects that are recognised as an important part of the human side of security e.g. (Saltzer & Schroeder, 1975[5]; Parker, 1997; Spruit, 1998). To be more precise in this regard, observing the difference between intrinsic and extrinsic motivation, it is rather easy to draw the conclusion that the conservative approach may not promote intrinsic motivation. This approach, at a first sight, does not leave much room for one's self-determination which is the ultimate reason for whether one, the end-user in this case, is intrinsically motivated or not[6].

Consequently, it is likely to be more negative in this respect than other the approaches, as the requirements posed by intrinsic motivation is most difficult to entertain. However, the conservative approach may be suitable for a military (type of) environment, given that an environment of that type satisfies one or both of the following conditions: I) the business environment is not dynamic; II) employees are accustomed to strict instructions. The second aspect can be met provided that the end-users in question regard the orders (or the idea and rules outlined by conservative approach) as intrinsically right, i.e. they share the view expressed by conservative guidelines (therefore it may satisfy the requirement posed by intrinsic motivation, i.e. self-determination).

The strength of the liberal approach depends on the preference of end-users, as it is likely to be more satisfactory in the eyes of end-users than the conservative approach. Consider for instance, the aforementioned motivational demands, which the liberal approach is more likely to meet than the conservative approach. The liberal approach meets the requirements of intrinsic motivation (i.e. one's self-determination) better. The weakness of this approach relates to its nature, as it easily leads to a state of insecurity. This is almost unavoidable, as it is very difficult to compose such a set of guidelines that would cover all the relevant issues in terms of information security. And, as the principle of liberal approach suggests, if the issues not required by guidelines are not take into account in any respect, they are acceptable, which may lead to potential risks from the security perspective.

The strength of the prima facie approach lies in its possibility to cover security concerns in a flexible manner. It is more flexible than conservative and it may lead to better situation in terms of security or business, particularly in unordinary situations that are not covered by (conservative/liberal based) security guidelines. Its weaknesses include, in comparison to the conservative approach, that it may better meet the

---

[5] Saltzer, & Schroeder (1975) first suggested that psychological acceptability should be taken as one principle of building secure systems.

[6] For instance, according to Deci (1975) self-determination is the primary factor that influences whether one is intrinsically motivated or not. Some approaches of how to achieve intrinsic motivation are discussed by the author (Siponen & Kajava, 1998).

preferences of end-users (consider the outlined motivational issues). The weakness of mentioned approach from the security viewpoint relates to exception rules, i.e. what determines or justifies the actions against guidelines or actions not covered by information security guidelines. The second condition was designed to help us in this respect (and for these reasons just mentioned, although it is logically possible, at least in some respect, to formulate it by other constraints, this constrain was favoured). This condition as currently presented, however, still leaves a possibility for the insecure[7] actions done in the light of prima facie approach. For example, the sub-principle of "benefits of compromising those guidelines (excluding a person's egoistic benefits) clearly outweighs the benefits of complying with the security guidelines" contains the weakness that, in the case of conflicting rules within the guideline, it puts the judgements on users and leaves room for subjective interpretations, as it may not be unequivocal what are "benefits", for instance.

The strengths and weaknesses of the superegorative approach are similar to those of the liberal approach, except that the superegorative approach may promote more positive attitudes towards security guidelines than liberal approach since it accentuates the virtue of observance of information security guidelines. However, neither sanctions related to the disobeying of security guidelines for purposes of deterrence nor preventive countermeasures (e.g. see Straub & Welke, 1998) can be installed if the superegorative approach is applied. Although, such sanctions are traditionally associated with security activities, and their absence is likely to be viewed as a weakness, the relevance of these sanctions is not self-evident[8]. However, the issue of whether they are relevant as a countermeasure or not, including different possible implications their use may raise, is out of the scope of this paper.

