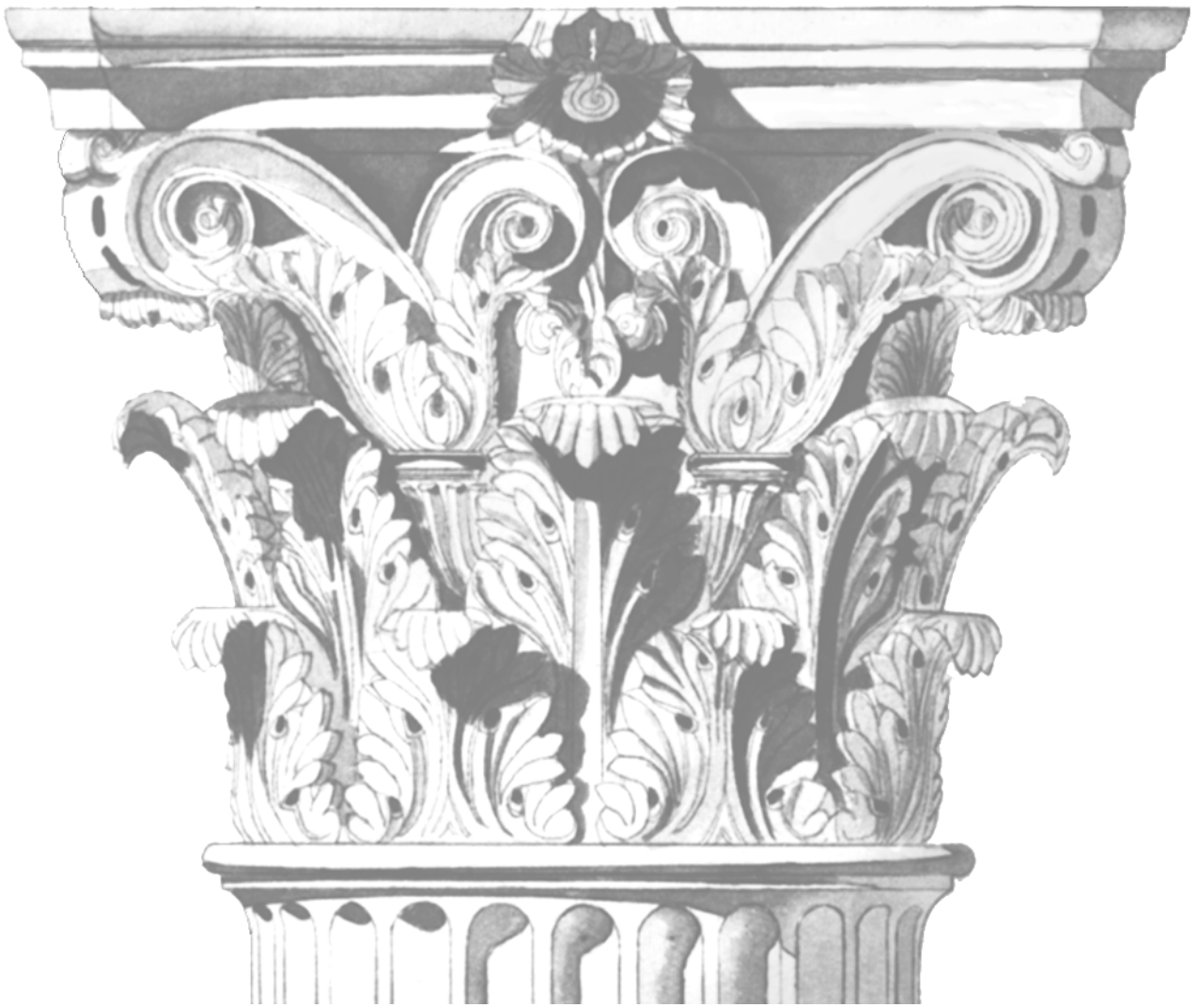
DESIGNING SECURE INFORMATION SYSTEMS AND SOFTWARE

Critical evaluation of the existing approaches and a new paradigm

MIKKO SIPONEN

Department of Information Processing Science and Infotech Oulu, University of Oulu

OULU 2002



MIKKO SIPONEN

DESIGNING SECURE INFORMATION SYSTEMS AND SOFTWARE

Critical evaluation of the existing approaches and a new paradigm

Academic Dissertation to be presented with the assent of the Faculty of Science, University of Oulu, for public discussion in Raahensali (Auditorium L10), Linnanmaa, on August 24th, 2002, at 12 noon.

OULUN YLIOPISTO, OULU 2002

Reviewed by
Associate Professor Gurpreet Dhillon
J. Mack Robinson Distinquished Professor Detmar W. Straub

ISBN 951-42-6790-7 (URL: http://herkules.oulu.fi/isbn9514267907/)

ALSO AVAILABLE IN PRINTED FORMAT
Acta Univ. Oul. A 387, 2002
ISBN 951-42-6789-3
ISSN 0355-3191 (URL: http://herkules.oulu.fi/issn03553191/)

OULU UNIVERSITY PRESS
OULU 2002

Siponen, Mikko, Designing secure information systems and software Critical evaluation of the existing approaches and a new paradigm
Department of Information Processing Science, University of Oulu, P.O.Box 3000, FIN-90014 University of Oulu, Finland, Infotech Oulu, University of Oulu, P.O.Box 4500, FIN-90014 University of Oulu, Finland
Oulu, Finland
2002

Abstract

This dissertation is composed of three contributions. First, it recognizes a set of key security issues for information systems (IS), and examines the extent to which these issues have been studied and resolved by existing research efforts. Second, it analyses and discusses the existing approaches for designing secure information systems (SIS), shedding light on their underlying foundations. Third, based on the findings, a framework is put forth, addressing the fundamental shortcomings of the existing SIS design approaches. A meta-notation for adding security into IS development methods is presented as a framework-based example. An action research intervention is accomplished to test the relevance, suitability and feasibility of the meta-notation in practice. Overall, this dissertation sets forth a novel approach for extending security in IS/software development methods.

Keywords: IS security, development of secure IS

Preface

I wish to thank my supervisor, Professor Harri Oinas-Kukkonen, at the Department of Information Processing Science, University of Oulu, Finland, for his important comments concerning the dissertation and for his support during my postgraduate studies.

I would also like to thank the preliminary examiners of this dissertation, namely J. Mack Robinson Distinguished Professor Detmar W. Straub, Department of Computer Information Systems, J. Mack Robinson College of Business, Georgia State University, Atlanta, USA, and Professor Gurpreet Dhillon, MIS Department, at the College of Business, University of Nevada Las Vegas, USA for their insightful suggestions and comments on the thesis.

Professor Juhani Iivari at the Department of Information Processing Science, Pekka Abrahamsson, Ph.D. at VTT in Oulu and docent Kari Väyrynen, Ph.D. at the Department of History, University of Oulu, have always been available to provide important comments and guidance during my postgraduate years. I am greatly indebted to them for these comments.

Professor Richard L. Baskerville at the Department of Computer Information Systems, J. Mack Robinson College of Business, Georgia State University, Atlanta, USA, has particularly contributed to the fourth chapter of this dissertation. The action research intervention, described in chapters 4.1 and 4.2 are based on an unpublished paper "A Paradigm For Extending Security In IS/Software Development Methods" co-authored by Professor Baskerville. I would like to thank the faculty members of the Department of Computer Information Systems, Georgia State University, Atlanta, USA, for their hospitality during my visit in the Department during the academic year 2000-2001.

I would also like to acknowledge all the members of the VRFlow and OWLA research projects, particularly Toni Alatalo and Virpi Kurkela.

This research was financed by the Infotech Graduate School, National Technology Agency of Finland, the HYTEC Research Lab at the Virgin Research Group, the VRFlow and OWLA research projects, the Oulu University Foundation, and the Department of Information Processing Science at the University of Oulu. Chapter four of this thesis, excluding the empirical intervention, was mainly written while I was with the Department of Computer Information Systems at the J. Mack Robinson College of

Business, Georgia State University, Georgia, USA. I also thank Idea Group Inc. and Kluwer Academic Publishers, who hold the copyrights of the original papers (I-V), for giving me permission to reprint the original texts as a part of my dissertation.

Finally, but not the least, I would like to thank my wife, Tuula, and my parents, for their immense support throughout this PhD research process.

Oulu, July 2002 Mikko Siponen

Abbreviations

BS7799	British Standard 7799
GASSP	Generally Accepted System Security Principles
IS	Information System
ISSD	Information System and Software Development
ITSEC	Information Technology Security Evaluation Criteria
SIS	Secure Information System
SW	Software

List of original papers

This dissertation includes five original research papers, which are referred to in the text by their roman numerals.

I Siponen MT & Oinas-Kukkonen H (2002) A survey of information systems security issues and respective research contributions. Submitted for publication.

II Siponen MT (2001a) A Paradigmatic analysis of conventional information security management/development approaches: implications for research and practice. Reprinted from the Proceedings of 16th International Conference on Information Systems Security, Paris, France, p 438-452.

III Siponen MT (2001b) A Survey of the recent IS security development approaches: descriptive and prescriptive implications. Reprinted from: In: Dhillon G (eds) Information Security Management - Global Challenges in the Next Millennium. Idea Group Publications Hershey, PA, p 101-124.

IV Siponen MT (2002a) Maturity criteria for developing secure IS and software: limits, and prospects. Reprinted from: the Proceedings of 17th International Conference on Information Security, Cairo, Egypt, p 91-108.

V Siponen MT & Baskerville R (2001) A new paradigm for adding security into IS development methods. Reprinted from: In: Eloff J, Labuschagne L, von Solms R & Dhillon G (eds) Advances in information security management and small systems security. Kluwer Academic Publishers, Norwell, MA, p 99-111.

Contents

1 Introduction

Information security, which may be defined in terms of confidentiality, integrity and availability (*e.g.*, ITSEC 1991, Parker 1981, 1998), has a long history. Encryption, for instance, has been used since the invention of writing (Kahn 1996), long before computers came into existence. Recently, the importance of information security considerations has increased due to the expanded use of the Internet by institutions, business organizations and individuals on the one hand and by criminals and abusers on the other hand (*e.g.*, Dean *et al*. 1996, Bishop *et al*. 1997, Klander 1997, Straub & Welke 1998, Cullinane 1999, Palmer *et al*. 2000). In fact, technically-oriented scientists and computer science researchers have responded rapidly to this increased importance of information security with a huge number of technical protection solutions in the areas of computer and communications security. Thus, from the technical point of view, there are a large number of solutions available. However, from the information system (IS) point of view (*cf*., Davis 1999, 2000) only limited solutions have been presented: "serious research into the nature of the management of information systems security is scarce" (Baskerville 1994 p. 385).

One of the key issues in managing information systems security is the question of how to design a secure IS. However, despite the recognized relevance of IS security (Baskerville 1992, Warman, 1992, Straub & Welke 1998, Anderson 1999, Dhillon & Backhouse 2001), security design aspects have been neglected in IS and software development methods (Booysen & Eloff 1995, Dhillon 1997, Hitchings 1996, Armstrong 2000, Tryfonas *et al*. 2001). The information security research community at large has become bogged down in small-scale technical questions (Thomas & Sandhu 1994, Dhillon & Backhouse 2001) and the thesis that the key issue in development is "formalization" (Anderson 1993, Barnes 1998). To fill this gap in the area of secure information systems (SIS) design, several methods for the development of secure information systems have been proposed, ranging from checklists (*e.g.*, Solms 1998, Chan & Kwok 2001, Eloff & Solms 2000a, Hopkinson 2001) to more recent approaches based on information systems (IS) or software (SW) development methods.

Particular interest has been given to scrutinizing the theoretical foundations of the alternative SIS design approaches. Baskerville (1988, 1993) and Parker (1998) have taken a critical look at checklists and security management standards, and Dhillon and

Backhouse (2001) have analyzed methods for developing secure ISs in the light of the work of Burrell and Morgan (1979).

1.1 Research questions, objectives and scope

Given this identified problem space, the overall research question (RQ) of this dissertation is to explore *how information security considerations can be integrated into existing IS development methods*. The quest to solve this is divided into three research questions (Figure 1):

- RQ1: To what extent are IS security issues examined and resolved by existing research?
- RQ2: What are the underlying assumptions, differences, commonalities and strength and weaknesses of the existing SIS approaches?
- RQ3: How can security issues be tackled by IS/SW development methods?

These RQs need to be examined in order. First, we need to recognize key information security issues and corresponding research contributions. Second, we need to analyze the scope of the existing approaches for designing secure IS/SW. Third, if the existing SIS approaches are found to be lacking in comprehensiveness, it is imperative that a new approach or paradigm for extending security into IS/SW development methods be found.

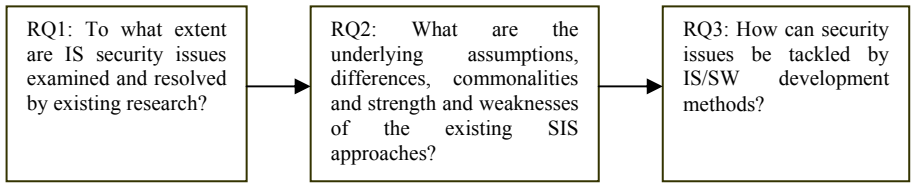


Fig. 1. Research steps in this thesis.

RQ1: The existing information security textbooks and review articles focus on certain subfields of information security, such as access control mechanisms (*e.g.*, Sandhu 1993, Sandhu & Samarati 1994, Castano *et al*. 1995, Sandhu *et al*. 1996), and methods for the development of secure IS (Baskerville 1988, 1993, Dhillon 1997, Dhillon & Backhouse 2001), or cryptographical (*e.g.*, Diffie 1988, Massey 1988, Kaliski 1993, Kahn 1996, Menezes *et al*. 1999). Yet, a comprehensive analysis of contributions in the field of information systems security is lacking. It is important, therefore, to take a closer look, from an IS security viewpoint, at the research contributions that already exist. Nevertheless, from the point of view of solving the overall research question, it seems to be necessary to consider how, and to what extent, IS security issues are covered by current research; in other words, what characteristics of IS do the existing information security contributions cover? To summarize, the aim of this first research question is to recognize security issues for IS, and examine the extent to which these issues are resolved by existing research.

The assumed contribution of this is twofold. First it will lead to an analysis of the existing research and, second, based on this analysis it will suggest future research directions. We believe that the analysis of the existing research will serve both pragmatic (*i.e.*, it will be successful in practice) and epistemic (*i.e.*, new scientific knowledge may be produced) research interests (*cf.*, Niiniluoto 1990, 1999). It will shed light on the existing research for practitioners, students specialising in security as well as researchers. For practitioners, this exploration will reveal the kinds of contributions that have been offered. Since IS security is widely perceived to be a weak link phenomenon, meaning that violators need only to find the weakest point to be able to attack the organization or IS, knowledge about how to strengthen the weakest points is of utmost importance (*e.g*, Finne 1995). On the other hand, researchers and students may be given insight into the key research approaches and reference disciplines being utilized today. Also, suggestions for future research serve the epistemic interests of science, *i.e.*, help to establish new scientific knowledge.

RQ2: Certain sets of SIS design approaches or methods can be seen to form alternative research paradigms (*cf.*, Kuhn 1962) or research programmes (*cf.*, Lakatos 1970, Nickles 2000). Both research paradigms and research programmes refer to a set of shared assumptions underlying the research and development of SIS methods (Masterman, 1970, Chalmers 1999 p. 130, Loose 2001)[1]. In other words, within each paradigm these assumptions provide researchers with a model for developing SIS methods as well as practising security. The assumption is that the checklists (*e.g.*, Kraus 1972, AFIPS 1979, Wood *et al*. 1987), management (*e.g.*, BS7799 1993, Sanders *et al*. 1996, GASSP 1999, Janczewski 2000), maturity/evaluation standards (*e.g.*, Murine & Carpenter 1984, Ferraiolo & Sachs 1996, Hefner 1997, SSE-CMM 1998a, b), formal methods (Anderson, 1993, Barnes, 1998), common sense principles (*e.g.*, Parker 1981, Schweitzer 1982, Perry 1985), risk management (*e.g.*, Guarro 1987, Fitzgerald 1993, Halliday *et al*. 1996), information/database modeling approaches (Pernul 1992, Ellmer *et al*. 1995, Pernul *et al*. 1998), responsibility approaches (*e.g.*, Strens & Dobson 1993, Backhouse & Dhillon 1996, McDermott & Fox 1999), viable IS (Hutchinson & Warren 2000, Karyda *et al*. 2001), Security modeling and business process (Herrmann & Pernul 1998, 1999, Röhm *et al*. 1998, Röhm & Pernul 1999) and security-modified IS development approaches (*e.g.*, Baskerville 1989, Hitchings 1995, James 1996, Straub & Welke 1998) can be thought of as such paradigms. The objective of the second research question is to complement the existing research efforts started by Baskerville (1988, 1993), Dhillon (1997), and Dhillon and Backhouse (2001) by analyzing the existing paradigms and respective approaches/methods from the viewpoints of the research objectives, the organizational role of IS security, the research approaches used, a conceptual metamodel for IS, and

[1] It should be noted that we do not want here to commit ourselves to, or address, the question of the maturity of alternative paradigms according to the criterion of Kuhn or that of Lakatos (*cf.*, Metaxopoulos 1989, Chalmers 1999, Nickles 2000, Loose 2001). Moreover, on the one hand, unlike Burrell and Morgan (1979) and Calas and Smircich (1999), we see paradigms as not wholly incommensurable, as this would lead to total relativism, *i.e.*, anything goes (Niiniluoto 1991). On the other hand, we do not want to declare a paradigm war (*cf.*, Weick 1999). This study is based on a belief that we can – and we should - carry out critical and constructive discussion on the underlying assumptions as well as disadvantages and merits of alternative approaches.

applicability to IS or SW development. In other words, the aim of the second research question is to explore how alternative SIS design endeavours can be classified in terms of paradigms and respective approaches. Another aim is to identify underlying assumptions of the alternative SIS design paradigms and respective approaches along with possible resulting weaknesses.

