

Four views on security

Teemupekka Virtanen



TEKNILLINEN KORKEAKOULU
TEKNISKA HÖGSKOLAN
HELSINKI UNIVERSITY OF TECHNOLOGY

TML-A1	Håkan Mitts Architectures for wireless ATM
TML-A2	Pekka Nikander Authorization in agent systems: Theory and practice
TML-A3	Lauri Savioja Modeling techniques for virtual acoustics

ISBN 951-22-6160-X
ISSN 1456-7911

Four views on security

Teemupekka Virtanen

Dissertation for the degree of Doctor of Technology to be presented with due permission for public examination and debate in Auditorium T2 at Helsinki University of Technology (Espoo, Finland) on Friday, 25th of October 2002, at 12 o'clock noon.

Helsinki University of Technology
Department of Computer Science and Engineering
Telecommunications Software and Multimedia Laboratory

Teknillinen korkeakoulu
Tietotekniikan osasto
Tietoliikenneohjelmistojen ja multimedian laboratorio

Distribution:

Helsinki University of Technology

Telecommunications Software and Multimedia Laboratory

P.O.Box 5400

FIN-02015 HUT

Tel. +358-9-451 2870

Fax. +358-9-451 5014

©Teemupekka Virtanen

ISBN 951-22-6160-X

ISSN 1456-7911

Otamedia Oy

Espoo 2002

ABSTRACT

Security is a term with many meanings and connotations. In this thesis several views to security are presented. These views are presented on a general level with some topics, which are typical for each view.

There are some conclusions, which should be highlighted from these views: besides a mathematical risk analysis security is also a feeling. People are not able to just calculate and be analytical in these issues. It is often a matter of trust, trust in the psychological sense, not technical. This trust is essential for commercial organizations, too, since people do not use their products or services without some level of trust.

Another important issue: capability. People do not behave in a secure way if they do not know how. Education must include, besides the problem solving methods, attitude and environment issues, too. A self-taught person who can solve the problem but does not understand the environment causes often more difficulties to the organization than a less creative employee. At the same time capability is also a good way to increase trust. A well trained user makes less mistakes, which increases trust.

Security is a supporting function. Each organization has a main function and security supports it. Security prevents losses caused by accidents and intruders. The relationship between security and quality is very close but while quality concentrates on the process itself, security guards the process against outsiders. Quality looks inside, security looks outside.

A division between information security and general or corporate security is not valid. Information is one type of asset and, despite of some special characteristics of information, it is protected using the same methods as the other assets of the organization.

KEYWORDS: security, corporate security, information security, trust, risk management

Life is a chaotic process. Basically, everyday existence is not consequence-free but one choice leads to another. In my life there certainly have been some key decisions which have changed the direction of my future. When I started my studies at Helsinki University of Technology I had no plan to concentrate on computers. I just found some "bad" company and my future career got a new direction. In the beginning of my postgraduate studies I decided to select psychology as my minor, targetting usability issues. That was a good choice. I have never really worked as a usability engineer but my minor gave me a solid background on users. Then, another quick career change: The Prime Minister's Office needed an information security officer and I decided to apply. I was selected without any formal credentials in the security area, and working as a young specialist among the gray eminences of the Finnish security business was a very valuable experience. Finally, after ten years and several employments within the Finnish security area, I returned to the university.

Without my returning to academia, this thesis would probably not have been published. However, my experiences in other organizations is as valuable as my time at the university. Without those experiences this thesis would not have been published, either.

Writing a thesis like this has several layers.

In the core is the thesis itself. At the final stages before publication, the life of the candidate is spinning around the thesis. I want to thank my opponent, prof. Louise Yngström and pre-examiners, prof. Matthew Warren and docent Mikko Valkonen, for their valuable comments on this thesis. My custos and predecessor, docent Arto Karila, has also supported me in many ways over the years and we have had long discussions about the topics in this thesis. There are several other colleagues and professional friends, too, who have commented on my work. Especially I want to thank Ronja Addams-Moring against whom I have had to defend my ideas several times, which has helped me to clarify my thoughts a lot. Unfortunately, she was not available when I published my first papers and one can see the difference. Minna Kangasluoma and Ari Mujunen have also given me some valuable comments.

The next layer: Working in various organizations has been the starting point of many ideas presented in this thesis. Discussing with colleagues has been a part of the process of developing these ideas. I especially want to mention Kalevi Tiihonen, Mikko Valkonen, Jyrki Ahvonen, Jaakko Häyhtiö, Ari Uutinen and Jukka Sonninen who, among several other people, have argued with me, supported and encouraged me during my career.

Last but definitely not least, there seems to be life even outside the thesis and professional career layers. The people in my personal life are precious and without their support there would be no life in the inner layers, either. I thank my parents, all my friends and especially my most beloved one, Merja, who survived the life of a candidate before me.

CONTENTS

Abstract	i
Preface	iii
Contents	v
List of Figures	vii
List of Tables	ix
Publications	xi
1 Introduction	1
1.1 About security	1
1.2 About the thesis	5
Background	5
Organization of the thesis	5
2 User's view	7
2.1 Social behavior	7
2.2 Trust	7
2.3 An ambassador in the electronic world	8
2.4 Privacy	10
2.5 Education	11
3 Developer's view	13
3.1 Security as a requirement	13
The security profile of a product	13
Usability	14
3.2 Security in the development cycle	15
3.3 Secure development process	17
4 Organization's view	21
4.1 Organizing security	21
4.2 Organizational security	21
4.3 Conflicts between security needs	22
4.4 Security culture and evolution	26
5 Scientist's view	29
5.1 Track comparison	30
5.2 Contents of the conferences	30
5.3 Comments about scientific areas	31
6 Other relevant views	33
6.1 Physical and information technology security	33
6.2 Security and quality	34

6.3	Security in a space	36
7	Security models	39
7.1	Information security vs. corporate security	39
	The governmental information security policy in Finland	39
	The corporate security model of Finnish employers	39
7.2	Comparing the models	39
7.3	A combined model	40
	Assets	40
	Mandatory protection methods	42
	Selectable protection methods	42
	The usage of the model	42
8	A method for classifying and analyzing systems	45
8.1	Classification	45
8.2	Analysis	46
8.3	A proposed classification and analyzing system	47
8.4	The cost model	51
8.5	Comments on the method	52
9	Conclusions	53
9.1	Summary	53
9.2	The results	53
9.3	Future work	54
	Bibliography	55

LIST OF FIGURES

1.1	The number of reported incidents to CERT [11]	2
1.2	The status of different protection methods in Finland [49, p.24]	4
3.1	Taxonomy of usability [72, p.25]	15
3.2	Usability and development cycle (qualitative only)	16
3.3	Requirements and learning ability (qualitative only)	16
6.1	Quality and cost [86, p.5]	34
6.2	Security and cost	35
6.3	Security and quality by Herrmann [45, p.29]	35
7.1	The 4 sector model	41
8.1	“Bathtub” model of reliability [66, p.174]	46
8.2	Top-down classification	48
8.3	Availability flow chart	49
8.4	Confidentiality flow chart	49
8.5	Threat analysis	50
8.6	The cost model	51

LIST OF TABLES

1.1	The FUNNET-CERT statistic [80]	2
3.1	Boehm's risk model [25]	18
3.2	Risk taxonomy [95]	19
4.1	Definitions of different types of Internet abuses [92]	23
5.1	Content according the to 8 sectors model (% of papers) . . .	30
5.2	Content according to the 4 sectors model (% of papers) . . .	31
8.1	Comparison of hardware and software reliability [57, p.7][108, p.4]	47

1. T. Virtanen, “A Study of Human Aspects of Information Security”, proc. of world conf. on information security education, Edith Cowan University, pages 261—272, ISBN 0-7298-0498-4, Australia, 2001.
2. T. Virtanen, “An Information Security Education Program in Finland”, proc. of world conf. on information security education, Edith Cowan University, pages 91—100, ISBN 0-7298-0498-4, Australia, 2001.
3. T. Virtanen, “Security Education in Finland”, proc. of Australian security research symposium, Edith Cowan University, pages 171—178, ISBN 0-7298-0497-6, Australia, 2001.
4. T. Virtanen, “The Security Model to Combine the Corporate and Information Security”, proc. of IFIP TC11 int. conf. of information security, Kluwer Academic Publishers, pages 305—316, ISBN 0-7923-7389-8, USA, 2001.
5. T. Virtanen, “Design Criteria to Classified Information Systems Numerically”, proc. of IFIP TC11 int. conf. of information security, Kluwer Academic Publishers, pages 317—325, ISBN 0-7923-7389-8, USA, 2001.
6. T. Virtanen, Ronja Addams-Moring, “An Information Security Curriculum in Finland”, proc. of IFIP TC11 int. conf. of information security, Kluwer Academic Publishers, pages 183—190, ISBN 1-4020-7030-6, USA, 2002.

This chapter is an introduction to the thesis. There is a section about security and some background information about the writer and about the structure of this thesis.

1.1 About security

Security has many viewpoints. In this thesis we describe security from several different points of view. These views have both common and unique elements and in some cases there are also clear conflicts between them. In this thesis we look around and collect several views into one picture. The focus is to introduce the views and some of the typical aspects of them. We will notice that there are common elements in these areas and thus also influence between them.

Security is emotions. From an individual's point of view it is always a subjective term. It depends on facts but also on feelings. Are these feelings important? Yes, because people are not driven by facts alone but also by feelings.[40]

The probability to get injured is much lower in an airplane than in a car, yet many people are scared of flying. A major accident with lots of casualties causes fear even if its probability is very low [40]. In the USA every month almost the same number of people die in car accidents as in the single terrorist attack on 11.9.2001 [99].

Security is a profile. It is part of each product and service. When somebody is designing something new the security feelings have to be taken into account or people probably will not buy the product or use the service. Security is one possibility for a company to differentiate itself from other companies, too. A high security product targets an other customer segment than a low security one.

Security is cost. Finnsecurity is the organization of Finnish people and companies in the security business. According to its survey in the year 2000 Finnish companies used as much money for security as heating or electricity (per an employee). [10] Computer Emergency Response Team (CERT) has published statistics about the number of security incidents and vulnerabilities. As we can see in figure 1.1 the number of reported incidents has grown dramatically. The year 2002 is an estimate based on the results of Q1. [11] In Finland there has been CERT only in the university network (FUNET) until year 2002. In Table 1.1 are some statistics of reported incidents from FUNET-CERT [80].

Security is optimization. Security incidents cause loss of assets: valuables, work and reputation. Security measures prevent those incidents, make the losses smaller and help to continue the main activity after the incident. However, security measures cost money and work. If security is more expensive than the incidents it is not efficient. Often the cost of

Type	2000	2001
Abusive communication	3	2
Denial of service	16	18
Probe	16	49
Root compromise	3	5
Unauthorised use	7	8
Virus	6	70
Warez	1	2
Total	52	155

Table 1.1: The FUNNET-CERT statistic [80]

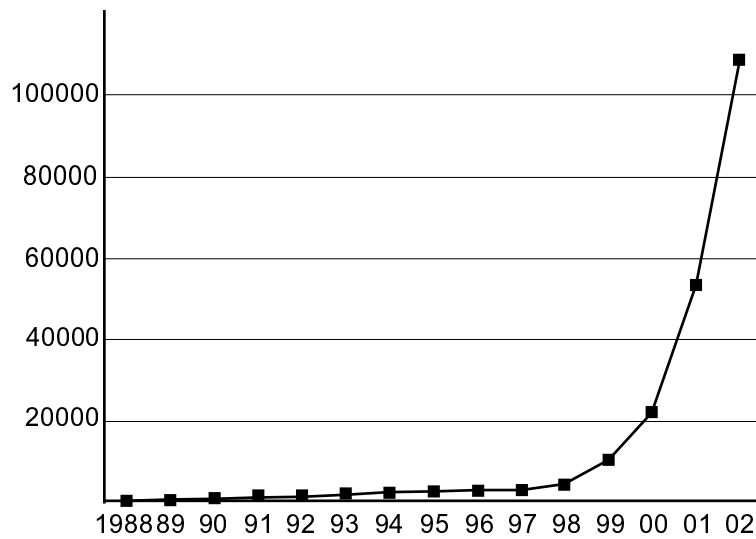


Figure 1.1: The number of reported incidents to CERT [11]

incidents is impossible to evaluate beforehand and thus the optimization is difficult but even in these cases it is essential to find an estimate for possible losses.

Security is conflicts between people and organizations. Often different parties have different security objectives. In an organization one department may optimize its own security so that problems are inflicted on another department or the whole organization. It is also possible that an employee and an employer have different security strategies.

In the 90's very heavy cars became popular in the USA. They were considered secure vehicles because in accidents the people using them were less likely injured than people in other cars. However, these drivers optimized their own situation. These cars caused much more severe injuries to the other people because their security was based on the fact that they just crushed anything with their large mass. The overall effect on security was probably negative. [38]

Security is preparedness. One of the goals for security is to prevent all the incidents which disturb normal work. If such an incident happens, however, there must be a plan for how to minimize the effects of the incident.

The president of the USA was shot in Dallas in 1963. Was that a security catastrophe? No, there was a plan for that situation. The vice president swore the oath in hours and the situation was in order again (organizational view). However, all those with emotional ties to John F. Kennedy may have a very different opinion (personal view).

Security is bureaucracy. The word has negative connotations but, as bureaucracy means standardization of working procedures and results, it is required. Bureaucracy is a method for collecting the best practices from employees and turning those practices into a company standard method.

If you go to a governmental office and a civil servant sends you back home because one form is filled incorrectly, it is bureaucracy. However, if you went to another office with your forms and a clerk said to you only: "there is a problem", it is lack of bureaucracy.

In the first case you know that filling the form properly (and you should be able to know this beforehand) your case will advance. In the other case there is nothing you can do. You do not know which form has to be used today and how it should be filled. You have to come back the next day with the same document and hope that it will be accepted then. In real life we have noticed that this is quite common in many cultures. Customers who do not accept the answer go to the next person to see if the answer would be better or come back the next day to ask again.

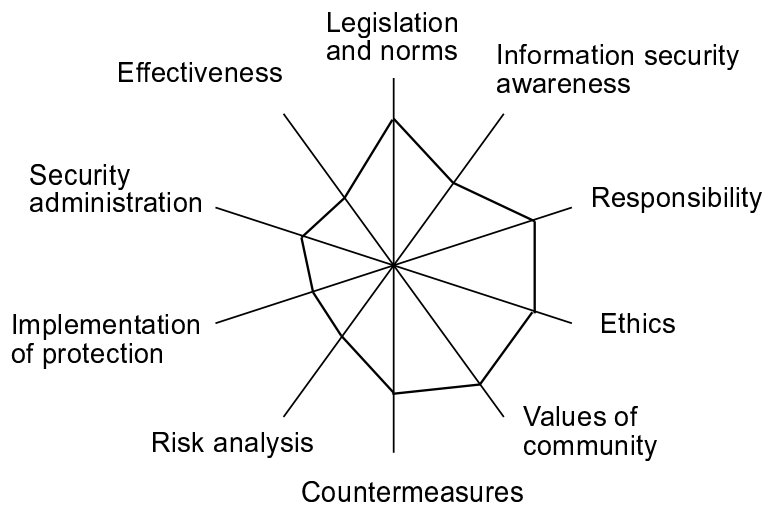


Figure 1.2: The status of different protection methods in Finland [49, p.24]

Huomo et al. undertook research looking at the state of information security in Finland. They state that trust is one of the basic requirements for an information based society. The new business models require companies to connect themselves to the Internet and exchange information with other members of the network. However, the information security level of small companies is, in general, not good enough.

Huomo et al. have also divided information security into eight areas and presented the status of these areas (figure 1.2). In the figure the result increases outwards from the center. [49]

Jayaratha has defined that there are five elements in the information security function [50]:

- information processing and usability function;
- educational and learning function;
- information systems development function;
- management and control function;
- strategy and planning function.