4. Conclusions and the future work

The role of information security polices with respect to end-user computing in the organisation level was considered focusing on an approaches behind security guidelines. Four possible approaches were analysed. From those, the approach referred to as conservative is perhaps the most often used. This is true despite the fact that it is rather unsuitable for modern companies, mainly due to its inflexible nature, as it advocates that all permitted actions are explicitly described in the guidelines. Its weakness involves situations where certain circumstances would require action that is not covered by security guidelines and therefore such an action can not be executed, no matter what positive results it may produce.

Both the weakness and strength of the liberal approach rests on the freedom that it allows the user. This approach, albeit favoured by users due to such liberality, is problematic from the security perspective as it easily leads to insecure states.

The prima-facie approach was outlined with two principles, and was argued to be flexible especially in dynamic environments. The weakness of this approach is its abstractness. In theory it leaves so much room for personal interpretation that it may lead to an insecure state.

The superegorative approach was also introduced. It states that the obeying of

---

[7] The criteria of what is insecure or secure state is, here, depends on (information) security polices in question, i.e. what the information security policy, for example, regards to be insecure or secure situation.

[8] Their usability has raised antithetical views as, for example, Denning (1990) sees that their relevance is clear, while some other scholar argues that their relevance is questionable.

information security guidelines is not compulsory. Users are encouraged to act virtuously and conform to the information security guidelines.

The agenda for future work includes the organisation of empirical studies in order to understand the strength and weaknesses of different approaches presented herein. One future research question in this respect includes how the motivation of employees correlates with the different approaches presented.

References

Abrams, M.D. & Bailey, D., (1995), Abstraction and Refinement of Layered Security Policy. In: Information Security - An integrated Collection of Essays. Edited by M. D. Abrams, S. Jajodia & H. J. Podell, IEEE Computer Society Press, Los Alamitos, California, USA.

Abrams, M.D. & Moffett, J.T., (1995), A higher level of computer security through active policies. Computer & Security, Vol. 14, No. 2, p. 147-157.

Conorich, D. G., (1996), UNIX Passwords. Information Systems Security. Vol. 7., No. 1.

Deci, E.L., (1975), Intrinsic Motivation. Plenum Press. New York. USA

Denning, D., (1990), Concerning hackers who break into computer systems. Proceedigs of 13th National Computer Security Conference.

Hale, R., (1996), End-User Computing Security Guidelines. Information System Security. Vol. 6, No. 1.

Hare, R.M., (1952), The Language of Morals. Oxford University Press. Oxford, UK.

Leiwo, J. & Zheng, Y, (1997), A Framework for the Management of Information Security. Proceedings of the 1997 Information Security Workshop (ISW'97). Ishikawa, Japan, September. Springer-Verlag, LNCS 1396.

Parker, D. B., (1997), Information Security in a Nutshell. Information System Security. Vol. 6, No. 1.

Poore, R. S., (1996), The Lowly Password. Information Systems Security. Vol. 7., No. 1.

Ross, W. D., (1930), The right and the good. Oxford University Press. Oxford, UK.

Saltzer, J.H. & Schroeder, M.D., (1975), The Protection of Information in Computer Systems. Proceedings of the IEEE, vol. 63, no. 1, Sept.

Siponen, M. T & Kajava, J., (1998); Ontology of Organizational IT Security Awareness. From Theoretical Foundations to Practical Framework. Third International Workshop on Enterprise Security. A part of the IEEE 7th International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WET ICE '98), Stanford, California, USA, 17-19 June 1998, California, USA. IEEE Computer Society Press. Los Alamitos

Spruit, M.E.M, (1998), Competing against human failing. 15th IFIP World Computer Congress. 'The Global Information Society on the Way to the Next Millennium'. SEC, TC11. Vienna.

Sterne, D. F., (1991), On the buzzword 'security policy'. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, pp. 219-230. IEEE Society press, Los Alamitos, California, USA.

Straub, D.W. & Welke, R.J., (1998), Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly, Vol. 22, No. 4, p. 441-464

Wood, C.C., (1995), Writing InfoSec Policies. Computer & Security, Vol. 14, No. 8, p. 667-674.