Attempts to increase our understanding of the underlying, fundamental assumptions of alternative approaches for designing secure IS are vital. For one thing, since a huge number of alternative IS security approaches exist (Baskerville 1992, Dhillon & Backhouse 2001), serious concern must be given to attempts at increasing our understanding of their strengths and weaknesses (*cf*., Hirschheim *et al*. 1995, Hirschheim *et al*. 1997). Indeed, in the light of the aforementioned viewpoints, an analysis fulfils this objective by providing a holistic picture of the theoretical assumptions in existing SIS design endeavours. For another thing, Kant (1993) insists that we as human beings are nothing more than what has been instilled in us in our education. Nevertheless, owing to education and upbringing, the fact remains that our perceptions and assessments of IS security methods and the nature of the reality that we confront when building IS/SW are governed by unconscious perceptions and biases. Hence it is crucial to recognize our possible biases. A good way to accomplish this is to perceive the underlying assumptions of our favoured approaches and to compare these with the fundamental assumptions of alternative approaches. Yet, a classification of the existing SIS design methods into paradigms and further approaches, also serves as a clarification tool for educational purposes (Iivari *et al*. 2001).

RQ3: It has been argued that the earlier SIS development methods cannot be integrated into IS/software development methods (Baskerville 1988, 1992) with the result that: "*particularly needed are security techniques that integrate well with rising general systems design techniques such as information engineering… and object-oriented analysis*" (Baskerville 1994). If this still holds with respect to the recent SIS methods and if there are other weaknesses residing in the existing SIS approaches, a third question is needed to explore how security issues can be added into IS/software development methods (to tackle some of the problems identified).

1.2 Research strategy

The dissertation utilizes conceptual-analytical, constructive and theory testing research approaches (Järvinen 1997, 2000; see Table 1). Conceptual analysis and the hermeneutic circle are offered to solve the first and second research questions, *i.e.*, to explore the underlying assumptions of the alternative SIS design approaches. The hermeneutic circle is commonly used by historians, philosophers and theologians to discover something from a document that is not explicitly present in it (Kvale 1983, Gadamer 1989, Mautner 1996 p. 188). Since one of the aims of this dissertation – the first and particularly second research question - is to scrutinize and compare the underlying assumptions of the existing SIS design endeavours, which are not explicitly indicated in the original texts, the hermeneutical circle is a natural methodological choice. It results from the

hermeneutic research strategy that the findings of this dissertation are based on our interpretations. The findings are not argued to be objective in the sense of natural science. Hence, this study adopts the interpretive research paradigm (*cf*., Gadamer 1989, Walsham 1996, Klein & Myers 1999, 2001).

Table 1. Research strategy: research approaches for solving the research questions.

Research questions	Chapters	Research approaches
To what extent have IS security issues been examined and resolved by existing research?	II	Conceptual analysis (hermeneutic circle)
What are the underlying assumptions, differences, commonalities and strength and weaknesses of the existing SIS approaches?	III	Conceptual analysis (hermeneutic circle)
How can security issues be tackled by IS/SW development methods?	IV	Constructive research and theory testing (action research)

With respect to the third research question, constructive research with a theory testing research approach is utilized. Constructive research is applied to construct the new solution, and theory-testing research is applied to test it. With respect to testing of the new construct (theory-testing research), action research was the approach adopted. In action research, one "identifies a question to investigate, develops an action plan, implements the plan, collects data, and reflects the findings of the investigation." (Johnson 1995).

Action research has been advocated as a promising research strategy (Lewin 1949, Blum 1955, Susman & Evered 1978, Baskerville & Pries-Heje 1999, Avison *et al*. 2001, Mumford 2001a). In fact, it has been argued that action research is ideal for studying IS methods in a practical setting (Baskerville & Wood-Harper 1996, 1998). By putting theories to work in practice, for example, scientific knowledge is expanded. This helps participating organizations to solve concrete problems with possible long-term implications (Baskerville & Wood-Harper 1998). It is therefore no wonder that action research studies examining the relevance of IS security methods in practice have been recently called for by IS security scholars (Baskerville 1994, Dhillon & Backhouse 2001), though only a few action research IS security studies exist, including Armstrong (2000), James (1996) and Straub and Welke (1998). Action research was chosen as the research methodology of the part of the thesis tackling the third research question). Action research (Baskerville & Wood-Harper 1998, Schein 1987) can be seen as an ideal way to empirically study the applicability of the proposed new solution in practice, and, thus, this technique was reflected in this thesis.

Action research is a form of field intervention driven by a problem in an organization. Action research is an empirical method that is interventionist, qualitative, interpretive (*cf*., Walsham 1993, 1996, Klein & Myers 1999, 2001) and even critical (by accomplishing a change in the participating organization; *cf*., Mumford 2001a). An action

research endeavour can last from weeks to years (Mumford 2001b p. 12). Its primary purpose is not to find general or universal mechanistic-causal laws (Klein & Myers 2001), but rather to test and adjust a theory through a practical and social setting. From the perspective of action research, theories are validated through successful use; successful use being defined through the social reflection of the collaborators in the research. To collect data during the intervention, interviews were used.

Seven validity criteria for IS action research results have been proposed (Baskerville & Wood-Harper 1998): (1) the research should be set in a multivariate social situation; (2) the observations should be recorded and analyzed in an interpretive frame; (3) there is researcher action that intervened in the research setting; (4) the method of data collection include participatory observation; (5) changes in the social setting are studied; (6) the immediate problem in the social setting must have been resolved during the research; and (7) the research should illuminate a theoretical framework that explains how the actions led to favorable outcome. These criteria are applied when evaluating the results of the intervention.

1.3 Structure of the thesis

The remainder of this thesis is organized as follows (Figure 2).

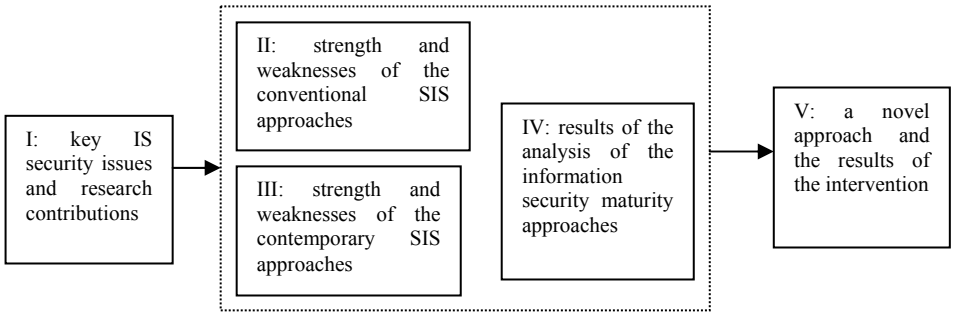


Fig. 2. The results of the thesis

The second chapter analyses IS security issues and the respective research contributions (I) -see figure 2. The third chapter critically analyses weaknesses and underlying assumptions of the existing SIS approaches and, with the help of five lenses, endeavours to classify these approaches in terms of SIS paradigms. The dotted box in figure 2 presents the framework within which the analysis of the existing SIS approaches is carried out. As figure 2 shows, this analysis is divided into three sub-chapters, namely conventional (II), contemporary (III) and maturity criteria (IV).

Even though maturity criteria are also analysed in 3.1 (conventional approaches) through these five lenses, section 3.3 offers deeper insight to information security maturity criteria (IV).

The fourth chapter, as seen in figure 2, proposes a new paradigm for adding security into existing methods for designing secure IS/SW (V). In the fifth chapter, limitations and implications of this dissertation are discussed, and in the sixth chapter, the key findings of this thesis are summarized. The original papers are included in the appendices.

2 A survey of information systems security issues and respective research contributions

This chapter identifies key IS security issues and examines the extent to which these issues have been studied and resolved in existing research. Information security is a highly diverse field. On the one hand, it has been studied by cryptologists, computer scientists and electrical engineers, and on the other hand by IS scholars. Owing to this diversity and fragmentariness in studies on information security, there is a serious need for sense to be made of the field as a whole.

In seeking for an appropriate vehicle for organizing and categorizations of the contributions on information security, we found the following set of questions useful:

- How can peoples' access to information be controlled?
- How can secure communication between people be ensured?
- How should IS security be managed?
- How should an IS be developed in order to be secure?

These issues are appropriate and instrumental for educational and sense-making purposes (*cf*., Iivari *et al*. 2001) and for studying the extent of IS security research in a variety of areas. We see that these issues represent an abstraction of IS security contributions. This means that security contributions can be mapped out according to these four issues and vice-versa.

Different types of information security requirements may be associated with these IS security issues. The following four requirements are widely agreed to be important, irrespective of the tradition of information security they emanate from (*e.g.*, Datapro 1992, Parker 1981, Abrams & Podell 1995, Röhm *et al*. 1998):

- *non-disclosure* (improper disclosure of information should be detected and prevented);
- *integrity* (information should not be modified by unauthorized subjects);
- *availability* (information should be available to authorized subjects when required);
- *non-repudiation* (one cannot deny an action that has been done).

Furthermore, we find *repudiation* to be the fifth security requirement referring to cases where one can deny an action that one has done. For example, a person may use a digital picture to communicate secretly with another person: the sender hides a message in the

digital picture and subsequently denies the existence of the message arguing that he/she only sent the picture without knowing about the hidden message.

We have found several potential frameworks in the IS literature with which information security issues and their respective research contributions can be analyzed. Dhillon (1997), Dhillon and Backhouse (2001) and Hirschheim and coauthors (1995, 1996) have analyzed existing methods in the light of Burrell and Morgan (1979), Iivari and Kerola (1983) have accomplished a feature analysis, Iivari (1989, 1991a) has scrutinized IS development methods from the viewpoint of a metamodel for IS, while Iivari (1991b), Iivari and Hirschheim (1996), and Iivari and coauthors (1998) have analyzed IS development methods in the light of research methods, organizational role of IS, schools of IS and research objectives. Of these, a meta-model for IS, research approaches and reference disciplines were regarded as excellent candidates for the present purposes of exploring the second research question of this thesis:

The viewpoint of a meta-model for IS (Iivari 1989, 1991a) is adopted to explore the question: what IS characteristics do the contributions cover?

The viewpoint of research approaches (Järvinen 1997, 2000) is utilized to study the question (Figure 3): which research approaches have been found and preferred in order to a) develop IS security methods and techniques; and b) to validate the solutions?

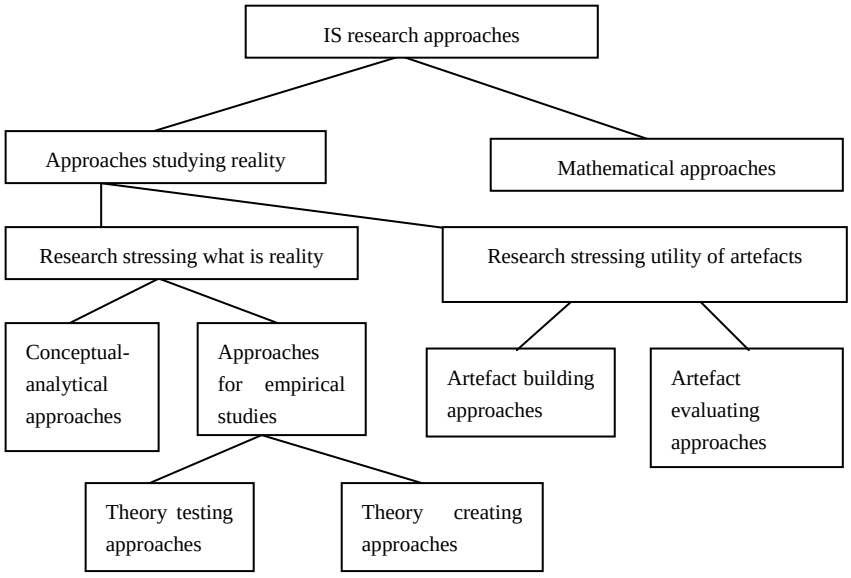


Fig. 3. A classification of IS research approaches (Järvinen 1997, 2000).

Following Järvinen (1997, 2000), IS Research approaches are first divided into "approaches studying reality" and "mathematical approaches". Approaches studying reality is subdivided into "approaches stressing what reality is" and "research stressing utility of artefacts" (Figure 3). The former is subdivided into "conceptual analytical approaches" and "approaches for empirical studies". Approaches for empirical studies is in turn divided into "theory testing" and "theory-creating" approaches. The latter is

divided into “artefact-building approaches” and “artefact evaluating approaches”. To simplify things, we also termed 'artefact-building' and 'artefact evaluating' approaches 'theory testing' and 'theory-creating' approaches, respectively (irrespective of whether they concern artefacts or not).

The viewpoint of reference/contributing disciplines (*cf.*, Lyytinen 1987) is taken up to scrutinize the question: Which reference disciplines have been viewed as most relevant and fruitful as the basis of information systems security research? Figure 4 depicts a taxonomy of IS research disciplines.

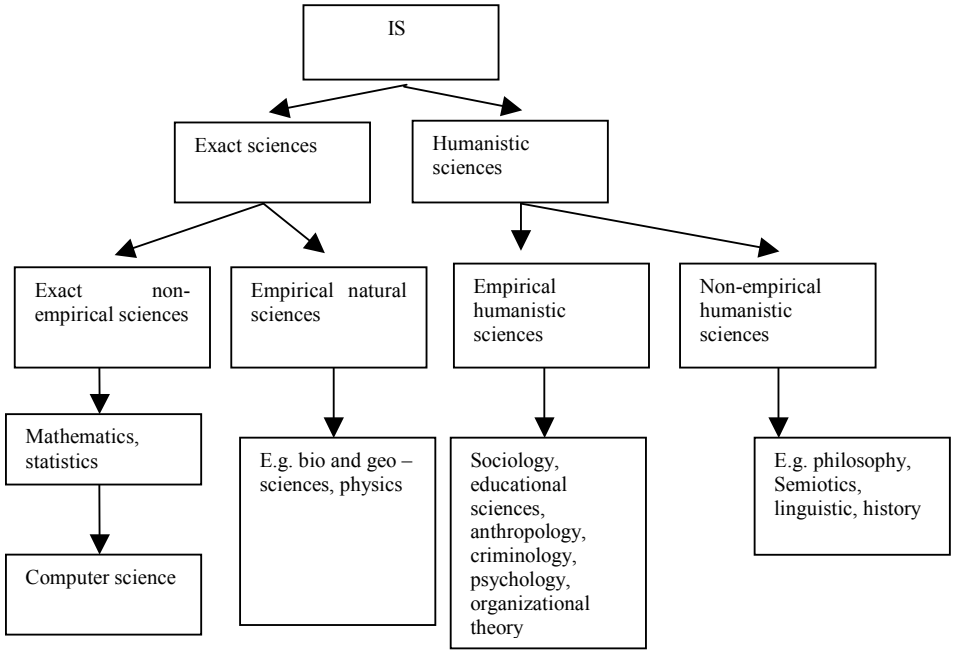


Fig. 4. A taxonomy of IS reference disciplines.