These functions are the basic elements of this thesis. Education and experience are presented in the user's view. Usability is also a part of the user's view but it is included in the developer's view in this thesis. Management is presented using a new model to organize security and a new method to classify assets organization-widely. Selecting the target security level is a part of the business strategy in every organization. The strategy leads to the security policy, which is a tool for profiling an organization in regard to security. A good reputation as a secure product or service may open new business opportunities.

The terms "security", "information security" and "corporate security" are all used in this thesis. One of the very basic themes in this thesis is that

there is no such thing as information security. Information is one asset and it is protected like the other assets. However, many of the examples and actual material come from the area which is usually called information security, since information is a vital factor of production in many areas of industry and there are several standards and practises published to promote information security [3] [5]. Thus the term “information security” exists in the thesis as a practical necessity.

1.2 About the thesis

Background

The writer of this thesis has a long experience in working life. This thesis is actually spurred by real-life experiences. The career in security related positions includes:

- Prime Minister’s Office: System specialist as the information security manager of the State Council of Finland;
- Finnish Defence Forces: Chief information security officer of Finnish Defence Forces;
- Alma Media Inc: Head of corporate security.

In addition to these main employments there have been several other security related activities like:

- Member of the Inter-Departmental Information Security Co-ordination Group;
- Member of the Scientific advisory board of Defence (computers and communication);
- Director of the education program for information security managers at Dipoli (part of Helsinki University of Technology).

Organization of the thesis

After this introduction (Chapter 1) there are two main parts in this thesis. First, four different views on security are presented, one in each chapter (Chapters 2-5). Then some other approaches to security are briefly presented in one chapter. In the second part some methods for organizing security and improving the security level of an organization are presented.

In Chapter 2 the user’s view of information security is presented. There are three different approaches: trust, privacy and education. Trust is, among other things, a basic element of electronic commerce and of using information systems in general. Security is one of the elements of trust and probably the most important element of the feeling of trust when using information systems. The need for privacy is another important topic within security. In the end of that chapter is a discussion about whether education is a suitable way to improve the feeling of security.

In Chapter 3 the developer’s view is presented. What security related aspects does the designer of a new product have to take into account? Security is a requirement for many products and services. As stated in Chapter

2 users require security in products they are using in e.g. electronic commerce. Security is also a way to create a difference between one's own and others' products. Usability is an approach to solve these challenges. Usability as a security point of view is presented. In the end of the chapter security aspects of the development work itself are considered.

Chapter 4 presents an organization's view. How to turn security into a business advantage? There are also suggestions how to organize security within a company. Security is also observed in the long run. The present security level is derived from changes in the history of an organization.

In Chapter 5 a scientist's view is presented. What kind of topics have there been in scientific conferences? These topics describe to some degree, which areas of security have been and are considered important among academic people.

Chapter 6 briefly introduces some other relevant themes. In this chapter security is compared to some other areas, like quality. There are also some considerations on security and geography and on combining physical and information security.

The second part of this thesis begins with Chapter 7. Two security models commonly used in Finland, a model for corporate security and a model for information security, are analyzed and then combined into one model.

In Chapter 8 problems with systematic classification of information and threat analysis of information systems are described. In a modern organization where many units are quite independent and some functions are even outsourced, an exact and uniform classification is needed. In a distributed environment also the threat analysis must be distributed. At the same time the information gathered in the analysis must be reusable. In this chapter a solution for these problems is also suggested.

Finally, the conclusions are given in Chapter 9.

A user is one of the most crucial elements of information systems [88]. In many cases a user is also a customer who can select which services are worth buying. In this chapter a user is considered both as a part of an information system and as an independent customer.

2.1 Social behavior

The human being is a social creature. In his hierarchy, Maslow presented the hierarchy of needs. According to this hierarchy when the lower level needs, like physiological needs, are fulfilled it is possible to move up to higher level needs. Security, social and ego needs, in this order, are the main levels of the hierarchy. Security is the basic element of the hierarchy and people must feel safe (i.e. warm, well fed, not thirsty,...) before they continue to the higher needs. [69]

The Prisoner's Dilemma is another example of human social behavior. The case was originally placed in a prison but the same phenomenon can be found everywhere in social life. If two people co-operate they both get a reasonable result. If one of them deceives the other he gets the best result when the other one gets the worst one. If they both deceive each other they both get a bad result; worse than when co-operating but better than if being deceived. Wu has shown that co-operation always gives the best result in the long run if there is a community. In a situation where one does not know anybody else and there will be no connection afterwards, deceiving is the best strategy. [109]

The community defines what kind of behavior is acceptable. The economics of fair play is a test setup where one person has to make an offer as to how a certain amount of money will be shared between him and another person. If the other person accepts the deal, they both get their shares, otherwise neither of them gets anything. Rationally thinking all the offers should be accepted since anything is more than nothing. However, people have an understanding about a normal offer in their culture and they do not accept an offer that differs too much from this opinion. [93]

These examples show that people do not always (or even usually) act rationally. When making decisions people take into account many irrational or larger scale assumptions. Considering social expectations is naturally rational when living in a society but the connection between a decision and the motives behind it can be difficult to notice. People assume something about other people, they trust some of them and do not trust the rest.

2.2 Trust

Trust is one important part of information systems. Among safety, security and privacy, trust is stated as the most important factor making users feel comfortable with electronic commerce [89]. However, trust is often expressed as a technical question, which differs from the common sense idea

of trust. According Adams and Sasse trust is a feeling a user has and a belief that the behavior of a system or another person is what is expected. [16]

According to a study there are at least six properties which are important when trust is formed. They are 1) seals of approval, 2) brand, 3) navigation, 4) fulfillment, 5) presentation and 6) up-to-date technology. Seals of approval and brand are in many cases transferrable from the real world to electronic commerce but it depends also on the kind of service. [8] Bank services is one case where the brand-based trust is transferrable [53].

The appearance of a service is a more complex issue. Technologically the system is expected to be up-to-date and at the same time the users appreciate simple and classic navigation and layout. Even long response times are reported to frighten the user. [76]

Trust is accumulated over time. In electronic commerce the first step is the try threshold, where a user decides to browse, search and test the service. This is, however, still an untrusted phase. The next phase is the formal level of trust, where a user considers, validates, registers and, after the purchase threshold, also transacts and confirms the purchase. The highest level of trust is the informal level when using a service is a habit. [8]

The formal level of trust requires an authority. Information Systems Secure Interconnection (ISSI) model stated that in the network there must be high level layers above the technical ones. These layers include legal and ethical protocols. [62] An extended model adds a social and group membership layer to the top [65].

The lack of legal, ethical, social and group membership layers on the Internet prevents the existence of such an authority which is required for the formal level of trust. Therefore, building trust is a very slow process on the Internet because one has to bypass the formal level of trust. In some cases it is possible to transfer the brand-based trust to electronic commerce and thus achieve the formal trust level. This, however, requires a real world connection, which usually adds the required legal framework.

Trustworthiness is another dimension. Not everything which is trusted is worth it. However, trust vanishes quickly if something unexpected happens. Trust is often based on one's own experiences, friends, common knowledge and a brand. Many business models on the Internet actually declare lack of trust and trustworthiness. People do not trust electronic commerce on the Internet and often there is a reason for the mistrust. There are several business models which are based on something a user probably does not like. Many sites collect information about users and sell it to advertisers. Subscriptions are renewed automatically, for convenience, using credit card numbers. These business models may be perfectly legal but not something users like or expect. Thus they do not create trust but suspicion.

2.3 An ambassador in the electronic world

An ambassador is an authorized messenger or representative [4]. This means that an ambassador is somebody who is trusted and who can make decisions (at least in certain conditions) on behalf of the authorizer.

If a task has special security requirements one should never use an equipment which is not known and understood. Using unfamiliar tech-

nology will increase the risk that something goes wrong because the system can do something else than expected. Unfortunately there are nowadays many systems, the actual technology of which are beyond the comprehension of normal users.

For example, William J. Caelli has presented that electronic signature is a system where a document is first shown to the user. Then the document is taken away and another document is set before the user folded so that the user does not see the content. “This is the same document, trust me, just put your name there” says the person who needs the signature. A system like this requires a real confidence and trust for the system. Perhaps this is the reason electronic signatures have not become very common. In his paper [27] Caelli has compared digital and electronic signatures with a traditional one. In the same way there are also compared certificates and notariate services provided by PKI¹ with their traditional counterparties. [27]

The same situation occurs when an Internet site asks a user to download a new plug-in to manage the content of that particular site. A user is expected to use some new piece of software without the possibility to ensure that it actually is what was promised. The user should have a possibility to check the functionality of the code or at least to restrict the code in an untrusted sandbox. One solution for this problem is to add a security policy to the plug-in. The user can compare the policy with his own requirements and decide if he trusts the code. [90]

Boris Balacheff et al. suggest that the trust required in the signature process may be solved using a special piece of trusted hardware, display controller in this case. [20] A display controller is a good choice since the main problem, as Caelli stated, is a broken connection between what is shown and what has to be signed. If a user can be assured that the connection is valid the electronic signature is easier to accept.

Balfanz and Felten have another approach. Instead of having a smart card which one has to insert into a computer one can have one’s own trusted device altogether. A problem when using a smart card is that it does not typically have its own display and thus it is not enough for the user to trust only the smart card. The computer using the smart card must also be trusted. If a user has his own device equipped with a display a text is transferred to the device, shown to the user, signed by the user and transferred back to the computer. If the computer is not trustworthy and tries to alter the text, the signature is not valid any more. There is an application for Palm Pilot for this purpose. [21]

The Shaman project has made specifications for PAN (Personal Area Network) which means “a cloud” of personal devices. These devices can communicate with each other and with devices outside the PAN. [9] The identity module is a natural part of the PAN and it probably is capable of showing and making signatures.

¹Public Key Infrastructure

Privacy is another crucial element of electronic commerce. People value privacy and they do not use systems where they assume their private information is used in the manner they do not like. In 1973 Horst Feisel stated that computers constitute, or soon will constitute, a dangerous threat to individuals' privacy. However, he could not see any reason why this problem could not be solved using cryptography. [36]

Privacy is defined as people's right to decide on the usage of their personal information [51]. The terms privacy protection and data protection are used in the same sense, too. However, the definition of personal information is often difficult. If a customer buys something in a shop, is the information about this transaction the customer's personal information? There are two participants in the commerce, a customer and a shop. Which one owns this information? If the customer, then it is under privacy legislation and the shop must not use it. If the shop, it may collect information about consumers and shopping habits without violating their privacy. In Finland this conflict has been solved with the privacy act which states that a shop or other organization must not collect unnecessary information about customers [51].

There are many potential participants in the privacy discussion. One participant is always a person, because of the definition of privacy. The other may be a commercial organization, e.g. a shop, an employer or a governmental organization, e.g. a school. The relationship between shops and customers is quite easy to manage because there is always a risk for the shop that the customer will select another shop next time if the shop uses the information it gets against the customer's expectations. In Finland there are loyalty programs in all three main shop chains. Together they have almost a million customer cards out and these cards are widely used when shopping [6][82]. It would be possible to make very precise models of a person's shopping habits but thus far none of these corporations have done this out of fear of a strong reaction among customers.

The relationship between an employee and an employer is much more difficult. The employer often likes, under the label of supervising, to monitor its employees in a way which disturbs employees. In Finland an act about privacy in working life was passed in 2001 [52]. It states that an employer, in principle, has the right to monitor its employees. However, the monitoring is not yet actually allowed before another act has been passed that regulates how the monitoring should be implemented in practice. The monitoring of users has also some advantages, it is possible to detect intruders by comparing their behavior with authorized users [101][85], or comparing their actions to a historical profile [64]. There are also applications in other areas, like detecting frauds in credit card payments [31] and mobile communication networks [48].

The most problematic is the relationship between people and government. Historically, in many countries the government has the right to collect information about its citizens for various reasons, like taxpaying. It has not been such a big problem until many of these governmental organizations have entered into the business area and started to sell this information.

Understanding the systems used is a good way to improve usability and trust [72]. The better users can use the system the less errors are being made and thus the trust between the user and the system increases. To be trustworthy the system must fulfill the expectations. Adèle Martins has also stated in her study that in an individual user level people need guidance in what kind of behavior is acceptable [68].

Since the security measures are most efficient when they are an integral part of the system [66], security education is not the most needed one but a general computer and information systems education is. Being able to manage work with computers in general prevents errors and creates trust.

The users may behave in a different way according to their skills [P1]. Hackos has described four different levels of users: novice, advanced beginner, competent performer and expert performer. Novice users fear failure and the unknown. They focus on how to do their work and are willing to learn how to do it. Advanced beginners still focus on the actual work but also start to develop a mental model based on their experiences. Competent performers are able to utilize their mental model for complex tasks and expert performers do this often. [43]

Another categorization is based on skill behavior. Actions are automated sensory-motor patterns, rule-based behavior or knowledge-based behavior. Automated sensory-motor patterns are like a reflex. Rule-based behavior is based on recognition and stored rules. Knowledge-based behavior is based on identification and planning. [84]

Novice and advanced beginner users are able to only do the tasks they have learnt and in the way they have been told. If there are proper security functions in the information systems, these users behave well. They do not try to break the systems or find their own solutions. However, if the security functions are not proper, these users are helpless.

Performers may work more efficiently but there are also some risks. If a performer develops a mental model which is false, the results may be unpredictable. There might be some untold or secret reasons why tasks have to be done in a certain way and a performer who optimizes his work may ruin this idea.

If a user wants to work in a secure way in an insecure environment he must understand both computer and security related questions since he must himself arrange the secure environment for work. In a secure environment systems and their administrators take care of many aspects of security but outside this area the user is on his own. He must be able to manage all the aspects of secure computing himself.

As seen in [P1], there might be conflicts between a user and an environment. If a user is capable of doing work in his own way, he may disturb the way other people in the organization work. On the other hand, if a user is not capable of doing his work, he is a security risk. In theory there is an optimum balance between these requirements which is, however, difficult to find since all the cases are different. It is also almost impossible to maintain since both the elements, the skills of the user, and the requirements of the systems change rapidly.

To manage the skills of the employees the company should educate them itself. If the users only learn how to solve problems, they probably will solve the problems very practically and in a personal way. The self-taught persons should be avoided. Instead there should be proper education for how these problems could be avoided or solved in the environment of the organization.

In some cases a user tries to get better security level than the organization is prepared to offer. Either the user has better knowledge of security matters or the user has different needs of security than the organization. These different arrangements may coexist if there is no conflict between the needs and policies. A conflict may occur if, for example, a user requires a protected connection to his bank and uses an encrypted terminal program, like SSH², while an employer does not allow any encrypted connections because he wants to monitor the content of connections. The connection itself might be allowed if the employer accepts this kind of personal usage but the security policies requirements conflict.

As seen in [P3] the government has taken an active role establishing security education for security professionals. Especially in corporation security area standardized requirements are needed in order to transfer some duties, which are this far required an official, to private companies. In information security area there are some commercial based programs, like in [P2], and there are courses for information technology curricula, like described in [P6]. However, security is not part of general knowledge and is not part computer driving licence [12].

²Secure SHell [15]

There are two different aspects of security when developing new products.

A product itself has probably some security features and security is thus one of the requirements on a new product set by the customer. In this sense a product may be a device or a service. Typically it is something a customer uses and is able to form an opinion about.

At the same time the development process itself has to be secure. A secure development process produces stabilized products in a predictable way. Security in this sense is often required by the management or shareholders of an organization.

3.1 Security as a requirement

The security profile of a product

When a new product is first being designed there is a vision about the product, for instance for whom it is intended and for what purpose. From this decision more precise requirements for the product can be defined, like the appearance, price, quality, usability and security. [103]

In a consumer markets these requirements are closely coupled. If the appearance is expensive the price may be high. If the quality of the product seems to be good, the price may also be high. Both of these may set the target user group as older and wealthier customers than if the main feature of the product is the price. Appearance may give the feeling of security as well as quality and usability.

The selection of a profile is a calculated decision and a part of the strategy of an organization. For the long term it may be a part of the brand of the organization. The brand itself is often a reason to select a certain profile. If there is already a certain image, it is easy to make a new product in the same segment. It is also possible that a company has made a big effort to build a brand. A unsuitable product may ruin this work and is therefore not sensible.

In the customer market the trustworthiness or real security of a product is often not as important as the feeling of these. The users have no possibility to evaluate the security level of a product nor the knowledge to analyze the requirements. If nothing too bad happens for a user or friends and there have not been any headlines, the product may be secure enough for a normal customer.

In the business markets there are two main differences. The companies have resources to analyze the products, although they probably do not have enough knowledge to completely define their exact needs. Another difference is the quality of the client. There may be big variations in the quality and security needs of a company. If a producer is targeting the high quality or security market, it is not worthwhile to sell anything to the low level client. If a client is not capable of defining the requirements, the product probably can not fulfill them. A client like this is seldom content with a product. Such a client has trouble anyway and somebody may think it is

the product which is faulty. These incidents may ruin the brand and the general acceptance of the product.

The decisions can be divided into three areas: strategy, design and implementation. In strategic level development one has to e.g. ensure the compliance with the corporate strategy and contracts, meet the security standards and possible certificates, take care about patents and other intellectual properties and get acceptance in the market. On the design level the security requirements have to be integrated with the system specifications. On this level risk analysis and prioritization are performed, too. In the implementation phase the actual security services are implemented. [104]

It is important to implement security features properly especially if the services are to be used on the Internet. In such a case there are two problems: the development has to be very fast and the need for security is high. For such a situation a rapid secure development approach is suggested [58]. It provides security from the beginning, rapid realization of services and integration of security and functionality. The five steps are

1. usage conception where functional and security requirements are specified using scenarios;
2. service specification where protocols and implementations are selected;
3. risk analysis;
4. measures that define how the identified risks should be avoided, reduced, limited and insured;
5. realization where the actual system is implemented.

In Chapter 6.2 we discuss the security and quality of information systems. One of the conclusions is that it is difficult to add security into existing systems. Security has to be a part of the whole process and therefore it has to be a part of the expertise of each participant.

Usability

The taxonomical environment of usability can be presented like in figure 3.1 [42], [72]. In this taxonomy usability is part of the usefulness of the system. For good usability the system must be easy to learn, efficient to use, easy to remember, subjectively pleasing and possible to use with few errors.

The word “security” does not exist in the taxonomy itself (figure 3.1). However, most of the elements of the taxonomy have security-related properties. Usability itself has a clear security property: few errors. One of the main functions of security is avoiding errors and mistakes. There are several sources of these errors and the user is one important source. If a user misunderstands the system he can not behave in a secure way.

Utility is another part of the usefulness in addition to usability. It is defined as the system’s capability to do what is expected. This definition includes all the security requirements of the system, like confidentiality of information, and methods how to fulfill these requirements.

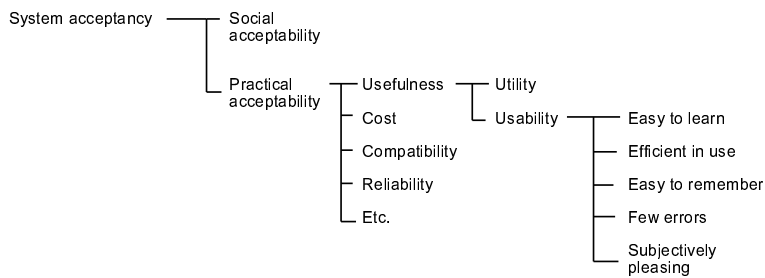


Figure 3.1: Taxonomy of usability [72, p.25]

Usefulness is a part of practical acceptability together with cost, compatibility, reliability and other practical aspects. Reliability is a part of security since availability of information is a basic element of information security.

If practical acceptability is considered a property based on personal experience, social acceptability is based on general experience. Then all the security related matters mentioned above are included also in social acceptability. In addition there are some other properties. As mentioned in chapter 2.2, the brand and company’s general reputation are among the most important factors when a user considers using electronic commerce.

What is then the connection between usability and security? If we want to create a new system people are supposed to use, we have to create trust between the user and the system. The feeling of security is a basic element in creating trust [69]. This feeling is strengthened by the user-interface of the system and usability is a method to assess this interface.

The user interface of a product always generates a mental model for a user. Many of the usability problems are caused by a unsuitable mental model. [83] If the model is somehow wrong the user may behave in such a way that the security level is not as good as the user assumes or the user interface presents.

3.2 Security in the development cycle

The development cycle is a process where an innovation grows into new kinds of products or methods. This process creates new products or new ways to make current products. [103] The cycle may be divided into three phases: the era of substitution, the era of design competition and the era of incremental change [17]. In the substitution phase the new technologies replace the old ones, in the design competition phase the best one is selected and after that there are incremental improvements of that technology. In the case of mature products the improvements typically affect several non-price factors like design, customization and quality [19].

There are several reasons why people adopt new technology. Process innovations lead to lower prices and thus a better relative value. They may also improve quality and that may — besides better relative value — lead to improved image, reputation or brand and make people buy a new product. A product innovation seldom makes a product cheaper but through higher relative quality it may give the buyer a better relative value [28].

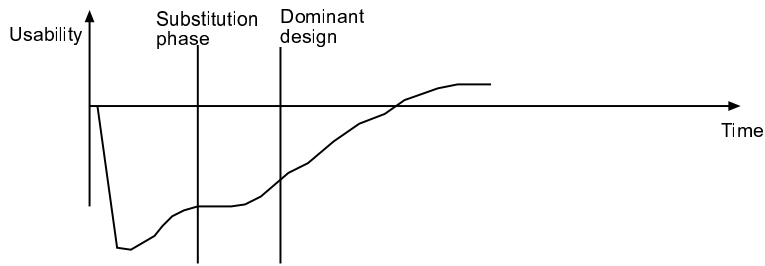


Figure 3.2: Usability and development cycle (qualitative only)

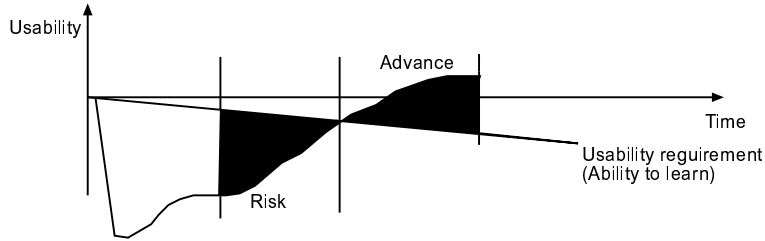


Figure 3.3: Requirements and learning ability (qualitative only)

The penetration of a new technology can often be forecasted with S-curves [70]. In the Bass model people are divided into innovators and imitators. In a penetration process there often is a gap between these groups. [24] Bridging this gap is crucial for promoters of a new technology. This gap is close in time to the emergence of the dominant design when the design competition ends and the incremental improvement begins. [17]. In the usability point of view this development cycle may be described as figure 3.2.

First the development is done with a solely technological view. No attention is paid to usability, the technology is difficult to use and only technologically oriented people will buy such a product. After the substitution phase there are some approaches to improving the user interface but there are still several approaches. Only after the dominant design phase the technology is established and there are remarkable improvements in usability.

In figure 3.2 usability is on the Y-axis. In the beginning usability is very poor compared to a traditional system. The X-axis is time. There is no scale on the Y-axis and the graph is qualitative only.

One can apply the same curve when describing other properties of a product like quality or security. It must be possible for people to make the technology they are using to behave in a secure way [P1]. If the usability of a product is poor, the risks of using such a product are higher.

Technologically oriented people are the first users of a new technology and they are probably able to manage the higher user requirements and therefore use new devices without increased risk. "Ordinary people", however, are comparatively slow in gaining new technology skills. Their learning curve may be described as a line. This line together with the requirement curve is presented in figure 3.3.

In figure 3.3 the requirements and skills are about the same in the beginning. After a new cycle begins there is a rapid increase of the requirements and the gap between the line and the curve is remarkable. However, this gap does not cause a significant increase of risk because the users in this phase are not ordinary users but technologically oriented. When the dominant design is achieved and requirements begin to decrease a number of ordinary people start to use the new technology. This causes a remarkable risk because requirements are not decreasing fast enough and the ability level of ordinary people has not risen enough. After some time usability increases near the ability level and a new product may be even more secure as the previous one.

In the risky phase people store secret files in public folders, delete files accidentally, send confidential material to wrong faxes and e-mail addresses, speak freely on a mobile phone, use typewriters with ribbon that stores all the letters and so on. One of the current problems is the Internet, which is used by many people without any of the needed knowledge to protect themselves.

3.3 Secure development process

Developing a new product is risky, especially in the software business. The development cycles are very fast and technology changes rapidly [91]. At the same time there are good possibilities to make a profit. In the USA the growth of the software industry is higher than of the economy in general [73].

To manage these risks several methods have been developed. In Boehm's risk management model (table 3.1) high level term risk management has been divided to assessment and control and in the end there are simple methods like checklists. [25]

Another method is the Software Risk Evaluation method. There are six phases in the risk management cycle: identify, analyze, plan, track, control and communicate. The risk taxonomy of Software Engineering Institute (SEI) is presented in table 3.2. [95]

Boehm's risk model fits fairly well security-related risks, too. Only some of the methods (the rightmost column in table 3.1) have to be changed. In security management risks have to be identified, classified and prioritized. Then the acceptable risk level is decided. After this decision the risks are either reduced below the level or transferred to somebody else, like an insurance company. Risks have to be monitored all the time.

In SEI's taxonomy risks are divided into three main areas: product related risks, project related risks and organization related risks. This chapter is mainly concentrated on project related risks but product related risks are discussed in Chapter 3.1 and organization related risks in Chapter 4.2.

Some of the risks in the development environment are based on the same requirements as product risks. The development environment has to be available, usable and produce correct output.

Development-specified risks are, when considering security, process control risks. The process control has to assure that all the decisions during the process are made with the correct reasoning and documented well. If e.g.

Risk management	Risk assessment	Risk identification	Checklists
			Decision-driver analysis
			Assumption analysis
			Decomposition
			Brainstorming
		Risk analysis	Decision analysis
			Network analysis
			Cost models
			Quality factor analysis
	Risk prioritization	Performance analysis	
		Risk exposure	
		Risk reduction leverage	
	Risk control	Risk management planning	Compound reduction
			Buying information
			Risk avoidance
			Risk transfer
			Risk reduction
			Risk element planning
		Risk resolution	Risk plan integration
			Prototypes
Simulations			
Benchmarks			
Risk monitoring		Analyses	
	Staffing		
	Milestone tracking		
	Top 10 tracking		
	Risk reassessment		
Corrective action			

Table 3.1: Boehm's risk model [25]

A Product engineering	B. Development environment	C. Program constraints
1. Requirements a. Stability b. Completeness c. Clarity d. Validity e. Feasibility f. Precedent g. Scale	1. Development process a. Formality b. Suitability c. Process control d. Familiarity e. Product control	1. Resources a. Schedule b. Staff c. Budget d. Facilities
2. Design a. Functionality b. Difficulty c. Interfaces d. Performance e. Testability f. Hardware constraints g. Non-developmental software	2. Development system a. Capacity b. Suitability c. Usability e. Reliability f. System support g. Deliverability	2. Contract a. Type of contract b. Restrictions c. Dependencies
3. Code and unit test a. Environment b. Product integration c. System integration	3. Management process a. Planning b. Project organization c. Management experience d. Program interfaces	3. Program interface a. Customer b. Associate contractors c. Subcontractors d. Prime contractor e. Corporate management f. Vendors g. Politics
4. Engineering specialities a. Maintainability b. Reliability c. Safety d. Security e. Human factors f. Specifications	4. Management methods a. Monitoring b. Personal management c. Quality assurance d. Configuring management	
	5. Work Environment a. Quality attitude b. Cooperation c. Communication d. Morale	

Table 3.2: Risk taxonomy [95]

there is a huge number of old PCs in stock it may be a good reason to select old PCs as the platform of a new product. This reason, however, has to be documented well because next time this reason may not be applicable. If somebody has made a “good explanation” for using old PCs, more of them may be ordered for the next project.

Security risks are often difficult to distinguish from normal operation risks. Risks belong to business. Without taking risks there is no profit. Which risks are normal and which are security risks? A project manager may take a risk when calculating an offer. If the facts are known, the risk is manageable and according to the corporate policy, it is part of the business. Otherwise, especially if it is against the policy, it might also be a security violation.

Risks in product engineering (Table 3.2) have security related questions in engineering specialties. Those questions are actually quite the same as in figure 6.2 where the parts of software quality are presented.

Finally, the program interfaces in the organization section (Table 3.2) are interesting because there are those interest groups which have to be taken into account when an organization declares its security policy. There are customers, contractors, management and society. Only stakeholders are missing.

Security is an important function on all levels of a hierarchy: individual, organization, government and global. Organization is, however, the level where most of the security functions are located. Individuals require security but do not have resources. Governments have powerful resources to protect themselves but the number of protected assets is low compared with all the other organizations.

4.1 Organizing security

A rapid change in organization structure has caused major changes also in the way security has been placed in the organization. In a traditional hierarchy the managerial relationships were clear. The upper level had total control over the lower level and the upper level was also responsible for its subordinates. Often there was a headquarter with some general staff and among them there was usually a security manager. The security manager could command all the units using the executive power of the managing director.

In a modern organization there is no such structure. The units may be quite independent and the organizational structure builds up from agreements. Units may buy products and services from each other and may even compete with each other. In such a situation there is no clear command structure but a network, instead. In this case also the security responsibility is delegated to the units.

Today many operations have been outsourced. Sometimes one may assume that services bought internally from another organization unit often include some security features even without an exact agreement but one can not expect any free services from another company. Thus all the requirements have to be stated in the outsourcing agreements and if those agreements are made at many locations in the organization, every signer of these agreements must be able to declare the security requirements along with the operational ones.

In these modern organizations security related requirements must be part of contracts between business units and partners. The requirements must be stated in the agreement and the cost of producing them must be a part of the price.

4.2 Organizational security

Security is always a part of an organization's work, either consciously or unconsciously. As defined in Chapter 7.3, security prevents incidents that disturb the work in the organization. Employees make the organization and thus those employees are the main concern when discussing organizational security. As said in [P4] employees are storages of information. The availability of this information has to be ensured somehow. If a piece of information is only in the mind of one employee, that information is

lost when the employee leaves the organization. Thus organizations have to transfer as much information as possible from a single employee to the organization itself (to all of the employees).

Another important point is described in Chapter 1.1. The decision process has to be uniform. If a decision has to be made the process should always produce the same output from the same input. Usually there is no room for personal opinions. This way the decisions are predictable and afterwards it is possible to analyze decisions. The reactions of a company must not depend on chance: who happens to be in charge today.

A method to solve both of these problems, information transfer and uniform decisions, is called bureaucracy. It collects the good practices, standardizes them and makes sure the employees use them. It also prevents unnecessary work when every employee does not need to invent the same procedures again.

This approach of course may cause conflicts between more advanced users (performers in Chapter 2.5) and the organization because when employees are capable of creating their own mental models they are also capable of making decisions in their own way.

4.3 Conflicts between security needs

There are many chapters in this thesis where conflicts between several subjects are mentioned (e.g. 1.1, 2.1, 2.4, 2.5 and 4.2). These conflicts should be solved in systematic and ethical ways in order to achieve a stable secure state.