IS researchers have utilized several contributing disciplines from mathematics to sociology, psychology and philosophy (Lyytinen 1987). Figure 4 presents a categorization of possible reference disciplines for IS (security) on the basis of Lyytinen (1987) and Hirschheim and coauthors (1995). Reflecting these scholars, disciplines contributing to IS may first divided into “exact sciences” and “humanistic sciences”. The former can then be further divided into “exact non-empirical sciences” (*e.g.*, mathematics, statistics) and “exact empirical sciences” (*e.g.*, bio and geo –sciences, physics). The latter, humanistic sciences, can be further divided into “empirical humanistic sciences” (*e.g.*, sociology, educational sciences, anthropology, criminology, psychology, organizational theory) and “non-empirical humanistic sciences” (*e.g.*, philosophy, semiotics, linguistic, history). It must be stated that this classification of

contributing disciplines is not inclusive, but offers a conceptual tool for understanding information security research contributions.

The results of the analysis of IS security issues in the light of these three viewpoints (meta-model for IS, research approaches and reference disciplines) are summarized and discussed next.

The contributions with respect to issues of "How can people's access to information be controlled?", includes access control models and policies, information flow control models, operating systems protection, anti-virus techniques, policies for web IS, watermarking, cognitive passwords, and endeavours to maximize users' intent to comply with security policy.

The existing information security contributions surrounding the issue of "How can secure communication between people be ensured?", includes cryptographical algorithms and systems, virtual private networks, anonymity techniques and steganography.

The existing information security contributions surrounding the issue of "How should IS security be managed?" concern: auditing, intrusion detection systems, security policies, firewalls and digital signatures.

The information security contributions on the issue of "How should an IS to be developed in order to be secure?", include secure programming, methods for developing and managing secure IS/SW, risk analysis, and testing methods.

With respect to the meta-model for IS, a comprehensive literature review suggests that most of the contributions on IS security issues take a technical approach. The fact that security research has concentrated on technical problems raises some implications from an IS point of view. First, the introduction of technological solutions always raises the question of how users will adopt these (*cf*., Mathieson 1991). Second, it is clear from the literature review that some issues are only solved via technical solutions although the issues are so complex that a purely technical solution is not sufficient. This means that cryptography-based solutions, for example, have been well researched (compared to non-technical security issues), but simple management policies covering encryption have attracted little to no interest, despite the fact that one of the main issues with respect to symmetric or asymmetric cryptography is clearly a management issue. That is to say, cryptographic solutions whether symmetric (one key system) or asymmetric (two key system) depend on successful key management (Davis & Ylönen 1997).

Consider another example: access control policies. These attract wide interest among information security researchers (Sandhu 1993, Sandhu & Samarati 1994, Dhillon & Hosein 2001). Yet access control policies are still unable to prevent leaks of information at the organizational level, *i.e.*, access control policies do not prevent abusers from obtaining information from authorized users at the organizational level nor do they prevent authorised users from being able to spread top-secret information. Despite this obvious weakness, little research has been carried out in this area.

A similar technical focus is also found with respect to security policies. The research on security polices has concentrated on small-scale formal policies, rather than high-level and/or large-scale (organizational) security policies. It seems that many researchers take the view that security-relevant subjects are, in the final analysis, processes (*e.g.*, Sandhu 1993). This assumption about the computer-oriented nature of security-relevant entities describes the overwhelming focus of modern information security research.

Across all IS security studies and particularly meta-analyses (*e.g.*, scrutinizing the very foundations and ultimate meanings of concepts), few overview studies are found. We believe that the neglect of interpretive reviews (or meta-studies) can be traced back to the predominant research interest of the security community, namely pragmatic research (*i.e.*, results applicable to practice are favoured). As far as critical studies are concerned, the community of cryptographers, computer scientists in computer security using mathematical research approaches, are an exception. It seems to be that research which does not utilize mathematical approaches, but produces different procedures, principles, methods and other non-technical research results, is too often uncritically accepted; or perhaps this kind of research does not generate enough interest from disciplined scholars.

Technological solutions are developed using mathematical modeling and philosophical logic (logical analysis) as their primary research approach. As the technical context focuses on presenting information in a form understandable by computers, mathematical and logical modeling are relevant research approaches. Also, mathematics and philosophical logic are pertinent reference disciplines.

Conceptual level contributions are mainly composed of IS security development methods. These IS security development methods propose different notations for modeling security aspects of IS at conceptual level. The principal research approaches are conceptual analysis and empirical research. We take the position that since the conceptual level contributions model security relevant entities and activities, the philosophy of language and semiotics would be relevant contributory disciplines.

As with the organizational context, the prevailing research approaches are conceptual analysis and empirical research. Yet the number of empirical studies published with respect to these different issues continues to be sparse.

3 A paradigmatic analysis of the existing approaches for designing secure IS/SW

Alternative SIS design endeavours are reasonably well understood as a result of earlier studies on IS security (Baskerville 1988, 1992, Dhillon 1997, Dhillon & Backhouse 2001). Baskerville (1988, 1992) presented a generational categorization of different SIS approaches, while Dhillon (1997) and Dhillon and Backhouse (2001) analysed IS security approaches using the concept of four paradigms of sociology of Burrell and Morgan (1979).

However, these studies (Baskerville 1988, 1992, Dhillon 1997, Dhillon & Backhouse 2001) are lacking two elements. First, these studies do not cover certain SIS design approaches (*e.g.*, information security maturity approaches, information modeling approaches, viable IS, business process approaches). Second, these studies do not evaluate particular important features of the approaches, including modeling support for the existing SIS approaches, the question of whether the SIS approach can be integrated to the IS development methods[2] and research approaches used. Hence, an additional systematic review of IS security approaches was needed. In order to accomplish such a systematic analysis, a good conceptual framework was first called for. Of the possible frameworks (*e.g.*, Iivari & Kerola 1983, Hirschheim & Klein 1989, Iivari 1991b, Lyytinen 1991, Hirschheim *et al*. 1995, 1997, Iivari & Hirschheim 1996, Iivari *et al*. 2001), the following analytical framework was envisioned. It is comprised of five viewpoints synthesised to permit analysis of a variety of IS security endeavours (Table 2).

[2] Baskerville (1988, 1992, 1993) studied whether the SIS approaches can be integrated to IS development methods in his papers, but since his articles, based on his 1988 works, several new approaches have presented. Therefore, an updated analysis exploring whether can one integrate the SIS approach into IS development methods is seen as necessary.

Table 2. Analytical framework

Viewpoints	Theoretical background of the viewpoints
1) What are the research objectives?	Chua (1986) and Habermas (1984, 1987)
2) What are organizational roles of information systems security?	Iivari and Kerola (1983), Iivari and Hirschheim (1996) and Kant (1993)
3) What research approaches have been used?	Järvinen (1997, 2000)
4) What levels of IS do the methods for development of secure IS cover?	Iivari (1989, 1991a)
5) Are the methods for the development of secure IS applicable to IS and SW development?	Baskerville (1988, 1992)

1) Analysis of the existing SIS approaches in the light of the research objectives is useful to highlight *the possible goals of the researchers*. Following Chua (1986) and Habermas (1984, 1987), potential research objectives includes: a) means-end oriented/technical; b) interpretive; or b) critical/emancipatory objectives. A means-end oriented view holds that the aim of research is to produce knowledge in order to achieve certain concrete goals or ends (Chua 1986) and to increase human control over phenomena or nature (Habermas 1984). Means-end (or technically) oriented research is aimed at achieving this by finding mechanistic-causality laws. The natural sciences and computer science research are typically means-end oriented, although we can find means-end oriented research aimed at finding causal laws/explanation in the social or IS sciences, too. Interpretive research means increasing people's understanding of the meaning of their actions (Chua 1986 p. 615), and it is therefore qualitative in nature, as opposed to research aimed at establishing causal relationships or statistical generalizations. The importance of interpretive research is widely advocated by historians, theologians, educationalists, social scientists, and has recently gained increased attention in the IS world (Hirschheim 1985, Walsham 1996, Galliers & Swan 1997, Klein & Myers 1999). The goal of critical, or emancipatory, research is to point out the weaknesses of existing theories/practices – particularly dominant ones.

2) It is important to understand which approaches favour which *types of organizational roles for IS security development* (*cf*., Iivari & Kerola 1983, Kant 1993, Iivari & Hirschheim 1996)? Possible organizational roles of information systems security includes: a) technical; b) socio-technical; or b) social. We see that the main theoretical underpinning for the organizational roles of IS security originates from Kant's imperative of human dignity (Kant 1993). According to the technical view, the emphasis in IS development should be on technical matters, with social implications being at best afterthoughts (Iivari & Hirschheim 1996). The technical view in its extreme form violates the Kantian imperative of human dignity, as one should never merely treat people as means but always as ends in themselves (*cf*., Kant 1993). The social view emphasizes the development of organizational systems (before technical matters), and the socio-technical view contends that technical and organizational systems are equally important (Iivari &

Hirschheim 1996). The social view takes Kantian imperative of human dignity more than seriously by putting users' ends before everything else, while the socio-technical view aims to respect the Kantian rule of human dignity as far as possible in respect of finding a balance between these other two views (technical, social).

3) Analysis of the existing SIS approaches from the viewpoint of the research approaches used (Järvinen 1997, 2000) is relevant[3] in order *to see what research approaches are used and preferred for developing IS security methods and validating the solutions*? Järvinen's classification was considered in second chapter.

4) A meta-model for IS (Iivari 1989), including the organizational level, the conceptual level, and the technical level, helps to see *what aspects of IS the existing SIS methods do cover*?

5) Applicability to IS and SW development (Baskerville 1988, 1992) is needed to explore *whether the SIS design approaches can be integrated into IS or software development*?

The analysis proceeds under three separate sections: (3.1) conventional (II)[4] and (3.2) recent, contemporary SIS design endeavours (III)[5]. Finally, information security management maturity criteria are analysed (IV) in 3.3.

3.1 Conventional SIS design approaches

Selected rationales to support the results of the analysis of conventional SIS design approaches (normative standards, risk management, formal methods and common sense principles) summarizes in table 3, are considered next.

---

[3] Although we are aware of other classifications of research approaches and methods, including those of Avison and Fitzgerald (1991), Jenkins (1985), Galliers and Land (1987), Iivari (1991b), Nunamaker *et al*. (1991), Stohr and Konsynski (1992), March and Smith (1995), and Wynekoop and Russo (1997) that proposed by Järvinen (1997, 2000) was chosen since it is systematic and holistic. The concept "research approach" operates at a higher level of abstraction than that of "research method", which means that one research approach can by addressed by means of several research methods.

[4] Checklists, information security management standards and information security management-oriented maturity approaches were discussed in II under the label "normative standards". II is a shorten version of a more comprehensive and detailed analysis of the conventional approaches described in (Siponen 2002).

[5] Security modeling and business process (Herrmann & Pernul 1998, 1999, Röhm *et al*. 1998, Röhm & Pernul 1999) and viable IS paradigms (Hutchinson & Warren 2000, Karyda *et al*. 2001) as well as an IS security planning methodology (Straub & Welke 1998) under the security-modified IS development approach paradigm were not included in III due to lack of space, but these are discussed in this extended summary under contemporary endeavours.

Table 3. An overview of conventional SIS design approaches

Analytical framework	Normative standards	Risk Management	Formal methods	Common sense principles
Research objectives	Means-end oriented	Means-end oriented and interpretive	Means-end oriented and critical	Means-end oriented (critical)
Organizational role of IS security	Technical	Technical	Technical	Technical, socio-technical and social
Research approaches	Not known	Conceptual analysis, empirical	Mathematical modeling	Not known
Applicability	Not applicable	Not applicable	Weak	Not applicable
Meta-model for IS	Organizational level	Organizational level	Organizational and technical levels	Organizational level

Normative standards

Normative standards include checklists, management-oriented maturity criteria and information security management-oriented standards. Information security checklists, management and maturity standards prescribe a list of generic security actions based on security experts' practical experiences (*cf*., Baskerville 1992). There are, however, small differences between "checklists", "management" and "maturity" standards. Underlying checklists is the view according to which possible security solutions and procedures can be identified and turned into a list, *i.e.*, a checklist. The difference between information security management standards and checklists is thus that the former do not support a checklist–orientation, *i.e.*, they do not include a place where one can tick a box. Yet, the aim of management standards is to enforce a general, even universal standard, while checklists do not argue that the lists are universally applicable. In maturity standards, in turn, the security prescriptions are divided into maturity levels, usually from 1 to 5. But, even though checklists and information security management standards may not *per se* incorporate the concept of maturity level, they can easily be modified to include maturity stages. One way to accomplish this is to decide which spots in the standards/checklists illustrate maturity more than others. Information security maturity standards also differ from other approaches in that they function as a sign for the public. In other words, information security maturity standards have a public or non-organizational facet, while traditional standards and checklists only encompass the organizational facet.

But given that information security checklists, management and maturity standards prescribe safeguards or countermeasures based on practitioners reflections on what security solutions seem to work in organizations, we consider these all under the label "normative standards", as is done in II. The dominant *research objective* of normative standards is means-end oriented. The following example of the AFIPS (1979) view illustrates this: "a primary purpose of this manual is to serve as a practical aid in the

planning and the implementation of a thorough, effective computer security program" (AFIPS 1979 p. 2). As this extract indicates, the aim of the AFIPS (1979) checklist is to equip managers with a practical, cost-effective tool that can help them to identify the necessary set of security controls. Another example of this view comes from Generally Accepted System Security Principles (GASSP 1999), which advocates a means-end oriented view, as deduced from the fact that it lists a few objectives that are clearly means-end oriented: a) improving security; b) increasing managers' confidence that the right kind of security has been implemented; and c) global harmonization of security principles, enabling smooth business co-operation between organizations (*cf.*, GASSP 1999 p. 29-30).

As for views on the *organizational role of IS security*, the dominant view of normative standards is technical, for two reasons. First, the primary concern of normative approaches rests on technical issues, including cost-effectiveness, and second, they do not address organizational structures or social implications. Users may be regarded as an important element, but a common, crucial view among these normative standards is that the users' own autonomy is not recognized. At best, the normative standards ensure that users can understand and follow their security missions easily. In the worst possible scenario, the users will not understand the relevance of security actions, with the result that their behaviour has to be enforced or transitioned in the right direction by enlightened individuals (security experts). The following example shows how the technical view bears on a normative standard. Like Wood and coauthors (1987), AFIPS (1979) and BS7799 (1993), SAFE (1972) sees the employees as necessary means for achieving security. For SAFE (1972), humans are purely instruments without autonomy, with the result that SAFE (1972) checkpoints are aimed at controlling humans in terms of security rather than pondering the social implications of security activities, for example.

With respect to the *research approaches used*, one feature common to normative standards is that they are not based on rigorous academic research and are therefore lacking scientific proof. For example, the AFIPS (1979), SAFE (Kraus 1972) and Moulton and Moulton (1996) checklists do not state the origins of their ideas, but we gain the impression that they reflect their authors' practical experiences. We also interpreted the comprehensive controls checklist of Wood and coauthors (1987) as having been developed on the basis of the authors' practical experiences. Wood and coauthors provide a small hint in this direction by stating that it was developed on the basis of a US Air Force project (Wood *et al*. 1987 p. v). Wood and coauthors do not reveal any further information on the discovery process that led to this checklist.

GASSP (1999) states that it is based on existing industrial conventions observed by practitioners "on the basis of experience", and not derived "from a set of postulates or basic concepts" (GASSP 1999 p. 33). But regardless of any conventions, the practices included in such a standard must be "generally accepted" (GASSP 1999 p. 33), whatever that means. The answer GASSP (1999) provides on this point is not very helpful, for its principles "become generally accepted by agreement (often tacit agreement)" (GASSP 1999 p. 33). Moreover, GASSP (1999) reveals that it has also reflected "information security textbooks and articles" when necessary in developing its standard (GASSP 1999 p. 34). Nevertheless, the above information allows us to conclude that GASSP (1999) is based on its authors' practical experiences and knowledge derived from information security management cookbooks rather than on empirical research and conceptual

analysis, as the process of finding “tacit agreements” can hardly be labelled as rigorous empirical research.

We see that the research approach adopted by BS7799 is very similar to that of GASSP. BS 7799 (1993) gives hints that it is also based on a process of observing industrial practices: “the controls documented [in BS7799] are widely accepted by large, experienced organizations as recommended good practices for all situations". This statement leads us to conclude that BS7799 is based on experts’ observations rather than rigorous empirical studies guided by a research method.

SSE-CMM (1998a) also relies on experts’ observations, as seen from the following example: ”The SSE-CMM…captures practices generally observed in industry” (SSE-CMM 1998a).