Conflicts between an employee and an employer are quite common. Especially Internet-usage has caused several conflicts and the pros and cons are discussed in several articles. Lim et al. use the term “cyberloaf” for any voluntary use of the company’s Internet access during working hours to surf nonwork-related web sites for nonworking-purpose. Nonwork-related e-mail is also considered “cyberloafing”. According to their study half of the users browse nonwork-related web sites a few times a week and about 80 % either use the employer’s e-mail system for private communication or check private e-mail elsewhere using the employer’s equipment. [67]

The usage of Internet in a company requires a policy. Simmer suggests that beside the policy there should also be an Internet policy management (IPM) which has four essential components:

1. Internet usage policy;
2. tools for monitoring and recording usage;
3. user training and
4. application for disciplines measure.

The monitoring is a very important part of management. [94]

When Siau et al. have studied acceptable Internet usage policy in various organizations they have defined a set of abuse types (table 4.1 [92]). In general most of the organizations have a policy against the types that are unlawful: general e-mail abuse, unauthorized use and copyright infringement. All the other restrictions depend on the organization. ISP-like

General Email abuse	Include spamming, harassment, chain letters, solicitations, spoofing, propagation of viruses and defamatory statements
Unauthorized usage and access	Sharing a password and access into networks without permission
Copyright infringement / plagiarism	Using illegal or pirated software that cost organisation millions of dollars because of copyright infringements. Copying of web sites and copyrighted logos
Newsgroup posting	Posting of messages on various nonwork-related topics from sex to lawn care advises
Transmission of confidential data	Using the Internet to display or transmit trade secrets
Pornography	Accessing sexually explicit sites from work place as well as the display, distribution and surfing of these offensive sites
Hacking	Hacking of web sites, ranging from denial-of-service attacks to accessing organizational databases
Nonwork-related download/upload	Propagation of software that ties up bandwidth. Programs such as Gnutella or Napster allow the transmission of movies, music and graphical materials
Leisure use of the Internet	Loafing around Internet, which includes shopping, sending e-cards and personal e-mail, gambling online, chatting, game playing, auctioning, stock trading and doing other personal activities
Usage of external ISPs (Internet Service Provider)	Using an external ISP to connect to the Internet to avoid detection
Moonlighting	Using office resources such as networks and computers to organize and conduct personal business (side jobs)

Table 4.1: Definitions of different types of Internet abuses [92]

organizations have, in general, less restrictions than educational institutes which have less restrictions than other organizations. [92]

Urbaczewski and Jessup have studied how monitoring of Internet usage affects the efficiency and satisfaction of work. In general, monitoring has a positive effect on productivity but it decreases work satisfaction. However, if the results of the monitoring are given instead of the employer to the employee as a feedback, this does not decrease the satisfaction as much and the productivity remains as high as in the first case. [105]

Panko and Beh have collected information about court cases where an employer has monitored either the Internet-usage or e-mail of an employee. According to these cases it is difficult to say where the limit of sexual harassment is. However, according to most justice cases an employer has had the right to monitor the Internet-usage and the e-mail of an employee in order to prevent or investigate sexual harassment. [74]

The previous examples are from the USA where the legislation and culture differ from the Finnish situation. As said in Chapter 2.4, in Finland there is an act to prevent privacy intrusion in workplaces [52]. The Ministry of Finance (of Finland) has published three guidelines about security when using the Internet. The author of this thesis has participated in all of these and is the main designer of the current guidelines [107].

One reason for the different situation between the USA and Finland may be a different cultural position on the individualism/collectivism scale. According to Erkki Kauhanen employees in individualistic cultures are emotionally very independent from their employers whereas in collectivistic cultures employees have strong ties to their employers [56]. In the collectivistic case the working place is a bigger part of the employee's life and thus they probably tend to do also private tasks at the working place easier than in individualistic cultures and employers also are more willing to accept that. According to Geert Hofstede's study, Finland is one of the most collectivistic cultures among the western countries when the USA is the most individualistic culture [47].

Jill Slay and Gerald Quirchmayer have presented a method for resolving conflicts between different bodies. In this method they first find out the common interests and beliefs of the bodies and then resolve the possible conflicts. In the end the viewpoints of the bodies are integrated to reach a common business strategy (their actual target is to resolve conflicts between companies doing business together). [96] In Finland the power distance between people is short [47]. The equality between genders and different social groups is stronger than in many other countries [13].

Thus we assume that the area of common interests and beliefs is generally bigger in Finland than e.g. in the USA and therefore it is easier to achieve a common view in the basic fair use principles. After that it is easier to be flexible in the minor issues and the acceptable use rules in companies do not need to be defined as tightly as in the USA.

Many Finnish companies assume that their employees spend many hours at the working place in addition to the official working hours. Almost 80 % of The Finnish Association of Graduate Engineer members work regularly in their free time and 10 % work more than 10 hours extra in a week [87]. For this purpose companies arrange many kinds of services, like pizza

and cola, to their employees to keep them at work longer. Some employers even send a babysitter to the employee's home to take care of ill children so that an employee does not have to be absent from work. In this culture it would be quite absurd to require that the employees not to use the employer's equipment to read their personal e-mail or to manage personal routines using the web.

Another real life problem, based on the experience of the author: a company required its employees to use external e-mail systems for private purposes. The employees did as the company wanted and most of them had a personal e-mail address from some ISP. After a while it was noticed that an increasing amount of business e-mail was addressed to these personal addresses. We noticed that many of the clients had also personal contacts with our employees. Although our own employees could see a difference between business and personal e-mail the clients could not. They replied to received e-mails and did not check the address. The company did not even know where the private accounts were and they seemed to cause a severe threat since the company had no control over them and there was a possibility that secret or otherwise critical information would go outside the control of the company. Accepting private e-mail usage was a smaller problem than a critical message in unknown mailbox.

Using e-mail has two participants: a sender and a receiver. E.g. copyright legislation grants an author the right to decide on the usage of his work. In Finland this right is granted automatically without any special ©-mark. If an e-mail is intended only for the recipient, the employer violates the copyright if the message is read. Since one can not conclude the nature of the recipient from the address it is impossible to say if the e-mail is intended for a person or a company. E.g. the address of the author of this thesis is teemupekka.virtanen@hut.fi. If he is an employee of the university there is a possibility that the university as an employer would have right to read e-mails. However, if he is a student, such a right would not exist in any case.

As a result of these problems the company decided to allow limited private usage of the e-mail system of an employer and grant the privacy of the messages. Usage was limited in the sense that an employee could only be told to limit the amount of the messages or the time spent handling those messages. For customer contacts there were non-personalized addresses, e.g. sales@company.com. The employees must take care (handle oneself or forward) all the business e-mail they received.

For web surfing the base solution was to gather information about how much time employees spend on the web. The content or the addresses of the sites were not monitored. If employees spent too much time on the Internet or there was too much data moving in our communication channels, we would have restricted the connections.

A technical solution the company considered was installing two proxies, one for business surfing and other for private usage. In the private proxy the privacy of the communication was granted and only the time and amount data would have been stored. In the business proxy all the connections would have been monitored. This approach would have granted the privacy of private communication and given the employer a possibility to restrict

the amount of surfing if necessary.

4.4 Security culture and evolution

Quality is a matter of organizational culture [86]. It is difficult to improve quality considerably without changing the working culture of the organization. As will be presented in Chapter 6.2 one may use the same approaches to security as to quality and thus also security depends on organizational culture.

Organizations tend to explain many failures as human failure. However there is no such simple explanation as “human error”. There are many organization-based factors that cause errors, like the lack of guidance or challenges, variation or the possibility to relax. There are pressures caused by punishment or rewarding. Then there most likely are disturbance, non-standard actions and errors. In all of these cases human error is an easy way to find somebody to punish or to avoid the need to remove the real cause of the problem. [98]

In [P1] we have studied the effects of the computing history of an organization on its present security level. We assumed that there is an effect. Most current information systems are based on a client-server architecture. There are servers, which provide storage and processing capacity and workstations, which are used as terminals. The servers and workstations are connected to a network, which offers also other services, like printers and connections to other locations.

There are two possible origins to this culture, the first of which is mainframe architecture. In this case early in the organization history there were mainframes and terminals. The mainframes were located in special computer rooms and operated by special staff. In earliest history ordinary users could not even use the computers themselves but had to provide tasks to the operators who would then run the task. Later several terminals were connected to the mainframe. Most of the peripheral devices were connected directly to the mainframe. After the breakthrough of microcomputers, terminals disappeared and workstations appeared instead. The mainframes changed to servers and the client-server architecture was achieved.

Another development scenario starts from microcomputers. In this case in the beginning there was a very limited number of microcomputers which were used by the few technically advanced employees. In some cases the first designated microcomputer owner was a director but he was probably not using the computer at all. After that several additional computers appeared and after some time those were connected together using a network. Common services, like printers and file storages, appeared and the architecture became a client-server one.

In the mainframe era there had been some policies from the beginning. Mainframes were expensive and thus there had to be a good reason to buy them. There were limitations to who was allowed to use them, too. The storage space was limited and peripherals few. If a user wanted to use a computer he had to accept the rules. Often several courses were required for those who wanted to use computers, or at least for those who were going to operate them.

In the microcomputer era almost everything was the opposite. The first users were individuals who made their computers suitable for their personal needs. There were no common policies but several individually equipped workstations. The users managed their own workstations without any limitations and were often self-taught persons in computing.

In the first case (mainframes) there have always been policies on how to use computers. There has also been staff who were educated and qualified to operate computers and networks. Often the policies stay even when the environment changes and thus they are probably present also today.

In the second case (microcomputers) such a culture has probably never matured. In the beginning no administration was needed and after it was created the administration is often considered a hindrance to real work.

Thus, at present we have organizations with seemingly the same computer architecture but very different computational histories. The actual security level of organizations varies a lot since the attitudes among the managers and the employees affect their willingness to accept the policies and rules.

There have been several scientific conferences about information security during the last decades. The content of these conferences gives us an impression about what are the most important areas of information security in this timeframe. For this purpose we have selected the IFIP Technical Committee 11 conferences. International Federation of Information Processing (IFIP) was established in 1960 and is a nonprofit umbrella organization of national information processing societies. IFIP has declared research, development and education as one of its principal areas. There are 13 technical committees for different areas of information processing, one of which is TC 11, Security and Protection in IP systems. [14]

There have been 17 conferences since 1983. In 1999 there was no conference. We have included the 11 latest conferences and some earlier conferences. The conferences are

- 1983 (1st): Security, IFIP/Sec '83, Sweden [106]
- 1984 (2nd): Computer Security: A Global Challenge, Canada [37]
- 1985 (3rd): Computer Security: The Practical Issues in a Troubled World, Ireland [41]
- 1988 (5th): Computer Security in the Age of Information, Australia [26]
- 1991: Creating Confidence in Information Processing, United Kingdom [1]
- 1992 (8th): Security and Control: From Small Systems to Large, Singapore [35]
- 1993 (9th): Computer Security: Discovering Tomorrow, Canada [32]
- 1994 (10th): Security and Protection of Information Processing Systems, Curacao [2]
- 1995 (11th): Security, the Next Decade, South Africa [34]
- 1996 (12th): Information Systems Security, Greece [55]
- 1997 (13th): Information Security in Research and Business, Denmark [110]
- 1998 (14th): Global IT Security, Austria/Hungary [75]
- 2000 (16th): Information Security for Global Information Infrastructures, China [81]

	83	84	85	88	91	92	93	94	95	96	97	98	00	01	02
Administration	32	34	26	23	25	36	27	29	38	30	29	21	26	22	24
Personnel	16	2	5	5	7	23	23	2	7	5	4	3	4	3	11
Physical	4	4	0	0	0	5	0	0	0	0	0	0	0	0	0
Hardware	2	0	5	10	2	0	0	4	0	5	0	7	6	6	4
Software	30	38	31	35	32	23	43	27	40	35	10	41	28	28	22
Communication	0	4	7	18	11	14	7	22	11	38	21	26	20	25	37
Data	0	4	7	3	2	0	0	4	4	3	6	0	10	3	0
Operational	4	13	14	0	5	0	3	10	0	8	2	2	2	9	2
No of papers	44	47	42	40	44	22	30	51	45	37	48	61	50	32	45

Table 5.1: Content according to the to 8 sectors model (% of papers)

- 2001 (16th)¹ : Trusted Information, The New Decade Challenge, France [33]
- 2002 (17th): Security in the Information Society, Visions and Perspectives, Egypt [39]

The scientific level of these conferences has varied a lot. In the beginning they were pure scientific conferences but in the beginning of the 90' there were some very commercial ones and e.g. in 1991 there was a conference in London where the proceedings was a binder full of handouts of slides [1]. Then the scientific level increased again and there has been a proper full paper review as in any proper conference.

5.1 Track comparison

In most of the conferences the program was divided into several tracks or sections. Even if there is only one track i.e. only one presentation at a time, there are sections with titles in ten of the conferences. The majority of conferences have a section for security management (9 times), cryptography (8) and network security (7). There have been also sections for risk management (6), access control (6), education (6) and database security (5). Trusted systems (3), policies (2) and protocols (2) have seldom had their own tracks. Privacy has earned an own section in only one conference out of ten.

There are of course several different titles and different ways to divide presentations into tracks. There have, for example, been privacy-related presentations in several conferences but within another section.

5.2 Contents of the conferences

Information security can be divided into eight sectors as will be stated in chapter 7 in this thesis. These sectors are administrative, personnel, physical, hardware, software, communication, data and operational security.

There were some common topics which were difficult to classify according to this division. Cryptographic devices belong to the hardware security

¹As one can see according to the proceedings there have been no 15th conference and twice 16th conference. This is probably due to the missing 1999 conference. Originally year 2000 conference was the 16th and it changed to the 15th conference when the previous one was cancelled.

	83	84	85	88	91	92	93	94	95	96	97	98	00	01	02
Administrative	36	34	28	27	29	36	29	27	38	30	31	20	28	22	24
Asset	0	2	8	3	0	0	0	2	0	0	0	2	4	0	0
Personnel	18	2	5	6	8	23	25	2	7	5	4	3	4	3	11
Physical	5	4	0	0	0	5	0	0	0	0	0	0	0	0	0
IT	36	45	45	64	55	36	43	55	51	81	33	74	60	63	63
Operational	5	13	15	0	5	0	4	8	0	8	2	2	2	9	2
No of papers	44	47	42	40	44	22	30	51	45	37	48	61	50	32	45

Table 5.2: Content according to the 4 sectors model (% of papers)

and cryptosystems in general to software security but there was no natural place for algorithms. In Table 5.1 they are classified in “software security”. Protocols are another difficult area. They are placed in “communication security”. Privacy issues are in “personnel security”, another possibility would be “data security”.

According to the division in 8 sectors model there are three popular sectors: administration, software and communication. Typically 70-80% of papers belong to these sectors. These areas, however, includes cryptography, risk analysis and protocols, which have always been popular topics.

Early conferences were clearly named as computer security conferences. According to the content of the conferences this naming is appropriate. The later conferences have names which refer to information security or protection of information. However, there is no change in the content of these conferences which would make this change acceptable.

According to this analysis it looks that the scientific view of information security consists of number of small areas which are easily presented in scientific notation. These areas include cryptography, risk analysis, protocols and some technical solutions, like access control and key management. There are very few presentations about personnel management, physical security or methods to classify information which are essential parts of information security.

Another division is presented in [P4]. In this model there are two mandatory areas: security management and asset management. In addition there are four protective methods: personnel, physical, information technology and operational security.

Using another model to divide content does not make any remarkable difference. Joining different aspects of IT-technology to an information technology security only makes the vision clearer. This area is the largest area and usually covers more than half of the presentations alone.