The absence of the use of research methods means that we have no real evidence for the normative approach as expressed above. This is unfortunate, since the use of a rigorous research method, including sharing information about the authors' observations and the conclusions based on them, give much more credibility to the research results. We conclude that the normative standards are based on their authors' practical experiences and observations rather than on the use of a particular research strategy.

When it comes to the *meta-model*, normative standards provide only organizational-level support for designing a secure IS. They typically consist of entities which can be classified as work procedures. Moreover, none contain modeling support. Furthermore, with respect to the question of *applicability to IS*, none of the normative standards can be smoothly integrated into the IS/SW development process.

Risk management

Risk management (RM) techniques can be defined as approaches dealing with information security risk (also including meta-studies with respect to risk management).

The thesis overview revealed two *research objectives* behind RM techniques, namely means-end oriented and interpretive. Examples follow. The approach of Saltmarsh and Browne (1983) is an example of the means-end oriented view, as their aim is to provide feasibility justifications for implementing certain security controls.

The approach of Halliday and coauthors (1996) also indulges in a means-end oriented view with respect to research objectives. The following extract illustrates this view: “approach to effective information technology risk management.” (Halliday *et al*. 1996 p. 19). The term effective approach illustrates the prevailing means-end oriented view. Consider also a second citation: “An important aspect of a risk analysis…is the provision of some means by which risks can be prioritised and countermeasures can be selected and implemented on a cost-effective basis”(Halliday *et al*. 1996 p. 21). This latter claim (that risks can be prioritized in a cost-efficient manner) also clearly implies that Halliday and coauthors favour a means-end oriented view as a research objective.

Guarro’s (1987) RM approach seems to indulge in means-end oriented and interpretive views. With respect to the means-end oriented view, it states that RM “is not only capable of identifying potential losses that could be unacceptable for a given system, but it can be used to determine which specific security controls and counter measures can be effective and justifiable” (Guarro 1987 p. 493). This indicates a means-end oriented view by advocating that RM techniques should meet certain concrete goals (*e.g.*, justify controls)

effectively. We also found two hints that could be regarded as expressions of favour for an interpretive view. In the first place, Guarro (1987) states that the objective is to "develop an understanding of the nature and the severity of risk" (Guarro 1987 p. 493). This statement clearly involves an interpretive dimension: to understand the business environment and its possible risks. The second hint, involving the need to "convince the decision maker(s) for whom they [results of RM] were expressly prepared and developed" (Guarro 1987 p. 496), can perhaps be also regarded as an interpretive research objective. One may interpret this as suggesting the use of RM techniques as an interpretive tool, *i.e.*, one that helps managers to understand hidden risks. We also see from the latter citation, however, that Guarro regards RM as an instrument (consider "convince") to persuade managers to achieve a concrete objective (*e.g.*, to accept that their organization will obtain certain security solutions). In that light, we see that Guarro's RM approach serves as an instrument to accomplish a means-end oriented research objective.

An interpretive view can be attested from the following quotation by Baskerville: "its [risk management] ostensible value as a predictive technique is less relevant than its value as an effective communications link between the security and management professionals…" (Baskerville 1991 p. 121). In other words, RM is a necessary communication tool, particularly for meeting managers' decision making needs.

The view founded on *organizational roles of IS security* is technical. To give an example, the organizational roles of IS security inherent in the generic RM approaches of Saltmarsh and Browne (1983) are technical. First, they aim to accomplish an efficient means for reducing risks, which represents a concentration on technical systems, and second, they do not concern themselves with the social or organizational implications of RM.

To give another example, Halliday and coauthors (1996) favour a technical view with respect to the organizational roles of IS security. This interpretation was reached on account of the fact that their focus lies on technical means for ensuring security in organizations. Even though their approach goes beyond technical systems to cover human issues, they do not ponder over its social or organizational implications. In fact, we see that according to their approach, a social system is regarded only as an instrument for improving the process of cost-effective RM.

The *research approach* commonly used with respect to RM techniques is that of conceptual analysis. For example, Saltmarsh and Browne (1983) deduced their approach from selected existing risk management approaches, and, thus, it is conceptual-analytical. The X-ifying RM approach (Frisinger 2001) makes an exception as, in addition to conceptual analysis, it also uses a web-based survey to find general risks in different lines of business (Frisinger 2001 p. 297-300). This can be classified as involving both the creation and testing of a theory (Järvinen 1997, 2000). The research method employed is that of a survey.

When it comes to the *meta-model*, RM techniques provide only organizational-level support for designing a secure IS, and they all propose different guidelines, which are classified as work procedures at the organizational level

As for *applicability to IS*, the RM approaches analysed all have a problem with developmental duality, *i.e.*, they do not provide any guidance as to how these techniques could be integrated into the IS development process.

Formal method

The common interest of all the approaches classified under the paradigm of formal method (FM) is that IS or SW development should be based on formally validated components or carried out by formal methods. The term 'formal' stems from the use of logic, taking hard analytical philosophy as the reference discipline. The use of formalism in Anderson (1993) and Barnes (1998) are good representatives of the paradigm of the "formal method" community.

With respect to *research objectives*, both Anderson (1993) and Barnes (1998) provide a tool for accomplishing a reliable and secure way to build IS/SW: "Robust security designs are those that make their assumptions explicit, and so the design methodology must force the team to examine its assumptions in a systematic and careful manner." (Anderson 1993 p. 40). Hence, the research objective of Anderson and Barnes is means-oriented. We also see that Anderson's objective encompasses critical research, as he argues that the rigorous use of formalism and public development are necessary – albeit usually missing in his opinion – at least in non-military development/research endeavours. Thus, insofar as Anderson is arguing for changes in conventional practices, he is engaging in critical research.

The views of Anderson (1993) and Barnes (1998) on the *organizational role of IS security* are technical in orientation. As for their demands for the use of formalism, these focus on technical systems. Poor technical quality – careless use of a formal method, or the lack of such a method - lies behind the security problems, because the most important condition for achieving secure systems is technical quality. Anderson recognizes the importance of proper training and management (*e.g.*, Anderson, 1993 p. 39), but in our understanding, only as necessary components of building secure IS. Thus, we see that both Anderson (1993) and Barnes (1998) hold a technical view of the organizational role of IS security.

The *research approach* favoured by the FM community is mathematical modeling. This is the approach of the natural sciences, aimed at finding "natural" laws and making general, even universal, predictions. In FMs, this idea manifests itself as the ideal for proposing "laws" and making "predictions" on security-related events and entities within computer systems.

According to the *meta-model* of Iivari (1989), this "modeling" support is concentrated on the technical and organizational levels. The demand for using FMs is for work procedures at the organizational level, whereas the use of a FM is, in itself, an artifact on the technical level. The FM approach does not presuppose any particular means of organizational or conceptual modeling.

With respect to *applicability to IS*, calls for the use of FMs perpetuate the problem of developmental duality. In other words, we found that FM approaches do not provide any guidance as to how these approaches can be integrated to IS development. Suggestions for the integration of security and normal IS/software development have been put forward, including that of Zhou and coauthors (1999) but they concentrate mainly on implementation issues (or even more specified ones), ignoring logical-level issues (*e.g.*, modeling). Anderson (1993 p. 38) also takes up the issue of integration, but does not suggest a concrete means by which this could be achieved.

Common sense principles

The common sense principles paradigm refers to a group of works which meet the three criteria. An author aspiring to a place in the common sense principles paradigm will put forward his/her own security management principles a) as developed on the basis of practical experience, and b) neglecting related work – particularly academic research presented in premier journals. Virtuous authors of security common sense principles do not, it seems, follow any research method rigorously.

The *research objective* of the common sense principles (Parker 1981, Perry 1985, Sherwood 1996) analysed in this thesis would seem to be means-end oriented, *i.e.*, to produce clear cost-efficient guidance for achieving the goal of more secure systems. Perry's objectives also include critical research, as his main arguments lie in changing the conventional attitude that computer security is a human problem rather than a technical one – "security is not a technical problem… security is a people problem" (Perry 1985 p. 7-8).

The *organizational roles* of common sense principles in IS security range from technical to social, *i.e.*, different common sense principles manifest all three organizational roles of IS security. For example, the organizational role of IS security in Parker's computer security program is technical, as its primary focus is on technical systems. Possible social implications are not addressed. The fact that Parker's book of 1998 regards violations of security regulations which are carried out in order to satisfy moral concerns as syndromes of one kind or another also stresses the technical view of the organizational role of IS security. In the latter example, the user's goal, even when accomplished in order to fulfil a moral concern, is not recognized – but all such goals are looked on as symptoms which need to be cured – another example of using people as a means only (technical view). To take another example, the organizational role of IS security in Perry's view is socio-technical, as he strongly advocates the view that security is a people problem (Perry 1985 p. 7-8) and provides principles for ensuring proper working conditions (*cf*., Perry 1985 p. 93-94). However, although recognizing the human issues, he shows equal concern for technical issues. He also proposes a list of tricks for fooling people into committing themselves to organizations' security policy/guidelines (*cf*., Perry 1985 p. 94). These two latter aspects lead us to believe that Perry's view on the organizational role of IS security is socio-technical.

Common sense principles do not follow any *research approach* rigorously. For example, Sherwood's (1996) approaches first look like being developed in a conceptual-analytical manner to address the concern that mainstream security methods do not take organizations' own security and business requirements seriously enough. Sherwood's use of the conceptual-analytical approach is less rigorous, however, as he does not refer to any other related research. Furthermore, he does not provide any empirical evidence to support the suitability of these principles in a practical setting.

To take another example, Parker's approach is "based on my twenty-eight years of study of real loss experience and on interviews more than two hundred perpetrators and their victims", as he says explicitly in his 1998 book. He did not deem it necessary, however, to reveal the details of this "research" or observation process, which is unfortunate, as his decades of experience might have been of value for future research

and practice, had he followed a more rigorous approach to collecting and analysing his data and reporting on his findings. As a result, one may look at Parker's use of his research approach/method in two ways. From the positive viewpoint, one may classify his approach as theory-creating and his methodology as that of action research, since his work is grounded in the notion of intervention in organizations (*cf*., Baskerville & Wood-Harper 1996, 1998). From the negative viewpoint, however, one may argue that Parker has not adopted any research approach or research methodology rigorously enough.

In terms of the *meta-model*, all these principles provide only organizational-level support for the development of secure IS/software (as functional abstractions, since they may be understood as work procedures).

As for the question of *applicability to IS*, the common sense principles face the problem of developmental duality, as they do not propose any means by which principles for managing security in an organization could be integrated into normal IS development. Of the common sense principles analysed in this thesis, only Sherwood (1996) recognizes the issue of developmental duality to some extent (*cf*., Baskerville 1993), as one of his main concerns is with bridging the gap between business and security requirements. In spite of this, we felt that his approach succumbed to the problem of developmental duality, as is does not give any guidance on how to integrate security with normal IS development.

3.2 Contemporary SIS design approaches

The results of the analysis of contemporary SIS design approaches summarized in table 4, are considered next.

Table 4. An overview of contemporary SIS design approaches

Analytical framework	Security-modified IS development approach	Information modeling	Responsibility modeling	Security modeling and business process	Viable and Survivable System Approaches
Research objectives	Means-end oriented and interpretive	Means-end oriented	Means-end oriented and interpretive	Means-end oriented and interpretive	Critical, interpretive and means-end oriented
Organizational role of IS security	Technical, socio-technical and social	Technical	Technical and socio-technical	Technical	Technical, Socio-technical
Research approaches	Conceptual analysis, constructive and empirical	Conceptual analysis	Conceptual analysis	Conceptual analysis and constructive research	Conceptual analysis
Applicability	Two support applicability	Weak	One support applicability	Weak	Weak
Meta-model for IS	Organizational and conceptual levels	Conceptual level	Organizational level	Organizational and conceptual levels	Organizational level

Security-modified IS development approach

The term "security-modified IS development approach" was used to describe approaches that are influenced by IS or software development methods. Such security-modified IS development approaches are:

- Logical modeling (Baskerville 1988, 1989);
- Virtual Methodology (Hitchings 1995, 1996);
- Spiral approach (Booysen & Eloff, 1995);
- James' (1996) approach;
- An IS security planning methodology (Straub & Welke 1998).

The proposals by Backhouse and Dhillon (1996), Dhillon (1997) and McDermott and Fox (1999) are also affiliated with IS development methods. However, we considered these under responsibility modeling - where Backhouse and Dhillon (1996), Dhillon (1997) and McDermott and Fox (1999) have had more influence. That is to say, Backhouse and Dhillon (1996), Dhillon (1997) and McDermott and Fox (1999) have all adopted the idea of finding work responsibilities[6] as the key point of departure for securing systems. We also included an IS security planning approach (Straub & Welke 1998) into the paradigm of Security-modified IS.

Since this approach was not included in III (*cf.*, Footnote 5), we next briefly summarize an IS security planning methodology by Straub and Welke (1998). It includes four stages: recognition of security problems, risk analysis, generation of alternatives,

[6] Originally presented by Strens and Dobson (1993).

decisions and implementation. Even though this approach has some similarities with certain common-sense principles, *e.g.*, that of Parker (1998), this approach is not classified under this paradigm because of a fundamental difference compared to common-sense principles. Straub and Welke's (1998) approach is based on rigorous empirical research (and a theoretical framework), as opposite to common-sense principles.

We interpreted this approach as entailing both means-end oriented and interpretive *research objectives*. Although they endeavour to present a model that can be of practical use to managers (means-end oriented research objective), we see the attempt to increase managers' understanding of security management as an indication of an interpretive research objectives.

They have utilized action research, influenced by Schein's (1987) clinical approach, as the *research approach*. In terms of Järvinen's research approach classification, we see their study as theory-testing (they test and validate their model in practice using action research). Their view of the *organizational role* of IS security lies between the technical and socio-technical. On the one hand, they work contains several indications in favour of socio-technical means. For example, they stress the use of security awareness programs and criticize the current approaches as too technical, omitting the behavioural (or human) side of security. On the other hand, they see the role of awareness programs as a means by which a deterrence system can be introduced into organizations. The following citation indicates this: "A major reason for initiating this training [within a security awareness program], however, is to convince potential abusers that that the company is serious about securing its systems and will not treat intentional breaches of this security lightly." (Straub & Welke 1998 p. 445). This suggests a technical flavour in terms of organizational role of IS security. We interpret this to means that Straub and Welke (1998) don't see the ultimate goal of a security awareness program as a means for gaining employees' acceptance of or commitment towards security policy, as James' (1996) user participation and studies on information security awareness (*e.g.*, Spurling 1995, Thomson & von Solms 1997, 1998, Siponen 2000) emphasize.

With respect to the question of the *applicability to IS*, we see that this study does not propose any concrete means as to how this approach could be integrated into an IS development process.

In terms of the *meta-model*, the approach is at the organizational level. Countermeasures matrixes and awareness programs are all within the organizational context. Yet, this approach does not include modeling techniques in the sense of IS and software development methods, which would be at the conceptual and technical levels.

Security-modified IS development approaches (Baskerville 1988, 1989, Booysen & Eloff 1995, Hitchings 1995, 1996, James 1996, Straub & Welke 1998) favor all three *organizational roles of IS security*; however, the technical one was found to be the most common. The technical role was adopted by Baskerville (1988 1989), Booysen and Eloff (1995) and Straub and Welke (1998). Two approaches also entail socio-technical organizational roles of IS security (Hitching 1995, 1996, Straub & Welke 1998), whilst one preferred the social role (James 1996). The key *research objective* held by Baskerville, Booysen and Eloff, Hitching, James, Straub and Welke tends to be means-end oriented, although three of the security-modified IS development approaches (Hitchings 1995, 1996, James 1996, Straub & Welke 1998) also encompass interpretive

research objective. All use conceptual analysis as a *research approach*; in addition, three also adapted empirical theory testing research (Hitchings 1995, 1996, James 1996, Straub & Welke, 1998). When it comes to question *applicability to IS*, Two of these approaches can be integrated into normal IS/SW development. Security-modified IS development approaches offer modeling support at organizational and conceptual levels following the terminology of the *meta-model*.

Information modeling

The paradigm of information modeling or data modeling includes methods motivated by the desire to build security notations (*cf*., Hirschheim *et al*. 1995), particularly for developing secure databases (hence, the reference to data/information modeling). These works include Pernul (1992), Ellmer and coauthors (1995), Pernul and Quirchmayr (1994), Pernul and coauthors (1998). Their view on the *organizational role* of IS security is technical and their *research objective* is means-oriented. The *research approach* utilized is conceptual analysis. With respect to the question of applicability to IS, the integration of the security approaches of the information modeling community into IS/software development, is difficult due to the fact that the information modeling paradigm has adopted a low-level (technical) database development-oriented view, without any consideration as to how to integrate this into IS development. However, with some adaptation, this idea may be transferred to IS/SW development. Information modeling approaches offer modeling support on the conceptual level in terms of the *meta-model*.