5.3 Comments about scientific areas

Security is a large and heterogeneous field. As presented in this thesis there are several possible views which have security related implications. Is security science? Yes, but not traditional “hard” science but more like social sciences. There are several smaller areas which belong to the traditional science, like cryptography and security protocols. However, building security using only these methods does not work.

The roots of information security are in the computer science. The names of IFIP conferences imply a strong connection with computers. The

first conferences were named as computer security conferences. In the 90's the name changed first to include security of information processing and then information security. In many universities information or computer security is part of computer science.

A corporate security is more difficult to locate in the university world than information security. Traditionally security professionals are educated in special colleges, like military, police and fire academies [P3]. According Hesse and Smith there are several colleges offering security courses in the USA within justice or crime prevention studies. They suggest that security is an interdisciplinary area which requires knowledge and skills from many areas. However, they do not suggest any faculty to be responsible for security education. [46] We have combined corporate and information security education at Helsinki University of Technology as a part of computer science [P6].

In the Finnish language there is only one word for both security and safety. According to our definition in this thesis (Chapter 7.3) safety is one part of security since operational security requires that the normal work is done in a secure way. When security in general is in many cases part of justice or crime prevention (or in special colleges), information security is a part of computer science. However in safety psychology is an essential part. We can not see any reason why the goal of security is to prevent people from doing something wrong while safety means getting people to do the right thing.

The result we have gathered on IFIP conferences can be compared with another conferences. Mary Zurko has analyzed citations of three conferences, namely Computer Security Foundations Workshop (CSFW), New Security Paradigms Workshop (NSPW) and IEEE Symposium on Security and Privacy (S&P) during several years. [111] In the year she has selected for her study (1996) the two most cited articles in each conference were divided as three articles in human aspects (trust management, user-centered security and social control), two in security protocols and one in computer security (Java security). The result is quite different from the IFIP conferences described in tables 5.1 and 5.2.

In addition to the four views presented in the previous chapters we like to introduce shortly some other relevant views. First we present that traditional physical security and information security have many common elements and definitions. Then we present security and quality together. At last we bring some ideas from the social geography to the “cyberworld”.

6.1 Physical and information technology security

Courtney has, in the early computer security literature, divided safeguards into preventative, detective, corrective and deterrent safeguards [29]. The preventive safeguards, as the name implies, prevents hazards to occur. The detective safeguards find out that something is going on. The corrective measures attempt to bring the original situation back. The deterrent measures try to discourage intruder from even trying.

This model is said to fit well against criminal activities, but not against an information war or a corporate espionage. Instead, a packaged safeguard model has been offered, in which there are five independent safeguard layers: the technology, the operational, the managerial, the organizational and the meta-safeguard layer. [23] Since critical systems must be protected by more than one safeguard there should be at least one method in every layer protecting against any hazard.

In another survey a taxonomy was used where deliberate hazards were divided into four modes: falsification, physical assault, cracking and malicious code. There were also three types of motives: fraud, espionage and vandalism. [22] In this survey Baskerville noticed that cracking was the most common hazard type altogether but when he investigated at motives, cracking was the most popular method only in vandalism.

The early model with four types of safeguards is an instance of physical security in the information area. In the physical security, as a part of corporate security, there are methods to prevent intruders, like walls, fences, doors and locks. There are also methods to detect if an intruder is breaking these barriers, like cameras, infrared detectors and radars. The next step is active countermeasures, guards, who are alarmed by detection and prevent the further intrusion. There are also deterrent elements keeping guards visible and placing warning signs outside the site.

In the physical security it is possible to determine the reasonable strength of a preventive barrier using formula $T_b > T_d + T_g$, which means that the time it takes an intruder to break the barrier has to be greater than the time of detection and time for a guard to arrive together. Of course there might be several barriers in which case the total amount of breaking times must be greater than the time it takes for a guard to notice the intrusion and come to prevent it. If there is no detection or countermeasures at all, the time becomes infinite. One can say that it is not possible to protect anything with only passive preventive method. If there is enough time, all the barriers may be broken.

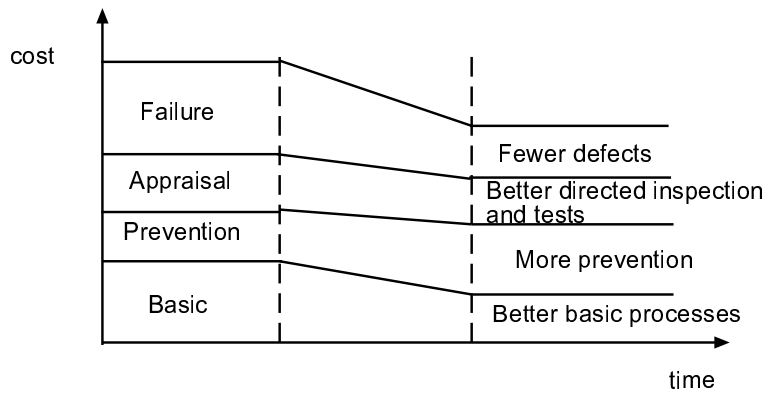


Figure 6.1: Quality and cost [86, p.5]

The same principles are true also in information area. Besides the preventive method, like access control, also intrusion detection is needed. There should also be countermeasures if something is detected. For example the minimum acceptable length of a password depends on how many wrong attempts are accepted and how fast these attempts are detected. Without any detection or countermeasures all the passwords are subject to broken by brute force.

If we compare the suggested new model in Chapter 7.3 with an old model [29] and a packaged safeguard model [23], we can notice that an old model presents information technology security as a counterpart of physical security. In this sense the old model is still valid. However, it is not a model of information security but information technology security. The packaged safeguard model has many similar elements as the new model: managerial, technology, operational and organizational elements can be found in the new model also. The most notable difference is the lack of the asset management and the physical security.

6.2 Security and quality

There are two main reasons to maintain quality in production: cost and benefits. The effect of quality improvements to cost is presented in figure 6.1. [86]

In the figure 6.1 the basic cost is the production cost. When the production processes become more efficient, these costs will decrease. The prevention cost include the efforts to prevent failures, for example training and eliminating causes of failures. The appraisal means evaluating if the product meets the standards and the requirements. The failure cost include all the cost caused by defect products found in appraisal or by customers. There is some advantage in ensuring that basic processes are efficient but the main advantage is in preventing failures.

The basic idea is the same in security. In figure 6.2 we present the cost effects of security in the same manner.

In figure 6.2 the improvement of basic processes means decreasing the

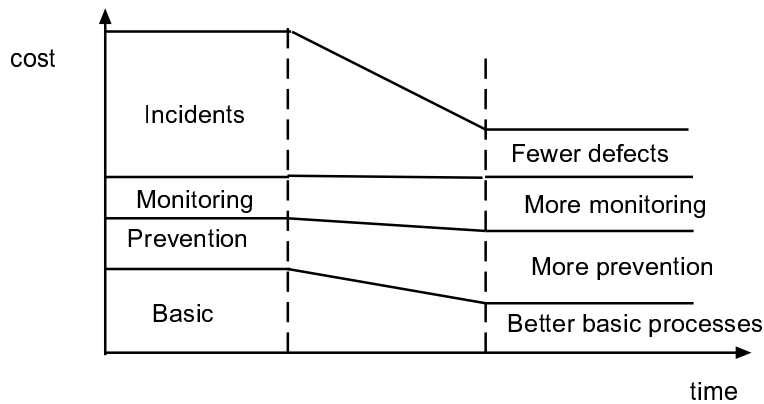


Figure 6.2: Security and cost

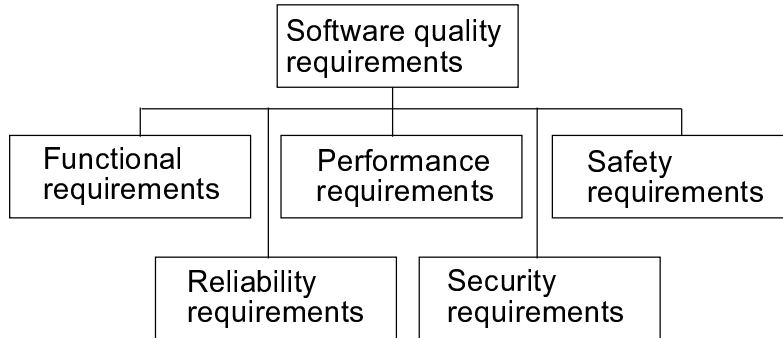


Figure 6.3: Security and quality by Herrmann [45, p.29]

amount of unnecessary work. The employees do not have to use their time to check security related matters. Instead they can concentrate on their work. The prevention and the monitoring increase when these duties are transferred from other employees to specialists. The main advantage is fewer defects.

There are lot of definitions for the terms security, safety, reliability, quality and how they interact each other. Ross Anderson has said: “Security engineering is about building systems to remain dependable in the face of malice, error or mischance” [18].

Another view is presented in figure 6.3 [45]. In that view quality is on the top. Software quality requirements include security features.

Functional requirements mean that the software fulfills the specification and is able to do the job. Performance is the ability to produce the output in given time in normal operation. Reliability means that the software is in normal operation often enough. Safety requirements prevent the software to cause harm to others and security requirements prevent others to cause harm to the software.

In the case of a software or even an information systems this taxonomy is acceptable. Software quality means that the software fulfills the require-

ments. Security is only one source of requirements. However, there are usually higher level security requirements. Usually there is a corporate security policy which states that the software must meet the quality requirements.

Another approach is to define quality and security as parallel functions which have a common goal: everything goes like planned. However, they have a different kind of threat. Quality prevents incidents inside the process. In this case the threat is inside software, a vulnerability or malfunction. In the quality case problems are avoided by a better designing and programming. Security prevents incidents coming outside the process. Threat is an outsider who prevents the software from working properly. Security incidents are prevented by preventing outsiders: people, nature or acts of God from disturbing the process. Usually both approaches have many common elements. If one of them is properly managed, it is reasonable enough in most cases.

As a conclusion about the quality vs. security discussion we can say that there are a lot of common elements. The goal is usually the same: working without incidents. The methods are basically the same: plan what to do, do what you planned and document the deviations. Quality is more interested in the system itself and the problems inside it, while security prepares against threats from the outside. Both of these elements have to be built into systems at an early stage. It is difficult to add quality in the existing system and adding security is difficult, too.

6.3 Security in a space

In the social geography one of the issues is what kind of effect spatial environment has on people, especially in certain social situations. The geography of fear is often connected with women's fear to walk at nights but in general there are several groups who avoid certain places or situations for the same reason. If we define security as a situation without the feeling of fear, spatial dimensions of fear become interesting.

In her thesis Hille Koskela has studied spatial dimensions of fear. Defining space as a surface it is possible to define vulnerable areas based on crime rate in an area. It is also possible to combine physical and social dimensions of space. In that case the fear may be connected to certain places. A third approach is to connect fear to social practices. [61]

In another study Koskela stated that social practises may be part of social control and they may have effects on equality among people. Fear prevents some people to visit certain places or make them behave in a certain way. According to this approach the high amount of fear is a sign of inequality in society. [60]

These same dimensions might be possible to identify in information space too. There are locations or "services", which are often considered as dangerous, like many sex-services. There are also some combinations of places and social aspects, like discussion or dating services. Also the social aspect is present. There are people who feel themselves uncomfortable always on the Internet.

On the Internet it easy to see the privatization, the same development

that Koskela has noticed in physical world [61]. Some people avoid some places because of their fear and thus those places are not common property any more. On the other hand, people try to restrict the admission to their neighbourhood of those, who they think may cause a threat. On the Internet there are immoral and thus places many people avoid, private services and hidden connections as well.

It would be interesting to study if the assumption about equality holds true on the Internet too. If in physical world women feel themselves as potent victims of crime and fear more, the situation should not be the same on the Internet. As there is no physical contact and it is actually difficult to even know the gender of other people, there should be no reason to fear according the gender. Maybe it is incompetent people who should be afraid that they were behaving in a wrong way and lose something.

In this chapter we present some existing methods to divide security and information security into several functions. Then we present a new division to combine corporate and information security as a one model.

7.1 Information security vs. corporate security

The governmental information security policy in Finland

Inter-Departmental Information Security Co-ordination Group set up a committee to prepare a policy decision on information security for the Finnish Government in 1992. In cleartext this means an information security policy for governmental organizations. The first version was published in 1992 and it was revised in 1998. This policy was once available in English, too but the current version it is only available in Finnish [7].

Information security is defined in this policy as the proper protection of information, information systems, communication and services both in normal and emergency situations using legislation and other protection methods. The confidentiality, integrity and availability of information are protected against threats and losses caused by hardware and software malfunctions, natural catastrophes and acts of malicious, careless or unskilled people [7].

In the policy information security is divided into eight areas: administrative information security, personnel security, physical security, communication security, hardware security, software security, data security and operational security. This division the writer of the policy adapted from the Royal Canadian Mounted Police [102].

The corporate security model of Finnish employers

The confederation of Finnish employers has maintained standards and education on corporate security for several years. This work is based on the thesis of Markku Pesonen [79] which has been published only in Finnish. The Finnish de facto standard security education is also based on this model [P3].

In this model security is divided into ten areas: security management, security of production and operations, occupational health and safety, environmental security, rescue operations, emergency planning, information security, personnel security, premises security, security of operation abroad, and crime prevention. These areas are described in [P4].

7.2 Comparing the models

We have compared these two models and some other models in [P4]. Both these models cover almost every aspect of corporate and information security. It is not possible to use both of them simultaneously if the duties of managing corporate and information security are separated. On the other

hand if there is only one manager for both areas this conflict does not disturb.

Information security is one part of the corporate security model. If we put the information security model inside that part we get a model where for example physical and personnel security are doubled. Another possibility is that we take all non-computer elements out of the information security model and then join the models. However, there are several internal contradictions in the corporate security model.

We tried to combine the models also by adding information security as another layer of corporate security. This satisfies the fact that information has something to do with all the areas of corporate security: is stored in physical houses, handled by personnel, protected from fire, transported, used abroad and so on.

7.3 A combined model

This new model has been presented in [P4]. There are assets and protection methods in this model. Some methods are mandatory while others can be selected according to the situation at hand.

Assets

An asset is something valuable for an organization. Losing an asset causes either direct or indirect losses for an organization. Some assets may have value in themselves. This means that to replace a lost item one has to buy a new one (e.g. raw material) or something valuable is lost (e.g. money). Another possibility is that the asset is required for normal operation, like machinery or a house. The assets are in the middle of the model in Figure 7.1.

Property is the largest group of assets. It represents all physical assets, like goods, monetary instruments, machinery or buildings. Losing, misusing, accidents, forging and so on may damage these assets.

Information is a non-physical asset. However, it is an important factor of production. Information may have the form of a substance, a tool or a product. Information may have monetary value when bought or sold and also strategic value if it concerns future plans of an organization. Denning uses the terms “operational” and “exchange” value of information [30]. Some information is the result of hard work, like a customer database, while others come from unique thinking, like a new invention. Information may lose its value if it is known by too many people, has deteriorated like a database which includes wrong information, or is not available when needed.

Personnel is the third asset. Strictly speaking, personnel is not independent from the other assets. For a company an employee is a manufacturing device, like a robot. At the same time he is a storage of a remarkable amount of information. However, the reputation of an organization requires taking care of the personnel and thus it constitutes an asset.

Reputation is the fourth asset. We discussed reputation and brand together with trust in Chapter 2.2. Beside of that many shareholders value the reputation of a company very high. A bad reputation lowers the price of shares.

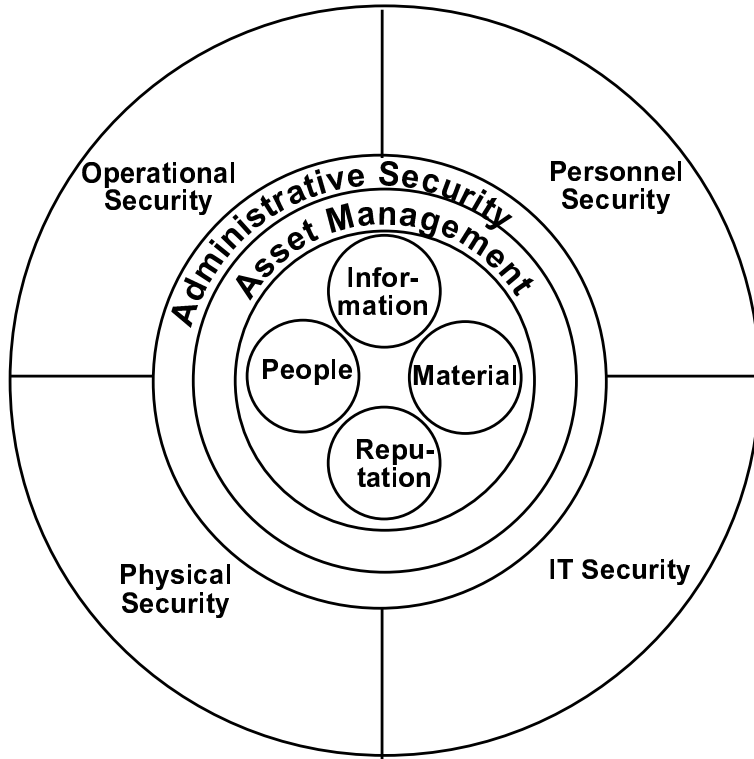


Figure 7.1: The 4 sector model

Mandatory protection methods

There are two mandatory protection methods which, as the name implies, have to be taken care of in every organization. They are placed as the inner layers in the model (Figure 7.1).

Security management is the most crucial part of security. There always has to be a connection between the business and security. Somebody has to define the acceptable risk level for an organization. The risk level defines the goal for security. There has to be a security policy, which defines the target and also the protection methods on a general level. The security functions have to be organized through the whole organization.

Another mandatory method is asset management. Protecting assets is useless if the valuable assets are not known. One can not protect everything against any threat. In addition to identifying the assets one has to classify the reasons why the assets are valuable and against which threats they have to be protected. Efficient asset management consists of a classification scheme which unifies the classification and protection of assets through the organization.

Selectable protection methods

Unlike the mandatory methods one may choose which of these methods produces the best protection for certain assets. One may also combine these methods for best results. Thus, they are in the outer layer of the model. These methods are set as sectors since their weighting may vary according to the situation (Figure 7.1).

Physical security is a basic protection method. Since physical security protects assets from threats coming from the outside only, efficient protection requires several security domains. Physical security may be passive, like walls and fences, or active prevention by guards. Active reactions require a system which finds out if something out of the ordinary happens.

Personnel security is probably the most important sector of security. Since physical security is only capable of protecting assets against outsiders, there is a need to define outsiders and insiders properly. This is the main function of personnel security. Another function is to take care of the knowledge of employees. The employees can not work in secure ways if they do not have enough education and training to manage their work [P1].

Information technology security is actually a counterpart to physical security. Physical security prevents people getting unauthorized access to physical objects, whereas information technology security prevents unauthorized access to objects in the information space. As on the physical side there are passive methods to prevent access, like cryptography and active systems to detect intrusion.

Operational security is more or less the same as quality of work. There are a lot of everyday routines which can be done in a secure or insecure way. The routines must be secure and there must be enough time to work at a secure pace.

The usage of the model

Organizing security according to this model has been relatively easy. According to National Emergency Supply Agency (of Finland) security is a

part of normal work and security related tasks should be done by the same staff as the rest of the work [44]. Most of the methods in this model can easily be assigned to some department of a typical organization.

The personnel security takes care of the hiring and firing procedures and the training of the staff. These procedures belong typically to the personnel department and thus the security measures can also be assigned to that department. Most organizations have a computer department, which is a natural base for the information technology security. The physical security has a natural connection to the premises and a department taking care of those. If we divide the function of an organization into operational and headquarter functions the personnel, computer and premises departments are typically assisting functions located at the headquarter.

The operational functions are the real business of an organization. Operational security is then part of that business. The work at the organization has to be done in secure way and with high quality as stated in Chapter 6.2.

The mandatory methods are discussed in the other chapters of this thesis. Administrative security is security management and it belongs to the general management. It includes organizational issues (Chapter 4) and the reputation of the organization (Chapter 2.2 and 3.1). Asset management is something everybody must do. A systematic method for this is presented in Chapter 8.1.

In the standard case, all these protection methods are required but the balance is formed according to the situation of each organization. At least some personnel security is required to select which employees are allowed to access what assets. Then some physical and/or IT security is needed to prevent unauthorized access and control authorized access. Also some routines are always required to manage security in the everyday work.

The model has been tested in several organizations. The author of this thesis has used it in Finnish Defence Forces and Alma Media Inc., unfortunately those documents are not public. However, there are several other applications of the model (e.g. [59], [78], [97]).

In previous chapters the risk analysis and classification of the assets were found to be essential for security administration. In this chapter we present a systematic method to execute these functions.

8.1 Classification

As we present in chapter 7.3, a classification is an absolute requirement for securing information. Without classification there is no knowledge about which information is worth protecting, why and against what. Previously many classification schemes were based on confidentiality. However, the availability of information may nowadays be more crucial.

For this purpose a new approach, the viable information system, has been introduced. Such a system is capable of maintaining its functionality and ability to produce the required service. [54]

Availability and integrity differ from confidentiality in the sense that the classification is usually done at the system level. Requirements for availability and integrity are set when the system is designed and a normal user does not have to know anything about this. Confidentiality is always present. All the new information has to be classified and everybody may have to take part of this. At least everyone has to apply the rules on how to use classified information.

Even the classification of confidential information has changed. Information is not the same as a document any more. We can not label a paper as secret because there is no paper. Information is located in files in computers and fields in databases. Beside actual data there is metadata which may be as important as the data itself but more difficult to protect.

The classification process itself has changed during the last ten years. In the beginning of the 1990ies information was still stored in paper documents. There were computers and the documents were prepared using them but after that the document was printed out and handled as paper. The classification could be done late in the process, it was possible to leave the document unclassified and classify it after somebody came in and asked for it. This kind of classification is not possible any more. Classification has to be done before a document is saved for the first time. Probably the location of the file and the permissions automatically define who has access to the file. In many cases it is necessary to re-classify a piece of information several times during the lifetime of the information.

In many cases information may be like a spreadsheet, a twodimensional collection of pieces of information. For example, personnel information consists of several columns: name, age, address and so on, there are also several rows: Alice, Bob, Cecilia, ... Classifying this kind of information actually means classifying either the whole file or a view into the file. In principle it should be easy to manage permissions to a database and thus classify a view. Restrictions are, however, difficult to enforce efficiently. Users may collect information from several views and then combine it in

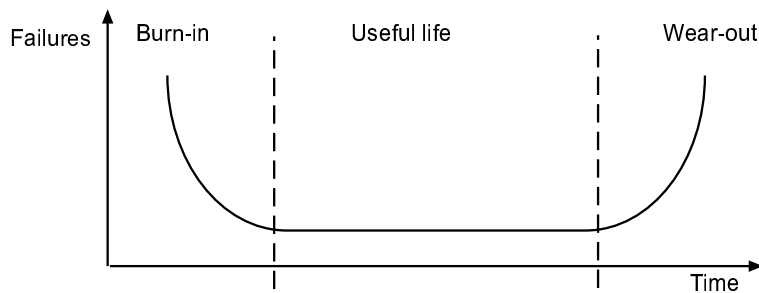


Figure 8.1: “Bathtub” model of reliability [66, p.174]

a manner that was not intended. It is even more difficult to manage a situation where a user has the permission to get information from many records but only when needed. A doctor has to get all the information of a patient and anybody may be a patient. The doctor must not, however, have admission to everybody’s data.

To manage information flows and classifications efficiently a method for handling classification automatically is needed. It should be possible to define a diagram about how the information flows and especially what parts of the information are actually needed in a certain part of a process. Being able to define the needed information makes it possible to keep the classification lower and thus also make the security requirements lower. This is especially important in modern organizations where some of the processes have been outsourced to other companies.

8.2 Analysis

The reliability of electronic components has a failure rate which is called the “bathtub” model because of its shape (figure 8.1). The probability of a failure is higher due to poor assemblies or weak, substandard components, which fail soon after startup. During the useful lifetime the probability of failure is constant. There is a chance of failure but its probability is low. In the end of the lifetime wearout failures will occur. [66]

We suggest that it is possible to use the same model in software components, too. In that case early failures are often due to poor implementation, poorly planned modification and incorrect assumptions about the operating environment. These failure rates may be even higher than those of electronic components. There are also failures within the useful lifetime. They may occur when a new or seldom used input is executed. In the end of the useful lifetime the software needs more modification and the environment has changed [66]. Another explanation would that in the beginning there are several errors in the software. One by one these errors are corrected until no more can be found in normal operation. At that point the useful lifetime begins. In the end of the lifetime changes have to be made to adapt to the changes in other systems and these changes add new errors to the system.

The increased complexity of systems has created a new accident type

Hardware	Software
Caused by deficiencies in design, production and maintenance	Caused by design faults
Due to wear or other energy-related phenomena, warnings are possible	No warnings
Reliability is possible to make better through preventive maintenance	No preventive maintenance
Time related reliability	Reliability grows when errors are detected and corrected
Environmental conditions affect	External conditions do not affect. Internal conditions, like insufficient memory, may affect
Can be predicted from physical bases	Can not be predicted
Can be improved by redundancy	Reliability can be improved by diversity
Failure rates of components are predictable	Reliability of software components is not predictable
Interfaces are visual	Interfaces are conceptual
Uses standard components	Uses proprietary components

Table 8.1: Comparison of hardware and software reliability [57, p.7][108, p.4]

called system accidents [77]. For Example, in conventional industry the intermediate storages have disappeared and several subsystems are coupled tightly together. This makes it more difficult to identify potential hazards because there probably is no specialist who understands the whole process [100].

The increased number of distributed systems causes new possibilities for failures. There may be several hidden dependencies in those systems which are difficult to notice and manage. [71]

For security flaws a taxonomy how-when-where was used to analyze incidents. “How” tells the genesis of an incident and how it got into the system. “When” tells the time of introduction and “where” the location of appearance. [63]

The threat analysis of distributed systems is difficult. There are many components, the environmental conditions of these components vary and the connections between these components are numerous.

8.3 A proposed classification and analyzing system

Classification and threat analysis are processes which can be placed in the same concept. If done systematically both require a proper system description. Classification is a top-down process. Although every piece of information has to be classified when it first comes to the organization, the value of information is recognized top-down. For example the importance of a process is defined according to the business management of an organization. Often the piece of information changes from confidential to secret after a

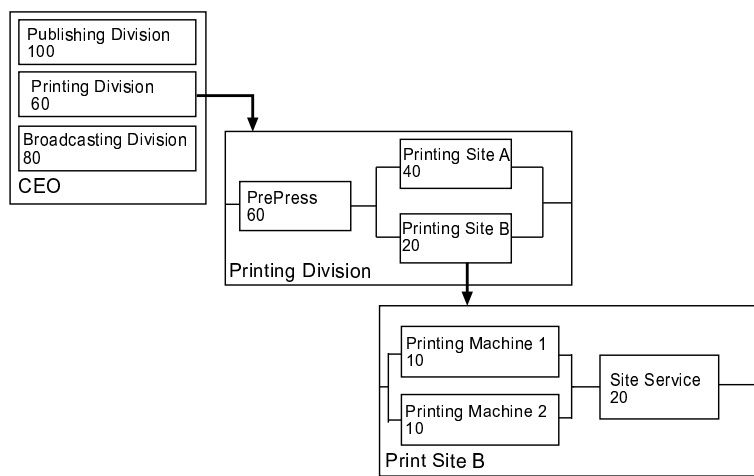


Figure 8.2: Top-down classification

decision of a high-level director when the possibility that something may happen turns to the decision that it will happen.

To manage the flow of information properly the amount of information and its exact classification should be known in all the phases of the process. Protecting the information is easier if there is no unnecessary piece of information which sets the classification higher than it needs to be. The classification of information may be decreased in two ways: horizontally by decreasing the number of fields or the quality of information or vertically by decreasing records or the quantity of information.

Availability can be managed in the same way. If the availability of a certain process is extremely important its criticality can be decreased by bringing in another parallel process to back-up the critical one. Integrity, too, may be improved by adding parallel processes to verify the modification of information.

There are two main principles in the proposed classification scheme: top-down and flow chart. Top-down means that every level of the hierarchy gets the classification from its upper level as in figure 8.2. For Example, the high level management states that the value of the work of the printing division is 60 out of 100. This information is then passed to the printing division. The head of the division analyzes the printing process and defines that the value of the print site B is 20. Again the manager of print site B knows the value of his site for the whole corporation. This stepwise refinement can be continued until there is nothing to be analyzed or the importance of elements drops below the threshold defined in the policy of the corporation.

The model does not require that all the pieces in the flow chart should be in the same organization. The classification sets well defined requirements between organizations when agreements are made.

Another key feature is the flow chart. In figure 8.2 the availability requirements are defined using a flow chart. A box means a part of the process and lines present information flow. When two boxes are parallel they are

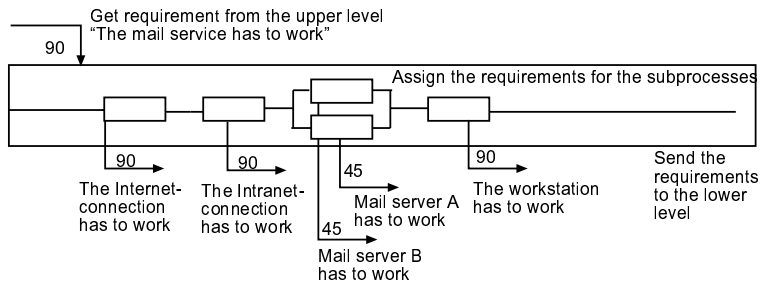


Figure 8.3: Availability flow chart

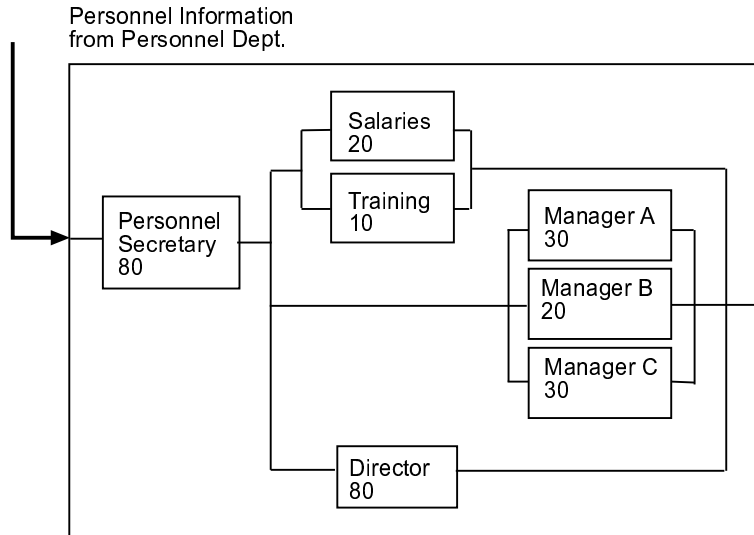


Figure 8.4: Confidentiality flow chart

independent of each other and may back-up each other. If there is a single box it means that there is no alternative process and thus the classification of such a box must be the same as the parent process, like for Site Service at Print Site B. If there are parallel boxes, the classification could be lower, e.g. there are two alternative print sites in the printing division. Site A is bigger and more important than Site B. Another flow chart is presented in figure 8.3.