Responsibility modeling

The advocates of the responsibility modeling paradigm believe that the security requirements can be found by exploring the role responsibilities in organizations. The use of responsibility as a basis for IS security development has influenced many researchers starting from Dobson, (1990) to Strens and Dobson, (1993), Thomas and Sandhu (1994) to Backhouse and Dhillon (1996), and Dhillon (1997). An approach by McDermott and Fox (1999) was also classified as belonging to this paradigm. Their views about the *organizational role* of IS security varies from technical to socio-technical, and the *research objectives* vary from means-oriented to interpretive. Conceptual analysis is most frequently used as the *research approach*. When it comes to the question of *applicability to IS*, most of the responsibility modeling approaches are still confronted with the problem of developmental duality as only one (McDermott and Fox) out of the four is clearly applicable to IS development approaches. Responsibility modeling approaches provide modeling support on the organizational level, following the *meta-model* for IS.

Security modeling and business process

The business process paradigm is presented by a German research group: Herrmann and Pernul (1998, 1999), Röhm and coauthors (1998), and Röhm and Pernul (1999). Their aim is to extend security issues into workflow and business process management. Here we analyze the approach by Herrmann and Pernul (1998, 1999). They have suggested a

framework according to which the security (mainly confidentiality) and integrity requirements of business processes can be modeled. The framework consists of a three-layered architecture for business process security, as follows. In layer three, the high-level security requirements of business processes are graphically analyzed. In the second layer, these are translated into more a formal, intermediate language, and the security elements are identified and divided into security blocks.

This framework is mainly concerned with layer three, providing five perspectives and their respective notations. The perspectives are the informational (represents information entities and their relationships; can be modeled using entity-relationship diagrams), functional (shows processes and data flows between different activities; can be modeled using data flow diagrams), dynamic (the possible states of each information entity; can be modeled by state-transition diagram), organizational (shows where something is being done and by whom; can be described by role models) and business-process (business processes, modeled by their own notation) perspective. Their *organizational role* is technical: their focus is on technical systems.

The *research objectives of* the Herrman and Pernul (1998, 1999) approach contain both means-end oriented and interpretive elements. Even though their ultimate point of departure is to improve the current situation, *i.e.*, lack of tools with which to address security aspects in workflow (Herrman & Pernul 1998) and business process (Herrman & Pernul 1999) management, an interpretive research objective is also present. Namely, modeling is needed to communicate the security requirements between the different people involved in the development in question (Herrman & Pernul 1998 p. 766). With regard to the *research approaches used*, they have used conceptual analysis and constructive research, employing the latter to sketch the modeling notation.

With respect to the question of *applicability to IS development*, we see that their approach succumbs to the problem of developmental duality. They do not address the issue of how their approach can be integrated into business process (IS development) approaches in general.

With respect to the *meta-model*, the informal perspective seems to correspond to the structured abstraction perspective (Entity-Relationship Diagram being at the organizational level) and a functional (data flow diagrams are at the conceptual level) by (Herrman & Pernul 1994) corresponds to Iivari's (1989) functional abstraction. The dynamic perspective corresponds perhaps to to Iivari's (1989) behaviour abstraction, on organizational and conceptual levels. A state-transition diagram is used to model the behaviour/dynamic perspective using the terms of Iivari (1989) and Herrmann and Pernul (1998, 1999), respectively.

Viable and survivable system approaches

Viable and survivable system approaches are proposed by Karyda and coauthors (2001) and Hutchinson and Warren (2000). Both Karyda and coauthors (2001) and Hutchinson and Warren (2000) have their roots in Beer’s viable system model, which consists of five systemic functions which need to be performed in order for an organization to be viable (or survivable). Nonetheless, they have three categories of differences. The first of these concerns the role of viable and survivable system approaches in the realm of IS security methodology. In this respect, Karyda and coauthors (2001) strongly advocate the viable

system approach as a paradigm shift in IS security thinking. They see that this consideration should be shifted from secure systems to what they call viable IS, *i.e.*, systems which stress survivability in future attacks. The view of Hutchinson and Warren (2000) is not so radical; they merely propose yet another IS security approach without arguing for its pre-eminence over alternative views on IS security thinking. The second difference emerges from the use of the viable systems model. Whilst we interpreted Hutchinson and Warren's idea as an approach for testing, or conceptualizing, organizations' vulnerabilities in the case of different attacks, Karyda and coauthors (2001) view its usefulness as an approach for designing secure or viable systems. Hutchinson and Warren (2000) investigate how different successful attacks are seen in the light of the five functions, whereas Karyda and coauthors (2001) endeavor to put foward a complete IS security design approach.

The third difference is that Karyda and coauthors stresses the survivability of an IS to accomplish its mission in a "dynamic environment". In our view that adaptability to a "dynamic environment" closely resembles the recent discussions on IS development in emergent organizations (*cf*., Truex *et al*. 1999, 2000), albeit Karyda and coauthors do not explicitly mention these.

We classified the *research objectives* of Hutchinson-Warren as interpretive, *i.e.*, the aim is to obtain an understanding of the vulnerability of systems by scrutinizing the potential attacks that may be made on an IS. Karyda and coauthors entails critical and means-end oriented *research objectives*. They argue that instead of focusing on secure IS, we should focus on 'viable IS': "[we] propose a new framework for building secure information systems, or as we suggest them to be called, viable information systems" (Karyda *et al*. 2001 p. 453); hence, the label critical view. As for the underlying means-end oriented research objective, this is identified by the whole idea of proposing a completely new approach aimed at achieving a secure (or viable) IS.

Both have used conceptual analysis as the *research approach*[7]. The *organizational role* in the Hutchinson-Warren Viable System approach is technical: their concern is with technical systems. When it comes to *applicability to IS*, the Hutchinson-Warren approach maintains the developmental duality between IS development and security development (the approach is applied afterwards to incorporate security into the IS). The organizational role in Karyda and coauthors (2001) is socio-technical; they value technical and social considerations as equally important: "In our view, an information systems is an human activity system comprising five elements, namely hardware, software, data, procedures and, above all, people…in order to support human activities in the context of an organisation." (Karyda *et al*. 2001 p. 454.).

On the one hand, Karyda and coauthors (2001) seem to recognize the problem of developmental duality (even they do not refer to it explicitly): "IS security should preserve the ability of the IS to deliver the required services to the organization, but most important to achieve the most effective coupling between the IS and the organization. The goal of IS should be the protection of the functionality of IS…"(Karyda *et al*. 2001 p. 458). They thus see it as vital that IS security development pays close attention to the organization's business requirements. On the other hand, we see a small drawback with

[7] We did not classify them as using a constructive research strategy as the construction of new artifacts were far and few between.

respect to integrating this approach into IS/software development methods in that they do not provide any concrete guidance as to how this can be done. On the positive side, we see that the idea of the "risk estimation diagram" may easily be added to many IS/software development notations. This can be done by embedding the risk factors in use (*e.g.*, putting a risk factor dimension in the textual description of a use case) or abuse cases (*cf*., McDermott & Fox 1999), data flow diagrams, etc. With respect to the *meta-model,* both are at the organizational level.

3.3 Information security management oriented maturity criterion

Studies suggest that the alternative methods for developing and managing secure IS are influenced by the IS/SW development methods of previous generations (Baskerville 1993, Dhillon & Backhouse 2001). It is interesting that perhaps the oldest approach, namely checklist-standard-based securing of IS (Baskerville 1993), has continued to exist. Even though the checklists are not a hot topic in the contemporary information security literature, their cognate method – security management standards (*cf*., Baskerville 1993, Dhillon & Backhouse 2001) – have received increasing attention from both information security researchers and practitioners (Fitzgerald 1995, Solms, 1997, 1998, 1999, Eloff & Solms 2000a, Eloff & Solms 2000b, Hopkinson 2001). Recently, following ideas and developments in the field of software engineering (*e.g.*, Pfleeger *et al*. 1994), a few new information security management-oriented maturity standards have been put forward, including The System Security Engineering Capability Maturity model (SSE-CMM 1998), an information security maturity approach by Murine and Carpenter (1984) and an approach by Stacey (1996).

Of all the standards targeted at management in the field of information security (*cf*., Solms 1996, 1999, Eloff & Solms 2000a), BS7799 has received the greatest interest, at least in terms of the sheer number of conference and journal articles. Utilizing the same gauge, it is surprising that the existing information security management-oriented maturity approaches, such as The System Security Engineering Capability Maturity model (SSE-CMM 1998), Murine-Carpenter 1984) and Stacey (1996), have not received similar attention. This is intriguing, given that the maturity ventures are currently the latest evolution of the checklist-management standard concept. In the field of software engineering, the comparable maturity paradigm has received a lot of both positive (*e.g*., Paulk *et al*. 1993, Kuvaja *et al*. 1994) and negative attention (*e.g*., Bollinger & McGowan 1991, Pfleeger 1999, Voas 1999, Rifkin 2001). The existing critiques of software engineering maturity models provide good lessons on the problems of maturity endeavours: why shouldn't we learn from our fellow scholars and practitioners in the fields of software engineering and IS, and thus avoid repeating the same mistakes again? Thus the aim of this paper is to scrutinize the alternative information security maturity approaches using these lenses.

Maturity endeavours started in the field of software engineering. The US Department of Defense (DoD) misjudged the ability of several its contractors to develop mature SW with the result that the DoD deemed it imperative to mobilize a maturity standard

(Bollinger & McGowan 1991, O'Connell & Saidian 2000 p. 28). Accordingly, several SW maturity criteria have been presented. Yet, several criticisms have been levelled against the SW maturity criteria. These problems about the existing software maturity models form the analytical framework of this study, *i.e.*, six lessons from which information security maturity criteria can learn. These perceived problems are summarized in table 5.

Table 5. The recognized problems of existing SW maturity approaches.

Problems
1. Do the criteria entail conventionalism or an operational focus?
2. Do the security maturity criteria entail naturalistic-mechanistic worldview?
3. Do the maturity standards support IS/SW development in emergent organizations?
4. Can the maturity criteria tackle the problem of the double standard?
5. Do the criteria succumb to spot focus fallacy?
6. What degree of ambiguity is present in the maturity criteria?

The framework (Table 5) has been synthesised from the existing discussion on software engineering maturity criteria.

1) Does the criteria entail conventionalism or an operational focus? Operational focus means emphasizing operational issues without any support for innovation (Rifkin 2001).

2) Do the information security criteria entails naturalistic-mechanistic world-view? It is argued that SW maturity criteria entail naturalistic-mechanistic world-view, which is seen to be too narrow to recognize that organizations are social systems (*cf*., Pfleeger 1999, Voas 1999, Abrahamsson 2002).

3) Do the maturity standards support IS/SW development in emergent organizations? (Bollinger & McGowan 1991, Truex *et al*. 1999, 2000, Baskerville & Pries-Heje 2001, Baskerville *et al*. 2001).

4) Can maturity criteria tackle the problem of the double standard? Double standard refers to the problem of distorting the truth with respect to maturity estimations (Bollinger & McGowan 1991, O'Connell & Saidian 2000).

5) Do the information maturity criteria succumb to the spot focus fallacy? The focus of inspection in SW maturity criteria is argued to be on predefined spots – not a holistic posture of overall maturity; hence, the label spot focus fallacy (Bollinger & McGowan 1991).

6) What the degree of ambiguity is present in maturity criteria? Such forms of ambiguity includes reference-only, subjective, partially objective and objective (Pfleeger *et al*. 1994).

The information security management-oriented maturity criterion is scrutinized from the viewpoint of the six lenses presented in table 5. Overall results are summarized in table 6.

Table 6. Security maturity criterion. the sign "+" indicates that the approach can cope with the issue "-" denotes that the approach in question succumbs to the problem "?" indicates an open question.

Problems	SSE-CMM	Information Security Program Maturity Grid	Murine-Carpenter maturity criterion
Operational focus	-	+	-
Naturalistic-mechanistic	-	+	-
Stable vs. emergent	-	+	+ ?
Double standard	-	-	-
Spot focus	-	+	- ?
The degree of ambiguity	-	-	-

In that The System Security Engineering Capability Maturity model (SSE-CMM) does not support innovations (operational focus), it succumbs to the fallacy of the naturalistic-mechanistic view. SSE-CMM assumes a very stable environment, and only peripherally touches on the issue of double standard, while not providing any concrete guidance on this matter. SSM-CMM succumbs to the fallacy of the spot focus as the process areas are prefixed, and entail all degrees of ambiguity.

The Information Security Program Maturity Grid can cope well with innovations, and it does not make naturalistic-mechanistic assumptions. Moreover, it is able to incorporate the requirement laid down for secure IS/SW development in emergent organizations with increasing success in the higher stage; and it does not address the issue of double standard. It avoids the fallacy of the spot focus, particularly in the highest stage in terms of maturity, owing to the fact that it requires organizations' security development to be in synch with organizational business requirements and the prescriptions are expressed at a very high level of abstraction. With respect to the degree of ambiguity, the Information Security Program Maturity Grid entails both reference-only and subjective views.

Murine-Carpenter maturity criterion does not support innovations, and it requires naturalistic-mechanistic assumptions as it aims to sketch a quantifiable maturity criterion. With respect to stable vs. emergent, it prescribes universal milestones which, even though these are in conflict with the idea of IS/SW development in emergent organizations, are only applicable at the very highest level of abstraction. At the lower levels of abstraction, developers are able to choose freely the techniques they prefer. Hence, it may suit

organizations desirous only of improving their SW security without any social concerns in an emergent environment. It does not pay any attention to the issue of double standard. The criterion seems to entail the spot focus fallacy. The reason is that the five milestones are universal. It also includes all degrees of ambiguity.

3.4 Synthesis of the analysis

The origins of the different SIS approaches can be traced back at different levels of abstractions to research communities. Here the concept of community refers to different sets of researchers sharing a certain orientation, whether owing to their education, upbringing or personal/work experiences. First, going from the bottom up, different IS security endeavours can be retraced to five "disciplines of information security": IS security, computer security, practitioners, database security and cryptology (Figure 5).

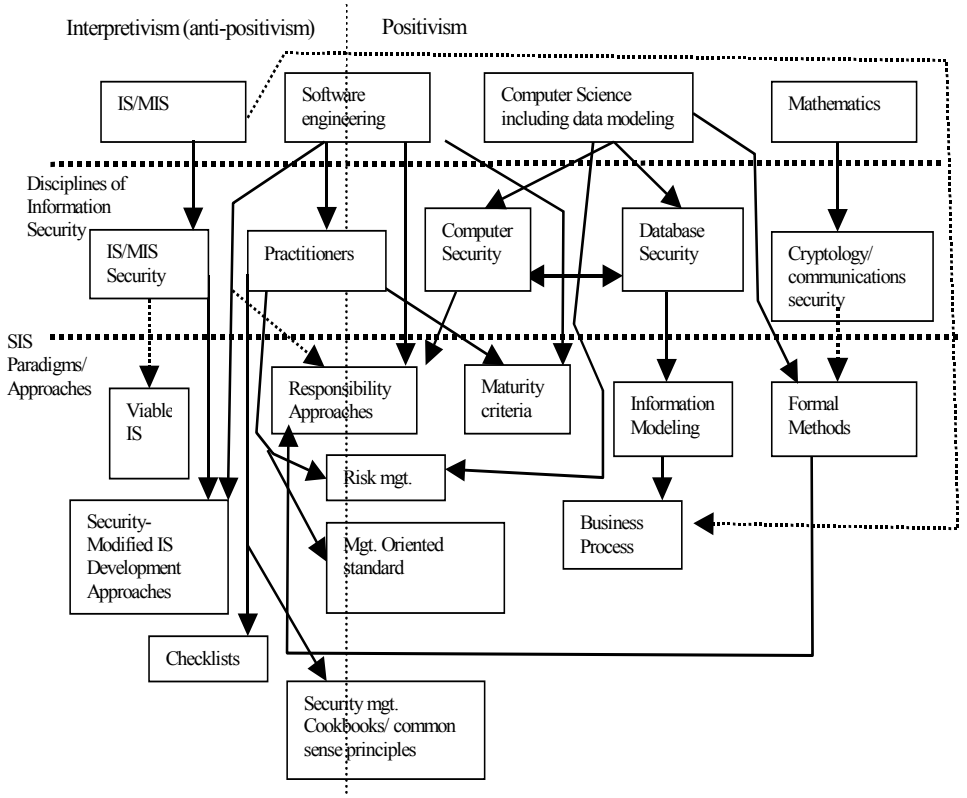


Fig. 5. The background and influences of different SIS approaches. The arrow shows influences. The dotted lines illustrate a weak influence.

Security-modified IS development approaches are influenced by the work of the IS security (*e.g.*, Baskerville 1988, 1992), IS and software engineering communities. Responsibility approaches may be associated with the IS security community and perhaps further with an IS community. One responsibility approach (McDermott and Fox) is influenced by the software engineering community. The Information/data modeling community has considered the security aspects from the data modeling point of view, aimed at extending the existing research in database security and their underlying philosophy of science is positivism[8]. The background of database security can be further traced back to computer science (including data modeling). Even though database security can be seen as a part of computer science, we may distinguish the information/data modeling community from the Computer Science community in the respect that the information/data modeling community has concentrated on security issues specific to databases (*e.g.*, Jajodia & Sandhu 1995), while the Computer Security community has concerned itself with the security aspects of computers in general, adapting technical means only (Baskerville 1988 p. 5, Brinkley & Schell 1995). The business process approaches are weakly influenced by the IS community. The point of departure of business process approaches is to construct a modeling notation for modeling security constraints in business process models (business process models are interpreted as falling within the domain of IS research issues).

The viable or survivable system paradigm (Hutchinson & Warren 2000, Karyda *et al*. 2001) is also slightly influenced by the IS security community. Despite the fact that Karyda and coauthors (2001) stress the role of humans and takes a social view in developing/managing secure IS/software – this is a common feature found among the authors of security-modified IS development approaches (Baskerville 1988, 1989, Hitchings 1995, 1996, James 1996) – they have not been classified under the paradigm of security-modified IS development approaches, as they stem from Beer's system model.

The Computer Science and Computer Security community has deep roots in positivism (Hirschheim 1985, Denning *et al*. 1989). Positivists claim that the universal research approach in the exact sciences (*e.g.*, mathematics) should form the basis for research in all fields of science (Stroll & Popkin 1979, Hirschheim 1985, Scruton 1995). Yet, the Computer Security community clearly (without explicitly expressing it) favours the ideas of Popperian falsification. This means that theories are preliminary rather than final, and theories must be made as explicit as possible (Popper 1985). This view can be seen in Thomas and Sandhu's (1994) and McDermott and Fox's (1999) works on responsibility modeling.

Practitioner community refers to a set of practitioners working in the field of information security who may not have a serious academic research attitude. The "research" problems of practitioners often arise from their personal practical experiences (hence, the label practitioners) rather than research problems and agendas put forth by research colleagues in scientific journals/conferences. Additionally, the "research" approach of the practitioner community is not very academically disciplined in the sense that they do not, for example, use research methods (and may neglect related research),

[8] Refers to the view according to which the methods of natural science form the basis of all the sciences, so that *e.g.*, social science phenomena are not seen as differing from those in natural sciences (*cf.*, Ray 2000).

but rather base the solutions (and validation of the solutions) on their own intuitions or personal experiences. As can be seen from figure 5, the practitioner community tend to propose normative standards (including information security checklists, management standards and maturity criteria), risk management and common sense principles. Risk management, normative standards, responsibility approaches, and common sense principle approaches have adopted the philosophies of positivism and interpretivism (or anti-positivism). Of normative standards, information security management-oriented standards and maturity standards also entail positivistic assumptions by aiming at capturing mechanistic-causal laws. Checklists can be seen to be more interpretivist than other normative standards, given that they do not stress the universal applicability of the security controls. With respect to the responsibility approaches, two such entail positivistic assumptions, (Thomas & Sandhu 1994, McDermott & Fox 1999), as discussed earlier, but there interpretive (anti-positivistic) approaches to responsibility modeling also exists (Backhouse & Dhillon 1996, Dhillon 1997).

Formal development is particularly favoured by the computer science community, but we see the influences coming from cryptology as well. Both formal development people and cryptologists have embraced one of the hallmarks of positivism, namely adherence to formal languages as a solid theoretical base on which to design secure IS. Indeed, Descartes (1596-1650) insisted that if a belief is either false or doubtful it should be rejected: "…*care must be taken not to admit anything as true which cannot be proven to be true*" (Scruton 1995 p. 28). Such doubt and the demand for formal proof is, in particular, shared by both formal method people and cryptologist.

The five disciplines of information security can be further retraced to four fields: IS, software engineering, computer science and mathematics (Figure 5). In other words, as cryptology is a part of mathematics, IS security scholars are part of the IS community (or at least influenced by the ideas in the field of IS), while computer and database security scientists come from a computer science background. Software engineering refers to "the practical application of scientific knowledge in the design and construction of computer programs and the associated documentation required to develop, operate, and maintain them" (Boehm 1976 p. 1226), *i.e.*, practical means of developing software (Sommerville, 1996, Jaaksi 1998). In addition, some software engineers stress positivism, *i.e.*, the vitality of applying the method of natural sciences in the development of software (*e.g.*, Boehm 1976, Humphrey 1988, Basili 1996, Basili & Lanubile 1999), whereas a few software engineering thinkers disagree with this view (Pfleeger 1999). Hence, software engineering is classified as belonging to the domains of positivism and interpretivism (or anti-positivism)[9]. One security-modified approach, namely Booysen's and Eloff's (1995)

[9] Interpretivism, here considered as synonym for anti-positivism, refers to views that regard traditional positivism (social science phenomena do not differ from those of natural sciences; hence, the methods of natural science form the basis of all the sciences) *per se* as too restricted philosophy for IS. Interpretivists (or anti-positivists) claim that social science phenomena are different from natural science phenomena, and therefore research on human phenomena requires different research approaches. Interpretivists stress that research is carried out by subjective human beings and thus cannot be objective (*i.e.*, found objective facts), but human behaviour needs to be understood in terms of social interaction and qualitative experience (*cf.*, Susman & Evered 1978, Hirschheim 1985). It should be noted that the use of terms 'positivism' and 'interpretivism (or anti-

spiral approach, is also influenced by software engineers. In this classification, computer science and software engineers are regarded as separate disciplines, following McDermid and Bennett (1999), Parnas (1999) and Tremblay (2000). Computer science initially originated from electrical engineering and mathematics departments (Ramamoorthy, 1976 p. 1200). Computer science relies on mathematics (O'Leary 1997, McDermid & Bennett, 1999). Yet, computer science is more theoretical and independent of practical application, aimed at fulfilling scientific goals (knowledge), than software engineering that is strongly driven by problems in real practice (McDermid & Bennett 1999 p. 179).

While software engineers have also employed ideas from social sciences (Sharp *et al*. 2000), software engineering differs from the field of IS (*cf*., Davis 1999, 2000) in the sense that the IS community takes into account the social and organizational aspects (Baskerville 1988, Dhillon 1997) and uses a variety of research approaches, also those common to social sciences (*cf*., Lyytinen 1991, Walsham 1993, 1996, Järvinen 1997, 2000). Even though IS scholars have adapted both positivist (*e.g.*, Lee 1989, 1999, Boudreau *et al*. 2001) and interpretive (Hirschheim 1985, Lacity & Janson 1994, Walsham 1993, 1996, Klein & Myers 1999) research strategies, we see the existing SIS approaches that belong to security-modified IS development paradigm and are influenced by IS (security community) rather interpretive than positivistic. Therefore the security-modified IS development paradigm is classified in the domain of interpretivism (*cf*., Figure 5). Of the security-modified IS development approaches, IS security planning methodology (Straub & Welke 1998) is interpreted as lying on the border between positivism and interpretivism. IS security planning methodology, on the one hand, has adopted an interpretive research strategy, including action research[10], which we see as implying interpretivism using the positivism/interpretivism classification employed in this study. On the another hand, their theoretical frameworks stem from quantitative studies (*e.g.*, Straub 1990) that are interpreted as positivistic.

Baskerville (1988, 1992) proposed a generational classification of IS security approaches. Following his lead, we offer an updated version of this generational classification including the disciplines of security (Figure 6)[11].

---

positivism)' in this thesis has been simplified; there exist many forms and definitions of positivism and interpretivism, including anti-positivism (*e.g.*, Stroll & Popkin 1979, Hirschheim 1985).

[10] Although action research is often regarded as a hallmark of interpretative or anti-positivistic research (Susman & Evered 1978, Badger 2000), positivistic forms of action research are also argued to exist (McCutcheon & Jung, 1990).

[11] Baskerville's (1988, 1993) classification does not include responsibility modeling, information modelling, formal method approaches, and most of security-modified IS development approaches and the disciplines of security.

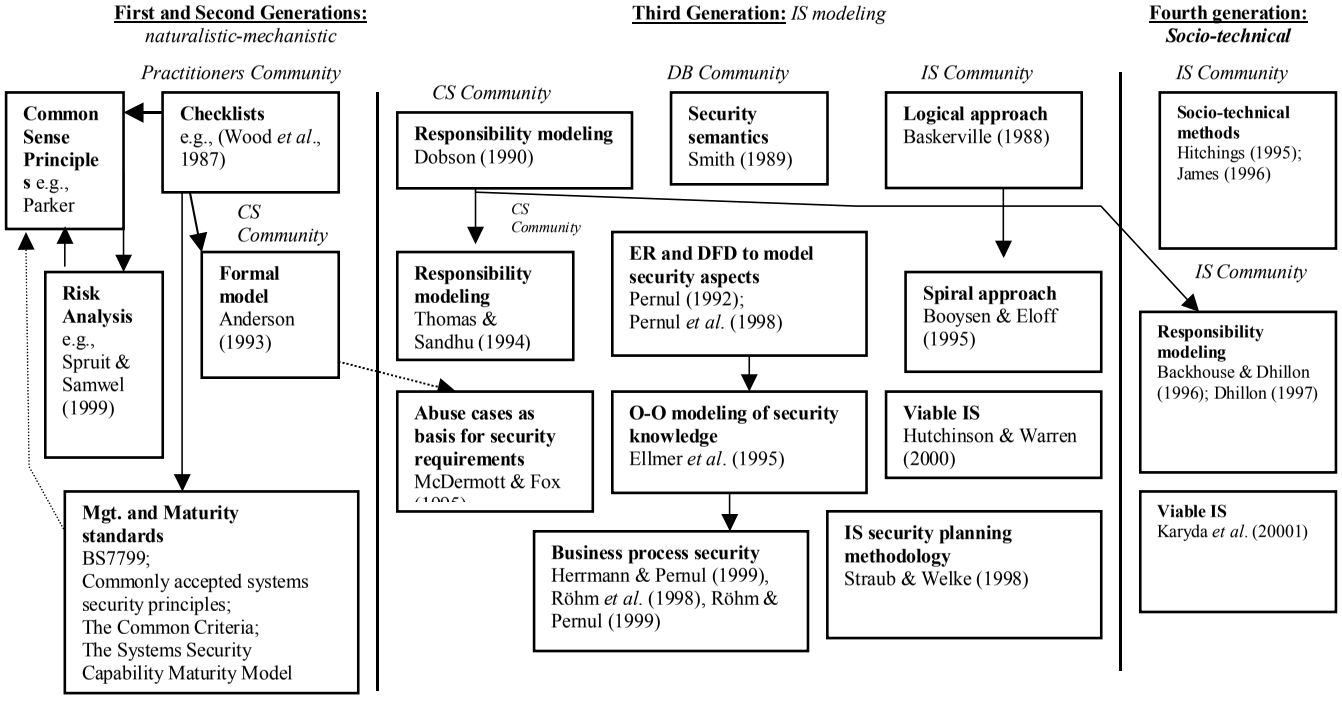


Fig. 6. An overview of the SIS generations and paradigms. The generational divisions are separated by lines. The arrow shows influences or inspirations (since the influence of work by earlier authors is very weak). Broken arrows mean that the approach is influenced by the deficiencies of certain approach or other. This also means that figure 6 is chronological: SIS approaches at the bottom of figure 6 are more recent than SIS approaches described at the upper end of the figure.

Figure 5 also includes research communities, which should not to be confused with the term paradigm (even research communities can be seen as paradigms).

In figure 6, the first and second generational methods are naturalistic-mechanistic. First and second generations approaches/methods are aimed at finding out what can be done, with the help of available technical solutions (Baskerville 1988, 1992). To put it philosophically, they violate Hume's law "no ought from an is" (*e.g.*, Popper 1948, Hare 1963, 1964a, 1986). Proponents of the first and second generational SIS design approaches claim to infer "ought" (what organizations should do) from "is" (what is possible to do, or what there exists), but there is no logical connection between the two. In fact, first and second generational approaches particularly present general, even universal, information security imperatives founded on the basis of the existing techniques/practices. Hence, first generation approaches deserve the label naturalistic, stemming from the "is from ought" inference. The second generational methods differ from the first generation in the fact that second generation recognize organizations' security requirements and are aimed at taking these into account with the help of control points, for example (Baskerville 1993).

The term mechanistic illustrates, on the one hand, the emphases on the functional, technical and natural science type of attitude to SIS design and on not paying attention to the social nature of organizations (Baskerville 1993, Dhillon & Backhouse 2001).

At this point it should be noted that some of these methods include elements from other generations. For example, formal development includes modeling *a la* logical positivists (*cf.*, Hirschheim 1985, Klein & Lyytinen 1985, Ray 2000), but since it lacks comprehensive modeling support it is not included in the modeling (third) generation (*cf.*, Baskerville 1993). This means that we found formal development approaches to lack modeling language, which with the help of *e.g.*, system requirements are communicated via developers and users/customers.

Third generational approaches include IS modeling, and fourth generational methods emphasize socio-technical design (*cf.*, Baskerville 1988, 1993). User participation utilized by James' security-modified IS development approach (1996) is an example of a fourth generational socio-technical design approach. A notable difference between first/second generations and generations from the third generations onwards, is that the later generations do not attempt to derive "ought" from an "is," in contrast to the first and second generations. In other words, the later generations take the organizational requirements as a point of departure, and do not just substitute the organizations' unique information security requirements for a generic list of predefined protection means invoked by outside information security gurus. Since the information modeling and business process paradigms focus heavily on modeling they are classified under the third generation. The viable approach of Hutchinson and Warren (2000) is incorporated into the third generation domain due to the technical organizational role attributed to IS security, whilst the approach by Karyda and coauthors (2001) is classified under socio-technical methods owing to the socio-technical role it entails.

This division of generations, which is an updated version of that of Baskerville (1988, 1992), is debatable, particularly if one argues that the different generations are better viewed in increasing order. However, all generations, paradigms and respective approaches come with their own sets of shortcomings. When considering the relevance and applicability of certain approach to certain practical situations, one should bear in

mind the context (*e.g.*, organization, environment) where an approach will be applied (*cf.*, Dhillon & Backhouse 2001).

As for practitioners, the important thing is to recognize the alternative paradigms and respective approaches/methods as well as understand the principles, weaknesses and strengths thereof. Hence, this dissertation does not aim at putting forth a waterproof classification of existing SIS design endeavours, but rather it aims at increasing our understanding of the different SIS design methods. The concept of generations can be seen as the highest level of abstraction, whereas paradigms, approaches/methods, and techniques/principles constitute the lower levels of abstraction, respectively (*cf.*, Iivari *et al*. 2001).

4 A Paradigm for extending security in IS/software development methods

In order to tackle the four problems identified earlier, the creation of a novel SIS design paradigm was seen to be a legitimate and major research contribution. This solution is discussed in this chapter.

First, a meta-notation is constructed to address the four problems. They are: that (1) different SIS design approaches cover the different levels of IS, but lack the comprehensiveness needed; (2) most of the approaches for designing SIS are difficult to integrate into IS development methods; (3) existing SIS design approaches do not assist the autonomy of developers; and (4) new IS development methods spring up very occasionally; however, given the trend of current SIS design approaches, security approaches always seem to come a few steps behind IS development methods. Second, to study empirically the applicability of the proposed meta-notation in practice (theory-testing research), an action research intervention (Schein 1987) was carried out in an organization. This action research turned out to be facilitative-clinical type of action research, where there is no cyclical process and the role of the researcher is facilitative (*cf.*, Schein 1987, Baskerville & Wood-Harper 1998)[12].

The action research interviews with a technical project manager and a developer were recorded as part of this action research.