It is possible to describe confidentiality in the same way. In figure 8.4 a department gets information about its employees from the personnel department of the company. The classification of this information is 80 on a scale of zero to 100. All this information comes to the personnel secretary and the classification of this information is then the same 80. The director of the department gets all the information, too. There are three units in the department, A, B and C. Those units get the information about their employees. Because the number of the employees is smaller from in the whole department the classification is also lower (decreasing by reducing the quantity of information). There are also two common functions

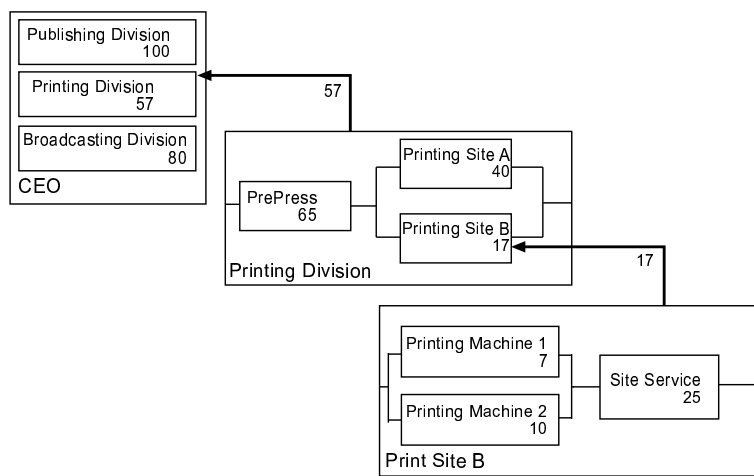


Figure 8.5: Threat analysis

in the department, salaries and training. These get information about all the employees of the department but not all the information and thus the classification is lower (decreasing by reducing the quality of information).

Making these flow charts is a manual operation. Classifying the subprocesses is also a manual operation. As seen in the figures, there is no mathematical function which can be used in classifying. However, this work should be fairly straightforward on one hierarchy level and the results can easily be passed to the lower level for more precise classification.

The same process description may be used when making a threat analysis for an organization. The processes and their relationships are already defined. If the low level threats are analyzed manually it should be possible to calculate higher level threats automatically.

In figure 8.5 we have the same situation as in figure 8.2 earlier. Now Print Site B has analyzed itself and found out that the reliability of Printing Machine 2 is less than required and thus the Print Site B does not meet the requirements. The result propagates to the upper level: Printing Division does not meet its requirements.

There are several possibilities to correct the situation. The manager of Print Site B may notice the situation and increase the reliability of Printing Machine 1 by making some preventive maintenance. This may even happen before the results are reported to Printing Division. Another possibility is that the manager decreases the value of Printing Machine 1 by increasing the capacity of Printing Machine 2 or purchasing a new Printing Machine 3.

If these alternatives are not possible for the site manager he has to report the bad numbers to Printing Division. The manager of the division has the same three alternatives: trying to improve the situation of Printing Site B, decreasing the importance of Printing Site B or reporting the unsuccessful result to the CEO. Improving the results means accepting higher cost and decreasing the importance means either improving Printing Site A or getting a new Printing Site C.

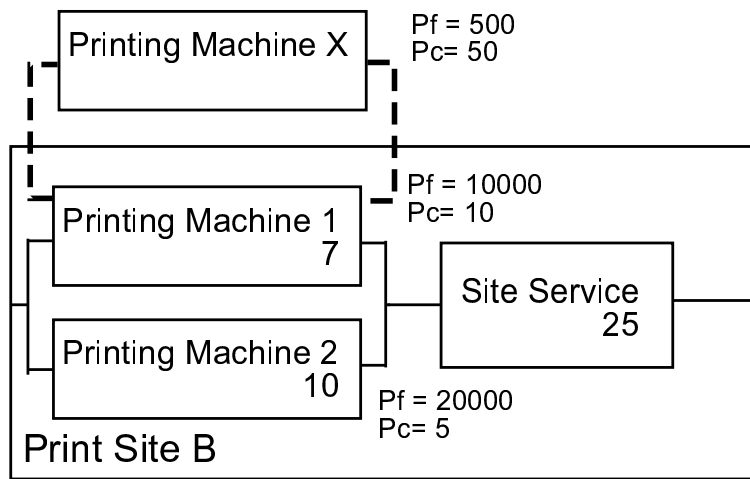


Figure 8.6: The cost model

The same analysis can be made according to confidentiality or integrity requirements. In these cases failing the requirements means that the data should not be passed to the failing subprocess until the requirements are met. It is also possible to decrease the classification of the data by decreasing either the quantity or the quality of the data.

On the low level, where availability is based on reliability of the system, it may be possible to improve the availability by adding parallel back-up systems. In accordance with the table 8.1 this means either redundant hardware or diversified software. The bathtub model (figure 8.1) should also be taken into account. In the high-failure phases there should be a reliable back-up.

On higher levels the back-up systems may be too expensive, like a new printing site in figure 8.5. However it may be possible to buy back-up capacity from other companies or otherwise arrange the possibility for extra capacity if needed.

8.4 The cost model

The method also gives the possibility to estimate the cost of back-up arrangements. These costs depend on the static cost of the back-up arrangement and the unit prices of back-up production.

One back-up arrangement is presented in figure 8.6. Print Site B has an agreement with another local print shop which promises to sell the needed printing capacity in an emergency case. This company requires a fixed price of 500 in a month for reserving the capacity and 50 as a unit price for each printed unit. On their own Printing Machine 1 the corresponding prices are 10000 a month and 10 per unit. If the probability of failure in Printing Machine 1 is 7%, it is possible to calculate the cost of the back-up capacity. The fixed prices must always be counted in and the unit prizes according to the probability. In this case $Pt = 10,000 + 500 + N(0.93 * 10 + 0.07 * 50)$.

If the number of units in a month is 100, the cost of Printing Machine 1 is 11,780. Without a back-up arrangement and with perfect reliability the cost would be 11,000.

8.5 Comments on the method

This method has several advantages. It

- systematizes classification and threat analysis
- reuses the results (when a process is analyzed the results may be used in several higher level systems)
- the work of classifying and analyzing may be distributed to several organization units
- makes the changes local and the flowchart can be recalculated automatically
- gives the possibility of local corrective action
- clarifies the requirements when making contracts between units or with subcontractors.

There are two main disadvantages: the lack of a supporting system and the initial cost. There is currently no system supporting this kind of modeling. There should be such a system, capable of presenting systems using flowcharts and making some calculations automatically. Even in that case there is quite a lot of initial work when the target system is analyzed and stored into this supporting system.

9.1 Summary

In this thesis there are three parts. In the beginning, chapters two to six, we have selected four different views on security. The user's view concentrates on the security needs of users when they use services, especially on the Internet. The key words are trust, privacy and capability. In the developer's view these user's requirements are taken into account when developing information systems. The methods are security profiling (brand) and usability requirements. The security and usability in the lifecycle of a product are also considered. There are also a few words about the development process itself and the security in it. In the organization's view another aspect of a brand — the business model — is presented. The ways of organizing security are also considered as well as the effect of historical reasons which lead to the current security situation. In the scientist's view, some conferences are analyzed to find out what aspects of information security have been the object of scientific interest. Finally, there are some considerations and suggestions in connection with other areas, like quality.

In the second part, chapter seven, we analyze two current security models and present a new one combining the earlier ones in a logical way. This new model has been tested using it as a base of security policy in two nationwide organizations. We have also conducted a development program for information security professionals using the same model and currently we are refining two university curricula according to the model.

In the third part, chapter eight, two practical problems in organizations are presented. They are classification and threat analysis. A generic solution to these problems is also suggested.

9.2 The results

Through this thesis there are three main themes: trust, systematic work and education. The main results are

- Security is an essential part of the business model. A company has to have a vision about what customer segment it is targetting and what are the security requirements in that segment. (Chapters 2.2, 3.1, 7.1 and [P4])
- Security is an essential part of new products. After the business model is defined all the new products must meet the required security level. In addition to this users must be able to use the products without fear of failures. (Chapters 2.2, 2.5, 3.1, 3.2, 6.2 and [P1])
- Security depends on the culture of an organization. Security is not only written policies and expensive devices. It is part of the employee's everyday work and the overall culture of an organization has to encourage security. (Chapters 2.5, 3.3, 4 and [P1])

- Corporate and information security are the same. The same policy and methods must be applied to protect all the assets including information. (Chapters 6.1, 7, [P4] and [P6])
- Education is an important part of security. Without education people can not do their work properly. At the same time “too smart” people may cause other problems if the culture in the organization allows that. (Chapters 2.3, 2.5, 3.1, 4.3, 4.4, [P1], [P2], [P3])

Trust is a requirement when new economy emerges. If there is no trust, there is no electronic commerce, either. Users’ trust for the systems may be increased by good usability, education and reputation. Stakeholders’ trust for the systems may be increased by proper management of the development process and systematic classification and threat analysis. Good understanding of systems and security related matters increases users’ trust to the systems and also decreases the number of mistakes, which again increases trust.

In organizations understanding the nature of security makes it possible to organize security functions properly between business functions. Security is not a separate function with a security policy and security manager who comes once a year to see if the rules are applied properly. Security is a decision that it is reasonable to prevent losses beforehand instead of spending time and money to find out afterwards who did what and how it can be corrected. It can also be a strategic choice to profile oneself as a secure company and therefore to be able to get new customers or a better price for one’s products.

9.3 Future work

We have noticed that there are many similarities between physical and information technology security. Thus we assume that these areas grow even closer in the future. The traditional physical security terms and methods will be adopted into the computer area. We suggest that some new methods should be developed to manage the “information space” in the same manner as the “physical space”.

The hierarchy of needs as presented by Maslow [69] is not applicable to the “information space” since the security needs in that hierarchy refer to very physical needs. However, these same elements exist in the “information space”, too. We suggest that the hierarchy of needs should be upgraded to this area.

Security standards are designed for business use. We suggest that there should be a consumer standard, too. Such a standard (with certificates) makes it possible for an ordinary consumer to evaluate Internet products and thus increases the consumer’s trust in the product.

- [1] Creating Confidence in Information Processing; Elsevier Advanced Technology, GB; 1991.
- [2] Security and Protection of Information Processing Systems; Curacao; 1994.
- [3] British Standard, Code of Practise for Information Security Management, BS7799:1995; ISO; ISBN 0-580-23642-0; 1995.
- [4] The New Webster's Encyclopedic Dictionary of the English Language; Gramercy Books, USA; ISBN 0-517-18367-6; 1997.
- [5] Cobit framework 2nd edition; 1998.
URL <http://www.cobit.com>
- [6] Etukortit (loyalty cards); an article in consumer newspaper about different loyalty cards (in Finnish), referenced in 25.5.2002; 1998.
URL http://kuluttajat-konsumennterna.fi/docs/kuluttajapuntari/1998_01_02/kortit.html
- [7] Valtioneuvoston periaatepäätös tietoturvallisuudesta (Council-of-Ministers Policy-Decision on the Development of Information Security); Ministry of Finance, Finland; 1998.
- [8] eCommerce Trust Study; Cheskin Research and Sapient/Studio Archetype, UK; 1999.
- [9] Security architecture for future mobile terminals and applications; eU-project IST-2000-25350, referenced in 24.5.2002; 2001.
URL <http://www.ist-shaman.org>
- [10] Yritysten vuosittaiset turvamenot keskimäärin 2500mk henkilöä kohden; referenced in 28.5.2002; 2001.
URL <http://www.finnsecurity.fi/uutiset/index.html>
- [11] Cert/cc statistics 1988-2002; referenced in 24.5.2002; 2002.
URL <http://www.cert.org/stats>
- [12] European computer driving licence; referenced in 1.9.2002; 2002.
URL <http://www.ecdl.co.uk/individ/index.html>
- [13] The Finnish Social Protection System 2001; Ministry of Social Affairs and Health, Finland; 2002.
- [14] International federation for information processing; referenced in 1.9.2002; 2002.
URL <http://www.ifip.org>
- [15] Openssh; referenced in 1.9.2002; 2002.
URL <http://www.openssh.org>

- [16] ANNE ADAMS, MARTINA ANGELA SASSE; Users are not the enemy; *Communications of the ACM* 42:40–46; 1999.
- [17] PHILIP ANDERSON, MICHAEL L. TUSHMAN; Managing through cycles of technological change; in *Managing Strategic Innovations and Change* (eds. MICHAEL L. TUSHMAN, PHILIP ANDERSON); page 45–52; Oxford University Press, USA; ISBN 0-19-510010-7; 1997.
- [18] ROSS ANDERSON; *Security Engineering*; John Wiley & Sons, USA; ISBN 0-471-38922-6; 2001.
- [19] C. BADEN-FULLER, M. PITT; *Strategic Innovation*; Routledge, GB; 1996.
- [20] BORIS BALACHEFF, LIQUN CHEN, DAVID PLAQUIN, GRAEME PROUDLER; A trusted process to digitally sign a document; in *Proc. of New Security Paradigm Workshop 2001* (eds. V. RASKIN, C.F. HEMPELMANN); page 79–88; ACM, USA; ISBN 1-58113-457-6; 2001.
- [21] DIRK BALFANZ, EDWARD W. FELTEN; Hand-held computer can be better smart cards; in *Proc. of USENIX Security '99*; USA; 1999.
- [22] RICHARD BASKERVILLE; A taxonomy for analyzing hazards to information systems; in *Information Systems Security* (eds. SOKRATIS K. KATSIKAS, DIMITRIS GRITZALIS); page 167–176; Chapman & Hall, GB; ISBN 0-412-78120-4; 1996.
- [23] RICHARD BASKERVILLE, J. PRIES-HEJE; Packaging information security safeguards; in *Global IT Security* (eds. GYÖRGY PAPP, REINHARD POSCH); page 549–553; Austrian Computer Society, Austria; ISBN 3-85403-116-5; 1998.
- [24] FRANK M. BASS; A new product growth model for consumer durables; *Management Science* 15:215–227; 1969.
- [25] B.W. BOEHM; Software risk management: Principles and practises; *IEEE Software* 8:13–24; 1991.
- [26] WILLIAM J. CAELLI (ed.); *Computer Security in the Age of Information*; North-Holland Publishing Company, USA; ISBN 0-444-88324; 1988.
- [27] WILLIAM J. CAELLI; Certificate based pki and b2b e-commerce: Suitable match or not?; in *Trusted Information, the New Decade Challenge* (eds. MICHEL DUPUY, PIERRE PARADINAS); Kluwer Academic Publisher, USA; ISBN 0-7923-7389-8; 2001.
- [28] T. CLAYTON, G. TURNER; Brands, innovation and growth; in *From Knowledge Management to Strategic Competence: Measuring Technological Markets and Organizational Innovation* (ed. JOE TIDD); Imperial College, GB; 2000.