It is natural for action research to focus on a single organization, as in this study. We searched for a software development organization with security development problems, and discovered an ideal research setting, a local film- and media production center in Northern Finland, called POEM. Established in 1997, POEM is a film and production center aimed at facilitating regional film and media production. In 1999, POEM recognized the potential of the Web to support their business activities, and hired people to achieve this goal. With respect to their business goals, POEM wanted to build a web-based database for scouting and infrastructure for the distribution of films and movies

[12] The type of action research done depends on the setting in question and cannot be known beforehand. For example, it is difficult, if not impossible, to estimate before the action research project is carried out what is the role of researcher (*e.g.*, facilitative) will be, or whether there will be one or more cycles.

through the Internet. To further improve their IS and software development practice as a means of achieving the aforementioned goals, POEM participated in the collaboration OWLA-research project carried out between the University of Oulu and several industrial organizations. POEM hired a Finnish software house to develop parts of the functionality of the IS. Because POEM intended to handle their business-related activities (scouting database, distribution of digital products), through the Internet, there was a crucial need to address the respective security concerns.

The role of researchers in the development reported here was to support both POEM and one of the software companies hired by POEM to develop POEM's systems. This software company followed an object-oriented modeling notation as the basis of their IS development. However, they were unable to address their security concerns with the current method in use and practice, as the following statement by a technical project manager of the company illustrates: "We did not have such [security methods] as we have for [normal IS/software] design and modeling … [but the design and modeling techniques we are currently using]... concentrate on doing software. We don't have a method which includes security aspects."

The company's incentive for the adoption of a method was to fill this gap of lack of notational support with respect to security aspects in their development practice.

This meta-level viewpoint could provide a possible avenue for addressing the four types of problems previously identified. Rather than present yet another security approach with its own novel security features, we propose that SIS design approaches must be elevated a level of abstraction above the barriers. Moving a level away from methodology takes us into the realm of meta-methodology, a new paradigm for SIS which will help developers to use and modify their existing methods as needed.

The meta-method level of abstraction offers a perspective on ISSD methods that are in a constant state of emergence and change. Hardly any systems problem setting is an exact repeat of a former setting, and hardly no method can actually be applied exactly the same way every time. This idea of the modification of ISSD methods is well known in practice (Kumar & Welke 1992, Madabushi *et al*. 1993, Slooten 1996, Jaaksi 1998), and also discussed in academic works (Malouin & Landry 1983, Kokol 1996, Plihon & Rolland, 1997, Truex *et al*. 2000). Neither, however, are systems problem settings and development approaches in total chaos and relativism. In other words, different development situations are not totally disparate. Otherwise, our earlier practical and empirical experiences on, say IS development, would have no value for the IS development tasks that will confront us in the future (*cf*., Hare 1986, Niiniluoto 1991). Instead developers recognize regularities or patterns in the way problem settings arise and methods emerge.

We used the following analytical process for discovering the pattern of security design elements. First, we looked across ISSD and IS security development methodologies in order to find common core concepts (subjects and objects). Second, we surfaced the patterns in existing SIS methods (chapter two of this thesis) resulting in four additional concepts (security constraints, security classifications, abuse subjects and abuse scenarios, and security policy). Finally, we consulted a panel of practitioners for comments about the patterns. This process led to a pattern with six elements. While some computer security researchers, particularly cryptographers, distinguish other security elements (*e.g.*, Menezes *et al*. 1997), the six described below proved to be sufficient for

our purposes in capturing most of the common patterns found in systems security development. Additional elements can certainly be added to the meta-notation on an ad-hoc basis as required. To summarize, the meta-notation includes six dimensions:

- security subjects;
- security objects;
- security constraints;
- security classifications;
- abuse scenarios;
- security policy.

These are utilized when needed. In other words, all dimensions need not be applied *pro forma*[13]. The terms security subjects and objects are commonly used in database security literature to describe computer access control policies and models (*e.g.*, McLean, 1990, Foley 1991, Sandhu 1993, Castano *et al*. 1995, Summers 1997). ISSD development concepts such as the 'actors', 'entities' or 'objects' can be mapped to security subjects and objects. Security classification stems from the need to classify security objects and subjects according to their information security sensitivity. Abuse subjects is a special class of security subjects referring to those that may carry out a security violation. The introduction of abuse subjects and abuse scenarios, influenced by McDermott and Fox (1999), may be needed for two kinds of situations. First, they may come in handy when there is a need to explore and identify what potential threat scenarios exist. Second, it is relevant for testing purposes. It helps to check that the system and software under design can cope with unwanted scenarios or attacks by unauthorized people or processes.

Security subjects denote the different security relevant entities, *i.e.*, entities that have a relevant security connection to the assets of the organization (security objects). Security subjects may include automated processes, network nodes, employees of the organization, business partners and third parties. Given that they have a security-relevant connection to the assets of the organizations, actors in use cases and stick figures in rich pictures are security subjects.

The term security objects refers to the assets of the organization that are of relevance in terms of information security. Such assets (security objects) may range from physical things such as paper to electronic entities such as files. In other words, putting it in terms of IS development, security sensitive objects, which actors access for some purpose, are potential security objects.

Security constraints may include write access, read access, etc. Security constraints may be discovered by analyzing the security requirements (confidentiality, integrity, availability and non-repudiation) for each security object. In order to pragmatically define the kind of access (*e.g.*, read, write, etc.) to objects that subjects need, a security classification of the security objects and security subjects may be relevant. If this is the case, subjects are classified according to their security sensitivity and need-to-know. For example, one may classify security objects and subjects into three categories: confidential, secret and top secret. V includes an example of an application of these dimensions.

[13] Note that in V "A new paradigm for adding security into IS development methods" there are only five dimensions; the dimension of abuse scenarios was added later.

4.1 Results of the intervention

Requirements analysis in the form of interviews was conducted with an analyst working with POEM along with a researcher. The analyst had early experience with development of the parts of the POEM system. The researcher collaborated clinically with the analyst to convert requirements into use cases. The recorded interviews and the preliminary use cases were sent, together with a written description of the meta-notation, to the project manager of the software company responsible for development of this part of the system. The software company then modified and made more use cases by following the meta-notation. The company responsible for developing the system reported that the meta-notation was simple and extremely useful, and they acquired a good understanding about the meta-notation and experiences thereof were recorded in an interview session.

As mentioned above, the action research “success” criteria hinge on the validation of theories through use as defined in the social reflection of the collaborators in the research. Under these criteria, the theory would seem to be well validated. The following reflective evaluations of the method by the practitioners involved in the project illustrate this validity. The following citations are taken from the interviews with the project manager of the software house and a developer.

The meta-notion method was found to be very simple and usable: "It was clear, some new lines were added [into the diagrams]." In fact, an analyst expected the meta-notation to be “much more difficult” as “usually methods [by academics] are complex and hard to understand, but this [meta-notation] was surprisingly clear.” All developers generally seemed to understand the terms. According to a developer, the concept of “security policy/specific security restrictions was the hardest.”

Also one developer found the concept/dimension of “access types to security objects” difficult to understand at first sight, but after considering the example describing the meta-notation, “everything became clear in the end”.

The developers did not identify anything missing from the meta-notation. The next citation illustrates this view: “Nothing [was missing]. I did not see a lack of anything.” Another commentator notes: “I can't think of anything to add.”

The developers regarded the meta-notion as useful and relevant. At the beginning of collaboration, the technical project manager of the software house felt that the meta-notation appeared to be ”remarkably better than the normal use case template for this purpose [*i.e.*, to develop the required software].” The following example also illustrate this: “This [security enriched use case] is much smarter than the normal use case, whether for security use or not.” According to another developer, the meta-notation was “OK. Useful extra fields [*i.e.*, the six security dimensions] were added to it.” The developer and the technical project manager of the software house agreed that they would use this information security meta-notation later: "Yes, if there were need for security”. Another developer commented that: “Yes, [I would use it]… immediately when we meet something with this kind of security [requirements]. This can be quite handy.” Another developer said: “it felt simple so I'm sure I would use it again [if there is a need for address security aspects].”

The overall evaluation of the meta-notation by an analyst and the technical project manager of the software company responsible for the development of the system was

positive. The technical project manager said: "[in rating from 1 to 10] I would give it eight out of ten." The analyst evaluated the meta-notation as "10 [out of ten]. Just add some lines [into the notation] and put the rest in there".

4.2 Relevance and validity of the results of the intervention

Next, findings of the action research on the meta-methodology paradigm and the resulting meta-notation are summarized, showing how the research endeavours to address the four problems confronting existing SIS design methods/approaches. The result suggests that meta-methodology formulation has a degree of both theoretical and practical strength. The paradigm is formulated with a theoretical framework that addresses SIS from a higher level of abstraction than is typical. A meta-method approach redefines SIS design methodology. Existing SIS methods have not provided the broader context that enables us to identify and overcome the barriers. The practical strength of the new approach is revealed in action research. The action research also provides a degree of empirical validity for the theoretical framework.

The first barrier arises because the existing SIS design approaches lack comprehensive modeling support (as noted in the third chapter). The meta-methodology approach embraces the ideal that no single approach provides a comprehensive modeling support. Following the higher level of abstraction, we are led to propose a meta-notation consisted of six dimensions. Developers can select from these six elements those elements that are relevant for the design setting (one does not have to apply all six elements just *pro forma*). In demonstrating the empirical validity through action research, we have also recognized that this meta-notation provides new methodological support for security aspects of web-based IS. This provision is an important implication given the rapid rise in the prevalence of this form of SIS.

The second barrier arises because many of the existing approaches cannot be integrated into ISSD methods (developmental duality). This solution avoids the problem of developmental duality. This meta-notation can be added to existing notations for modeling IS or software. Within the new paradigm, it is possible to contextualize security specific notation in existing and proven modeling notational schemes.

The theoretical framework indicates that the combined modeling approach will allow security and functionality to be consistently modelled. The practical success of the facilitative-clinical action research solution supports this claim.

The third barrier regards the autonomy of developers; the need for them to select and use the methods they prefer as a basis of ISSD. Existing security approaches constrain this autonomy in developing SIS by limiting developers to secure development methods. The new paradigm adapts security design to the preferred methodology. The practical success of the facilitative-clinical action research solution also supports this facet of the theoretical frame.

The fourth barrier arises in the need to design systems in organizations known to be emergent and evolving. Methods suitable for emergent organizations need to be routinely modified by practitioners to fit regularly changing situations. The practical setting of the

facilitative-clinical research provides only limited support for this claim, since the paradigm was applied in a one-shot fashion. The ease with which the notation was adapted implies further adaptation will occur with equal ease, but this cannot be confirmed from the facilitative-clinical case described in this part of the thesis.

Validity of the results. The research described in this part of this thesis tests the relevance, feasibility applicability of the paradigm of meta-methodology by testing the notation in practice in an action research setting. Action research was selected because it is known to be the most suitable research methodology for initial testing and possible adjustment of the approach. The action research ended up as the facilitative-clinical type of action research (*cf.*, Schein 1987, Baskerville & Wood-Harper 1998). As a result of this, the empirical research turned out to be theory-testing.

The research in this part of the thesis conforms to the seven validity criteria for IS action research (Baskerville & Wood-Harper 1998). First, the research was set in the multivariate social situation involving a complex relationship between an ISSD contractor and their client. The client required a SIS. Second, the observations were recorded and analyzed in an interpretive frame. Windows into this data and the interpretation have been provided. Third, the researcher actively intervened, working directly with the ISSD developer to introduce the new paradigm into their practices. Fourth, the method of data collection included participatory observation as well as interviews. Fifth, the outcome of the ISSD process was assessed in terms of the collaborators' reviews of the usability and success of the modified ISSD approach and the ISSD modification process. Sixth, the immediate problem in the research was resolved during the research according to the evaluation of the collaborators. Finally, the actions in the setting were tightly linked to the meta-methodology theoretical framework. This framework defined the actions and explains clearly how the actions led to the favorable outcome.

To summarize, the facilitative-clinical action research experience suggests that the meta-notation was relevant in use, feasible, and easily applied for extending normal ISSD security. With regard to limitations on this validity, the key to success to action research is that both researchers and practitioners in participative organizations have an agreed understanding of what is going to happen (Mumford 2001a p. 20). Perhaps the fact that the company developing the software had a concrete (and therefore high) motivation to adapt a workable solution was a key factor with respect to the general success of the action research intervention.

5 Discussion

This dissertation aimed at exploring how information security considerations can be added into existing IS development methods. This process was divided into three research questions that are recapitulated in the following (Table 7).

Table 7. Research questions and respective results

Research question	Results
To what extent are IS security issues examined and resolved by existing research?	Information security research issues are mainly solved via technical solutions developed following the paradigm of the natural science
What are the underlying assumptions, differences, commonalities and strength and weaknesses of the existing SIS approaches?	Recognition of similarities and differences of alternative SIS design paradigms/approaches, increased understanding of the underlying foundations of the existing SIS design approaches and possible weaknesses thereof, and suggestion of several implications for researchers and practitioners on the basis of this analysis
How can security issues be tackled by IS/SW development methods?	A meta-notation that can be applied to existing modern IS/SW development methods

5.1 Findings

RQ1: to what extent are IS security issues examined and resolved by existing research? The analysis shows that information security research in general, has focused on technical issues (such as access on the technical level). The main reference disciplines utilized have been mathematics and philosophical/mathematical logic, and the dominating research approach has been mathematical modeling (logic). Yet, answering the first research question revealed that, from an IS security management viewpoint, further research is needed with respect to several issues. Empirical studies on how to ensure that users are committed to security policy and the role of deterrence and rewards

in halting computer abuse are particularly to be welcomed. There is also room for studies (perhaps based on conceptual analysis) pondering the usability of ethics or human morality with respect to computer abuses/security violations and how to construct consistent security guidelines for emergent organizations. As far as emergent organizations are concerned (*cf*., Truex *et al*. 1999, 2000), future research should focus on the process of developing and managing secure IS and identifying what development processes and strategies emergent organizations should follow. Also from the secure IS design viewpoint, studies that provide organizational level modeling are needed. Moreover, ideas with respect to what modeling requirements in terms of security will be brought along with the use of web information systems (Isakowitz *et al*. 1998, Schwabe & Rossi 1998, Oinas-Kukkonen *et al*. 2001) should be added to the list of future research topics.

RQ2: What are the underlying assumptions, differences, commonalities and strength and weaknesses of the existing SIS approaches?

Several approaches for developing and designing secure IS/software have been put forth. Due to recent comparative studies (Dhillon 1997, Dhillon & Backhouse 2001), the IS security community has a certain understanding of the alternative SIS design approaches, including their theoretical and philosophical underpinnings. The objective of this thesis, and the second research question particularly, was to complement these contributions. In order to do this, alternative SIS design methods/approaches were first classified in terms of paradigms for developing secure IS – namely conventional (normative standards, risk management, common sense principles and formal development) and contemporary (Information/Data Base modeling, responsibility modeling, and the security-modified IS development, business process security and viable IS). These approaches can be seen as alternative paradigms, as they advocate different ways of designing secure ISs. These paradigms are not mutually exclusive, in that an information security maturity criterion, for example, may advocate the use of risk management techniques and/or formal methods (as SSE-CMM in fact does), and may include some common sense principles. In spite of this, it is relevant and insightful to scrutinize these paradigms separately. In fact, all the approaches within these paradigms, have been proposed as stand-alone methods as well. An overview of the implications analysing the existing myriad of SIS design endeavours are presented (Table 8).

Table 8. Implications in the light of different viewpoints.

Viewpoints	Findings	Implications
Research objectives	Mainly means-oriented	Alternative approaches are needed
Organizational role of IS security	Mainly technical	Alternative approaches (more socio-technical, social) are needed
Research approaches	Conceptual analysis was the research approach most used	Additional empirical studies are needed
Applicability to IS or software development	Most of the SIS design approaches cannot be integrated into IS or software development	SIS design approaches cannot be integrated into IS development. More guidance is needed about how this could be done
Meta-model for IS	The approaches were not comprehensive: they primarily give organizational level support	Given that all levels of IS are relevant to the model, new approaches that can provide comprehensive support are needed

The most commonly held *organizational role of IS security* was the technical view. As for the conventional paradigms, the technical view was the most commonly accepted. With respect to contemporary approaches, the technical view is held by the database/information modeling community, business process community, responsibility modeling people (Dobson 1990, Strens & Dobson 1993, Thomas & Sandhu 1994), Viable IS (Hutchinson & Warren 2000) and security-modified IS development approach (Baskerville 1988, 1989, Booysen & Eloff, 1995, Straub & Welke 1998). The socio-technical view is held by James (1996), Hitchings (1995, 1996), Backhouse and Dhillon (1996), Dhillon (1997), Karyda and coauthors (2001) and McDermott and Fox (1999). This results in practitioners having only technical approaches available to them, and a few socio-technical ones, when setting out to choose an IS security development approach. Many recent authors (*e.g.*, Baskerville 1988, Dhillon 1997, Dhillon & Backhouse 2000) have strongly advocated the relevance of the socio-technical role, mainly arguing that a technical "engineering" approach is too technical in an organization, which in any case is a social institution (Dhillon & Backhouse 2001). Nevertheless, one may regard approaches entailing a wholly technical view of the organizational role of IS security *per se* as morally questionable in social settings, as they are likely to violate the Kantian imperative of human dignity (by treating people only as means). Even though all the approaches may be seen to have particular purposes of their own (*cf*., Iivari & Hirschheim 1996), the technical approaches, for example, may in fact be adequate for certain types of computer systems that have a limited social-organizational dimension. An example of the social view on the organizational role of IS security is the security-modified IS security approach by James (1996). She was perhaps the first to embed user participation in the designing secure IS. However, user participation may be rejected by security personnel. They may see that user participation is a security threat. On the other hand, the worst possible "de facto" standard of handling users, namely to forget their views and to force security policy/procedures upon the users with punishment, may be a far more serious threat in the long run. It is hoped that user

participation and similar ideas will receive more foothold in future IS security design methods.