- [29] R. COURTNEY; Security risk assessment in electronic data processing; in Proc. of AFIPS Conference Proceedings; NCC, USA; 1977.
- [30] DOROTHY E. DENNING; Information Warfare and Security; ACM Press Books, USA; ISBN 0-201-43303-6; 1999.
- [31] J.R. DORRONSORO, F.GINEL, C. SGNCHZ, C.S.CRUIZ; Neural fraud detection in credit card operations; *IEEE Transactions on Neural Networks* 8:827–834; 1997.
- [32] E. GRAHAM DOUGALL, DARREN JONES (eds.); Computer Security: Discovering Tomorrow; Canada; 1993.
- [33] MICHEL DUPUY, PIERRE PARADINAS (eds.); Trusted Information, the New Decade Challenge; Kluwer Academic Publisher, USA; ISBN 0-7923-7389-8; 2001.
- [34] JAN P. ELOFF, SEBASTIAN H. VON SOLMS (eds.); Security - The Next Decade; Chapman & Hall, GB; ISBN 0-412-64020-1; 1995.
- [35] GUY G. GABLE ET.AL. (ed.); Security and Control: From small Systems to Large; 1992.
- [36] HORST FEISEL; Cryptography and computer privacy; *Scientific American* page 15–23; 1973.
- [37] JAMES H. FINCH, E. GRAHAM DOUGAL (eds.); Computer Security: A Global Challenge; North-Holland Publishing Company, USA; ISBN 0-444-87618-9; 1984.
- [38] HAMPTON C. GABLER, WILLIAM T. HOLLOWLL; The aggressivity of light trucks and vans in traffic crashes; referenced in 1.9.2002; 1998.
URL <http://www-nrd.nhtsa.dot.gov/departments/nrd-11/aggressivity/980908/980908.html>
- [39] M.ADEED GHONAIMY, MAHMOUD T. EL-HADIDI, HEBA K. ASLAN (eds.); Security in the Information Society; Kluwer Academic Publishers, USA; ISBN 1-4020-7030-6; 2002.
- [40] HENTY GLEITMAN; Psychology; W.W.Norton & Company, USA; ISBN 0-393-95955-4; 1991.
- [41] JANE B. GRIMSON, HANS-JUERGEN KUGLER (eds.); Computer Security: The Practical Issues in a Troubled World; North-Holland Publishing Company, USA; ISBN 0-444-87801-7; 1985.
- [42] JONATHAN GRUDIN; The case against user interface consistency; *Communication of the ACM* 32:1164–1173; 1989.
- [43] JOANN T. HACKOS, JANICE C. REDISH; User and Task Analysis for Interface Design; John Wiley & Co, USA; ISBN 0-471-17831-4; 1998.

- [44] PENTTI HARMANEN; Tietojenkäsittelyn turvaaminen tietoyhteiskunnassa; PTS, Finland; ISBN 951-53-0990-5; 1996.
- [45] DEBRA S. HERRMANN; Software Safety and Reliability; IEEE Computer Society Press, USA; ISBN 0-7695-0299-7; 1999.
- [46] LAYNE HESSE, CLIFTON L. SMITH; Core curriculum in security science; in Proceedings of the 5th Australian Security Research Symposium (ed. HELEN ARMSTRONG); page 87–104; Edith Cowan University, Australia; ISBN 0-7298-0497-06; 2001.
- [47] GEERT HOFSTEDE; Hierarchical power distance in forty countries; in Organizations Alike and Unlike: Towards a Comparative Sociology of Organizations (eds. D.J.LANNERS, D.J. HICKSON); page 97–119; Routledge, GB; 1979.
- [48] JAAKKO HOLMEN; User profiling and Classification for Fraud Detection in Mobile Communication Networks; Acta Polytechnica Scandinavica, Finland; ISBN 951-666-555-1; 2000.
- [49] HUOMO, SUNDQUIST, MUHONEN, SOINI; Kansalliseen tietoturvallisuusstrategiaan liittyvä tietoturvakatsaus; HM & V Research Oy, Finland; 2002.
- [50] N. JAYARATHA; Understanding and evaluating methodologies: NIMSAD, a systemic framework; McGraw & Hill, UK; 1994.
- [51] MINISTRY OF JUSTICE (FINLAND); Henkilötietolaki, 561/1999; 1999.
- [52] MINISTRY OF JUSTICE (FINLAND); Laki yksityisyyden suojasta työelämässä, 477/2001; 2001.
- [53] KRISTIINA KARVONEN, URSULA HOLMSTRÖM; Expressing trust; in TBA; 1999.
- [54] MARIA KARYDA, SPYROS KOKOLAKIS, EVANGELOS KIOUNTOUZIS; Redefining information systems security: Viable information systems; in Trusted Information: The New Decade Challenge (eds. MICHEL DUPUY, PIERRE PARADINAS); page 453–468; Kluwer Academic Publisher, USA; ISBN 0-7923-7389-8; 2001.
- [55] SOKRATIS K. KATSIKAS, DIMITRIS GRITZALIS (eds.); Information Systems Security; Chapman & Hall, GB; ISBN 0-412-78120-4; 1996.
- [56] ERKKI KAUKANEN; Lännen sankari on idän luuseri (a western hero is an eastern loser); *Tiede* 2002.
- [57] SAMUEL.J. KEENE; Comparing hardware and software reliability; *ASQ Reliability Review* 14:5–7; 1994.
- [58] P. KIRSCH, H. WEIDNER, K. BAUKNECHT; Secure conception of internet services; in Global IT Security (eds. GYÖRGY PAPP, REINHARD POSCH); page 477–483; Austrian Computer Society, Austria; ISBN 3-85403-116-5; 1998.

- [59] HEIKKI KONTSAS; Turvallisuusauditointi puolustusvoimien turvallisuusyksiköissä (security audit in the security units of Finnish defence forces); in Tutkielmajulkaisu, 6. Turvallisuusjohdon koulutusohjelma (Proceedings of 6th development program for security managers); Dipoli, Helsinki University of Technology, Finland; ISBN In Print; 2002.
- [60] HILLE KOSKELA; Bold walk and breakings': Women's spatial confidence versus fear and violence; *Gender, Place and Culture* 4:301–319; 1997.
- [61] HILLE KOSKELA; Fear, Control and Space; Publicationes Instituti Geographici Universitatis Helsingiensis, Finland; ISBN 951-45-4631; 1999.
- [62] S. KOWALSKI; Computer ethics and computer abuse: A longitudinal study of Swedish university students; in Proc. of IFIP TC11 6th International conference on Information systems security; Finland; 1990.
- [63] CARL E. LANDWEHR, ALAN R. BULL, JOHN P. MCDERMOTT, WILLIAM S. CHOI; A taxonomy of computer program security flaws; *ACM Computing Surveys* 26:211–254; 1994.
- [64] T. LANE, C.E. BROADLEY; Sequence matching and learning in anomaly detection for computer security; in Proc. of AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management; USA; 1997.
- [65] JUSSIPEKKA LEIWO, S. HEIKKURI; An analysis of ethics as foundation of information security in distributed systems; in Proc. of 31st Hawaiian International Conference on Systems Sciences; USA; 1998.
- [66] NANCY G. LEVESON; Safeware - system safety and computers; Addison Wesley Publishers, GB; ISBN 0-201-11972-2; 1995.
- [67] VIVIEN K.G. LIM, THOMPSON S.H. TEO, GEOK LENG LOO; How do i loaf here? let me count the ways; *Communications of the ACM* 45:66–70; 2002.
- [68] ADÉLE MARTINS, JAN ELOFF; Information security culture; in Security in the Information Society (eds. M.ADEED GHONAIMY, MAHMOUD T. EL-HADIDI, HEBA K. ASLAN); page 203–214; Kluwer Academic Publishers, USA; ISBN 1-4020-7030-6; 2002.
- [69] ABRAHAM H. MASLOW; Toward a Psychology of Being; D.van Nostrand Company, USA; 1968.
- [70] N. MEADE; The use of growth curves in forecasting market; *Journal of Forecasting* 3:429–451; 1984.
- [71] PETER G. NEUMANN; Computer Related Risks; ACM Press, USA; ISBN 0-201-55805; 1995.

- [72] JACOB NIELSEN; Usability Engineering; Academic Press, USA; ISBN 1-12-518406-9; 1993.
- [73] J. NUKARI, M. FORSELL; Suomen ohjelmistoteollisuuden kasvun strategiat ja haasteet; in Teknologiakatsaus 67/99; TEKES, Finland; 1999.
- [74] RAYMOND R. PANKO, HAZEL GLENN BEH; Monitoring for pornography and sexual harassment; *Communications of the ACM* 45:84–87; 2002.
- [75] GYÖRGY PAPP, REINHARD POSCH (eds.); Global IT Security; Austrian Computer Society, Austria; ISBN 3-85403-116-5; 1998.
- [76] ROBERT PEDLOW; Making electronic commerce usable: The role of usability in developing web based electronic commerce systems; in Proc. of 17th International Symposium on Human Factors in Telecommunication (ed. LEIF ELSTRØM); page 201–208; Denmark; 1999.
- [77] CHARLES PERROW; Normal Accidents: Living with High-Risk Technology; Basic Books Inc., USA; 1984.
- [78] JUSSI PESONEN; Pk-yrityksen riskien ominaispiirteitä ja kokonaisvaltaisen riskienhallinnan toimintamalli (the special features of risks in small and medium size companies and how to manage them); in Tutkielmajulkaisu, 6. Turvallisuusjohdon koulutusohjelma (Proceedings of 6th development program for security managers); Dipoli, Helsinki University of Technology, Finland; ISBN In Print; 2002.
- [79] MARKKU PESONEN; Yrityksen turvallisuusjärjestelyt (Security Arrangements of a Company); Yliopistopaino, Finland; ISBN 952-90-4705-3; 1993.
- [80] LEILA POHJOLAINEN; Private discussion; 2002.
- [81] SIHAN QING, JAN P. ELOFF (eds.); Information Security for Global Information Infrastructures; Kluwer Academic Publisher, USA; ISBN 0-7923-7914-4; 2000.
- [82] JORMA RAHKONEN; K-kaupat kasvattivat markkinaosuuttaan keski-suomessa; an article in a newspaper about market shares of shops and amount of loyalty cards (in Finnish), referenced in 25.6.2002; 1998. URL <http://lehti.keskisuomalainen.fi/s1/1998-05/26/-tal/kxkaupat.htm>
- [83] MERJA RANTA-AHO, M. KÖYKKÄ, R. OLLIKAINEN; Connections, locations and shared workplaces. what should the user understand about network services for on-line collaboration?; in People and Computers XIV - Usability or Else! (eds. S. MCDONALD, Y. WAERN, G. COCKTON); Springer Verlag, GB; 2000.
- [84] J. RASMUSSEN (ed.); What Can Be Learned from Human Error Reports?, Changes in Working Life; John Wiley & Sons, USA; 1980.

- [85] J. RYAN, M. LING, R. MIIKKULAINEN; Intrusion detection with neural networks; in Proc. of AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management; USA; 1997.
- [86] JOC SANDERS, EUGENE CURRAN; *Software Quality*; Addison Wesley Publishers, GB; ISBN 0-201-63198-9; 1994.
- [87] JARNA SAVOLAINEN; DIA-kunnan hyvinvointi ja elämänhallinta; TEK, Finland; ISBN 952-5005-50-X; 2000.
- [88] THOMAS SCHLIENGER, STEPHANIE TEUFEL; Information security culture, the socio-cultural dimension in information security management; in *Security in the Information Society* (eds. M.ADEED GHONAIMY, MAHMOUD T. EL-HADIDI, HEBA K. ASLAN); page 191–202; Kluwer Academic Publishers, USA; ISBN 1-4020-7030-6; 2002.
- [89] GEORG SCHYCUDA; Users and Data Protection in Electronic Commerce; 231–240 pages; Proc. of 17th International Symposium on Human Factors in Telecommunication, Denmark; 1999.
- [90] R. SEKAR, C.R. RAMAKRISHNAN, I.V. RAMAKRISHNAN, S.A. SMOLKA; Model carrying code (mcc) a new paradigm for mobile-code security; in Proc. of New Security Paradigm Workshop 2001 (eds. V. RASKIN, C.F. HEMPELMANN); page 23–32; ACM, USA; ISBN 1-58113-457-6; 2001.
- [91] B.J. SELIG; Technology’s impact on risk; *Risk Management* 1993.
- [92] KENG SIAU, FIONA FUI-HOON NAH, LIMEI TENG; Acceptable internet use policy; *Communications of the ACM* 45:75–79; 2002.
- [93] KARL SIGMUND, ERNST FEHT, MARTIN A. NOWAK; The economics of fair play; *Scientific American* 2002.
- [94] CLAIRE A. SIMMERS; Aligning internet usage with business priorities; *Communications of the ACM* 45:71–74; 2002.
- [95] F.J. SISTI, S. JOSEPH; *Software Risk Evaluation Method Version 1.0*; Software Engineering Institute, CMU, USA; 1994.
- [96] JILL SLAY, GERALD QUIRCHMAYR; The role of culture in the development of global e-commerce systems; in *Information Systems: The e-Business Challenge* (ed. ROLAND TRAUNMÜLLER); page 101–115; KluwerAcademic Publishers, USA; ISBN 1-4020-7174-4; 2002.
- [97] MARTTI SOUDUNSAARI; Palvelutoimistojen turvallisuusasioiden seuranta- ja kehittämisjärjestelmä laatu-järjestelmän osana (security audit and development as a part of quality in branch offices); in *Tutkielmajulkaisu, 6. Turvallisuusjohdon koulutusohjelma* (Proceedings of 6th development program for security managers); Dipoli, Helsinki University of Technology, Finland; ISBN In Print; 2002.

- [98] M.E.M. SPRUIT; Competing against human failing; in *Global IT Security* (eds. GYÖRGY PAPP, REINHARD POSCH); page 392–404; Austrian Computer Society, Austria; ISBN 3-85403-116-5; 1998.
- [99] RAINO ÖSTLUND, JUSSI HEINO, LEENA PAARTOLA, MIKKO RÄSÄNEN; *Road Traffic Accidents 1999*; Statistics Finland and Central Organization for Traffic Safety in Finland, Finland; ISBN 951-727-799-7; 2000.
- [100] JOUKO SUOKAS; *On the reliability and validity of safety analysis*; Technical Research Center of Finland, Finland; 1985.
- [101] K. TAN; The application of neural networks to unix computer security; in *Proc. of 1995 IEEE International Conference on Neural Networks*; USA; 1995.
- [102] MATTI TENHUNEN; Private discussion; 1992.
- [103] JOE TIDD, JOHN BESSANT, KEITH PAVITT; *Managing Innovation*; John Wiley & Sons, USA; ISBN 0-471-49615-4; 2001.
- [104] T. TRYFONAS, EVANGELOS KIOUNTOUZIS; Security concerns for contemporary development practises; in *Trusted Information, The New Decade Challenge* (eds. MICHEL DUPUY, PIERRE PARADINAS); page 421–436; Kluwer Academic Publisher, USA; ISBN 0-7923-7389-8; 2001.
- [105] ANDREW URBACZESKI, LEONARD M. JESSUP; Does electronic monitoring of employee internet usage work; *Communications of the ACM* 45:80–83; 2002.
- [106] V.A.FÅK (ed.); *Security*; North-Holland Publishing Company, USA; ISBN 0-444-86669-8; 1983.
- [107] TEEMUPEKKA VIRTANEN, TIMO KIRAVUO, RISTO HEINONEN, ANTTI HOLMROOS, MIKAEL KIVINIEMI, ARI SAAPUNKI, TUOMO SALMINEN, TIMO TUOMAILA; *Valtion Internetin käyttö- ja tietoturvallisuussuositus (Guidelines for Internet-usage and -security for administration)*; Ministry of Finance, Finland; 1998.
- [108] ELLEN WALKER; Bridging the software/hardware reliability gap; *RAC Journal* 4; 1996.
- [109] JIANZHONG WU, ROBERT AXELROD; How to cope with noise in the iterated prosiner's dilemma; *Journal of Conflict Resolution* 39; 1995.
- [110] LOUISE YNGSTRÖM, JAN CARLSEN (eds.); *Information Security in Research and Business*; Chapman & Hall, GB; ISBN 0-412-81781-2; 1997.
- [111] MARY ELLEN ZURKO; Tracking influence through citation index comparisons and preliminary case studies; in *Proc. of New Security Paradigm Workshop 2001* (eds. V. RASKIN, C.F. HEMPELMANN); page 115–118; ACM, USA; ISBN 1-58113-457-6; 2001.