The most common *research objective* is means-oriented. All the checklists and management and maturity standards analysed were of this kind, but the formal method paradigms was also influenced by critical research objectives. Of all conventional methods, risk management was the only paradigm, which had one interpretive-oriented approach. An interesting finding with respect to research objectives was that two authors with different security techniques in mind suggested a somewhat similar idea, that security techniques (risk management and checklists) could function as tools for communication, to convince management of the relevance of security. Baskerville (1991) suggested this with respect to risk management, and Kraus (1972) saw that his checklist could function in this role, as well. There are no empirical studies explaining this question further, however, thus that this remains a task for future research.

With respect to recent, contemporary approaches the means-oriented research objective is favoured by logical modeling, responsibility modeling by Thomas and Sandhu (1994), security-modified IS modeling approach by Booysen and Eloff (1995), viable IS (Karyda *et al.* 2001), and information modeling approaches. The interpretive objective can be found in work on responsibility modeling, security modified IS development approaches by Hitchings (1995, 1996) and James (1996), and viable IS by Hutchinson and Warren (2000). Straub and Welke (1998) and the business process community encompassed both mean-end oriented and interpretive views. It is noteworthy that the interpretive approaches (*e.g.*, Hitchings) may include certain open questions, such as how the different models of IS security, or users' views about IS security should be brought into agreement? What are the criteria in this respect? Currently, these interpretive approaches do not offer any criteria hereof, and the worst possible situation is drifting to relativism (all views are equally correct).

Of all SIS design approaches, only a few approaches have a critical research objective. First, it has been widely suggested that, alternative approaches, particularly the interpretive ones, are needed due to the social dimensions of IS (Klein & Lyytinen 1985, Hirschheim 1985, Walsham 1996, Galliers & Swan 1997, Klein & Myers 1999), and it has also been postulated that critical approaches are needed as well. In the first place, critical studies help us to recognize possible weaknesses in the existing, perhaps dominant, approaches and also ensure that nothing can taken for granted or adopted dogmatically. Criticism therefore plays an essential role by keeping us on our toes and forcing us to prove our ideas. Second, critical approaches, when successful, tend to be the ones that are able to make the most contributions to science (Popper 1985). To put this in terms of Kuhn's notions of scientific revolution/paradigms (Kuhn 1962) and the Lakatosian concept of research programs (Lakatos 1970), the critical approaches are the best candidates for raising scientific revolutions, paradigms and research programme shifts. Third, one of the key issues in education is the process of reform, meaning that educational activities should improve the current situation through changes in education. Critical approaches are good candidates for accomplishing such reforms.

Conceptual analysis was the most widely used *research approach* when empirical studies were largely lacking. Additional empirical studies are needed to test ease of use, usability, acceptance and empirical validity of the methods pursuing IS security. However, the use of conceptual analysis by many of these approaches, particularly by

normative standards and common sense principles, nevertheless, represents an inadequate level of rigour. Although the authors of these approaches had not provided any information on the exact sources from which they were derived, there are reasons to believe that the normative standards and common sense principles analysed here had all ignored the results of important research accomplished by IS security investigators (perhaps due to lack of awareness of these works). At least, they did not regard it as relevant to refer to such research, which is unfortunate. Furthermore, to our knowledge there are no studies exploring the implications of the adoption of normative standards and common sense principles in various organizations. In order to try to address these weaknesses, we suggested that any forthcoming normative standards and common sense principles should satisfy two things. First, any such approach should contain a theoretical base that includes the exact sources and rationale for every suggestion. This would give the necessary grounds for serious practitioners and researchers to evaluate the real merits of the normative standards and common sense principles and provide a vital basis for their improvement. No human construction is perfect; thus, unveiling the very foundations of the normative standards and common sense principles is an excellent way to guarantee ongoing, yet progressive development of these approaches. Second, we would particularly welcome empirical investigations – both qualitative and quantitative - into how the different approaches affect organizations in different countries, of different size and in different lines of business. Additionally, such studies should address questions such as whether the IS security approach adopted was worth all the investments and what complications the use of a standard may have raised in organizations?

With respect to *applicability to the IS/software development process*, the conventional approaches analysed here succumb to the problem of developmental duality (*cf*., Baskerville 1993). In other words, none of these conventional SIS approaches could be easily integrated into IS development. The contemporary SIS approaches do not fare much better, as only two contemporary SIS approaches strongly address this issue. Nevertheless, these approaches restrict the autonomy of developers, as developers are not able to use the IS/SW development approaches they prefer. The existing and forthcoming SIS design approaches should take the thesis of developmental duality more seriously, and give more guidance on the integration of different IS security approaches into IS development. Furthermore, the SIS design approaches should pay due respect to the autonomy of developers over the choosing of method applied.

It is concluded from the viewpoint of the meta-model for IS that the different IS security approaches cover the different levels of IS, but lack the comprehensiveness needed. This may be a problem given that all levels of IS are indeed relevant and should be covered in respective IS security approaches. Recently, methods and requirements for developing web IS have been presented (Isakowitz *et al*. 1998, Schwabe & Rossi 1998, Oinas-Kukkonen *et al*. 2001). However, these approaches do not pay attention to Web security issues with the result that additional security methods capable of addressing the requirements posed by the Web environment are needed for designing secure Web IS.

The information security management oriented maturity criteria were analysed from additional six lenses. Pfleeger and coauthors reported with respect to software engineering standards that their "effectiveness has not been rigorously and scientifically demonstrated. Rather, we have too often relied on anecdote, 'gut feeling', the opinions of expert or even flawed research, rather than careful, rigorous software engineering

experimentation" (Pfleeger *et al*. 1994 p. 71). Furthermore, they continue that "even when scientific analysis and evaluation exist, our standards rarely reference them." (Pfleeger *et al*. 1994 p. 72). The results of the analysis of information security management-oriented maturity criteria suggest that this is also the reality in the realm of information security management maturity standards. At any rate, the findings of this study suggest that the information security management maturity standards have not learned from their cognate software engineering maturity standards. The main suggestion is that information security management-oriented maturity standards should be revised to address the issues considered here. In addition, numerous empirical studies are needed to study the relevance and validity in reality of the individual prescriptions for alternative maturity standards. At present such studies are few and far between. Moreover, we would like to see the inclusion in any information security maturity criterion of a complete reference list of related work, with respect to each of the processes areas, milestones, from where the prescriptions originate. As with other information security management standards, practitioners have no evidence on which to judge whether the prescriptions suggested by the information security management-oriented maturity criteria really make sense. With respect to the innovation vs. operational focus, it is suggested that future information security maturity standards should consent to looking for innovative and novel ways of securing IS/software. Future standards should avoid the naturalistic-mechanistic and the spot focus fallacies and include means for tackling the problem of double standard.

RQ3: How can security issues be tackled by IS/SW development methods? Of the weaknesses found in the analysis, four shortcomings were tackled. First, the existing SIS design approaches lack a comprehensive modeling support. The different IS security approaches cover the different levels of IS, but no single approach provides a comprehensive modeling support. Second, many of the existing approaches cannot be integrated into ISSD methods. This complication is termed the problem of developmental duality (*cf*., Baskerville 1992). Third, the existing security approaches restrict the autonomy of developers, as developers are not able to use the ISSD approaches they prefer. Fourth, IS development methods are known to be emergent and evolving (Truex *et al*. 1999): novel methods arise every now and then, and are modified by practitioners to fit different situations. However, it is difficult to put forth one predefined universal security method that will match every existing, forthcoming and unpredictable ISSD method and their permutations. It is argued that a meta-level viewpoint is one avenue to address the aforementioned concerns.

Consequently, a meta-notation consisting of six dimensions was proposed. It should be noted that developers can select from these six elements those elements they need. With respect to the problem concerning a lack of comprehensive modeling support by existing single methods, this thesis proposes a meta-notation which provides modeling support for different levels of IS. The same goes for the lack of methodological support for security aspects of web-IS.

The solution avoids the problem of developmental duality. It is believed that this meta-notation can be added to the existing notation for modeling IS or software. Given that one wants to avoid the problem of developmental duality, it is impossible to provide security specific notation (excluding the meta-notation that can be applied to different, if not all, existing modeling notations). Security specific notation would inevitably lead to the

problem of developmental duality. Such security specific notation cannot be used to model normal ISSD, as security development and normal ISSD would be carried out using different methods. However, any introduction of a new method, which includes both normal and security development, would restrict the autonomy of developers to use the approaches they prefer (they would have to use this particular approach and in all likelihood abandon the methods/practices they are currently using). This proposed solution facilitates the developers' autonomy: developers can use the methods they prefer as a basis of ISSD. An action research intervention was utilized to test the relevance, feasibility applicability of the meta-notation in practice. Action research was perceived to be the most suitable research methodology for testing and possibly adjusting the approach. To summarize, the action research experience suggests that the meta-notation was relevant in use, feasible, and easily applied for extending normal ISSD security, *i.e.*, valid in terms of the accepted action research criteria. The action research intervention was generally successful.

5.2 Limitations

This thesis has some limitations. With respect to the analytical parts (the first and second research questions) of this thesis scrutinizing the existing studies, the limitations are research methodological: one is to do with the reliability of the results of the analysis and another concerns the conceptual-analytical research strategy generally. As to the former issue, a limitation stems from the interpretive research strategy utilized, namely that the results are founded on our interpretation; they are not objective in the natural science sense (*cf*., Gadamer 1989). The latter concern may arise as this study analyses the different SIS approaches conceptual-analytically without offering any empirical evidence on their usefulness and effectiveness in real-world practice (*cf*., Iivari *et al*. 1998, Wynekoop & Russo 1997). However, although it is relevant to scrutinize the success of IS security methods in the light of real life settings (*cf*., Wynekoop & Russo 1997, Björck 2001, Dhillon & Backhouse 2001), it is also relevant to scrutinize the theoretical assumptions as well as the strengths and weaknesses of the different IS security approaches. We do not, however, argue that the review of existing IS security approaches offers an exhaustive account of their underlying assumptions, strengths and weaknesses. Rather the analysis is aimed at increasing our understanding of some of the underlying key assumptions, weaknesses and strengths of these approaches.

Also doubts can be cast upon the applicability of the idea of the meta-notation in the different IS/SW development methods. It is postulated, albeit we do not have wide empirical evidence for this claim, that the proposed idea seems to fit well at least in structural or object-oriented ISSD methods. It might also be objected that the meta-notation, as currently concentrating solely on modeling, resembles some features of functionalism because is it focused more on technical design rather than socio-political aspects (*cf*., Dhillon 1997, Dhillon & Backhouse 2001). While it is true that this approach does not primarily contribute to social issues surrounding security, the meta-notation

entails an interpretive dimension, however, as modeling notation, being a language, is indeed aimed at being used as a means of communications (as an ordinary language).

Nonetheless, it must be stated that, at present, the meta-notation is not comprehensive design method, one which includes, for example, a process and risk analysis.

Moreover, the lack of wide empirical evaluation can be regarded as a limitation of the meta-notation part of this thesis. The proposed meta-notation was only tested in one case, according to action research principles. One may claim that action research, being based on one case, provides only a very limited support for the meta-methodology. For example, the meta-notation method was accepted and applied as such. One interpretation is that this was the case because of the goodness of the meta-notation. An alternative explanation is that the research setting was not challenging enough.

Also, theory-evolution with several cycles (*i.e.*, where a scholar refines his/her theory based on feedback from application of the theory in practice) is little used in this thesis. Thus, given that theory-evolution is often seen as a hallmark of action research (*e.g.*, Lewin 1949, Baskerville & Pries-Heje 1999, Tillotson 2000), it may be criticized that this thesis did not utilize orthodox action research. As mentioned earlier, there was a lack of theory-refinement since the meta-notation method was perceived to be good as such in this setting. Nevertheless, this is not a requirement of all action research criteria or methods (*cf.*, Susman & Evered 1978, McCutcheon & Jung 1990, Baskerville & Wood-Harper, 1998).

Moreover, it is generally seen that in ideal action research, the "theory" stems from the practice rather than originate outside of the problem setting (Oberg 1990). The meta-notation was primarily created beforehand; most of it did not stem from praxis. However, it has also been reported that in action research projects the theory can be known before it is tested in practice (McCutcheon & Jung 1990, McKay & Marshall 2001 p. 51, Mumford 2001b p. 15).

5.3 Main implications and future research

The results are useful for both practitioners and researchers. For practitioners this study shows what kind of contributions there are on offer when securing the different aspects of IS. Researchers and students also benefit through a knowledge of what methods of scientific inquiry are preferred, and what reference sciences are most relevant.

The contributions of the analysis of existing methods for designing secure IS/SW are of relevance to practitioners and academicians alike. First, it is crucial to recognize the underpinning assumptions of our favoured approaches and to compare these with the fundamental assumptions of alternative approaches. It is imperative that university students are gripped with knowledge of alternative SIS methods and that people are able to choose SIS methods autonomously. Otherwise an educator would violate students' autonomy by instilling in them a few paradigms only and neglecting certain alternatives (*cf.*, Hare 1964b, 1975, 1976, Smart 1973). Second, a classification of the myriad of alternative SIS methods in terms of paradigms functions as a clarifying tool: it allows one to get a grasp of the core elements and assumptions of alternative paradigms and

respective methods (*cf*., Iivari *et al*. 2001). Third, recognition of alternative paradigms and their theoretical underpinnings equip future SIS methods developers with the conceptual basis necessary to introduce fundamental paradigm changes (*cf*., Kuhn 1962, Lakatos 1970) in SIS methods thinking. Otherwise, future developers of SIS methods run the risk of duplicating the same fundamental assumptions since they would be concentrating on small-scale and piecemeal modifications (*e.g.*, consider myriad of risk management methods). As a result of this analysis, a list of problems of the existing shortcomings and several research avenues to address these problems were laid down.

This thesis has also suggested a new paradigm for addressing security aspects in ISSD. This new paradigm proposed that, in order to integrate security smoothly into ISSD processes, we should move a level away from methodology - into the domain of meta-methodology. Yet, by adapting such a meta-view, the proposed approach has shown a new direction to pay attention to developers' autonomy. The possibility to maximize the use of the developer's preferred ISSD methods may avoid such problems as the ever increasing cost of system development (*e.g.*, Necco *et al.* 1987) and lack of developer's satisfaction with respect to the methods used (Mahmood 1987). The result of the action research intervention in a practical setting suggests that the proposed meta-notation was a useful and applicable way of embedding security aspects in ISSD methods.

As for practitioners, the proposed meta-notation (six dimensions) ensures that security issues are addressed properly and easily in ISSD. Yet, this proposal satisfies the requirements of autonomy better than any existing approach for designing secure IS/software. Practitioners can continue to use their favoured ISSD methods as a basis for the development and management of secure IS. The action research intervention shows that that the meta-notation was founded very useful and easy to use. To test the feasibility and relevance of this solution at large empirical theory testing research is included in the list of future research questions. Future research should also study can this kind of meta-approach, by facilitating developers' autonomy, improve the developers' motivation with respect to methods.

6 Conclusions

This dissertation consisted of three research steps. Since there are no broad and systematic studies on IS security contributions, it identified key IS security issues and examined the extent to which these issues have been examined and resolved by existing information security research. The results of this survey suggest that information security research has focused mainly on technical issues, while the main reference disciplines have been mathematics and philosophical or mathematical logic, and the dominant research approach has been mathematical modeling. The need for empirical research, particularly on the organizational level, was stated.

This review also revealed that several SIS design and management approaches, from checklists to more advanced endeavours reflecting IS development, have been put forward. In order to increase understanding of the underlying assumptions of these approaches as well as their strengths and weaknesses for the development of secure IS, these approaches were scrutinized within an analytical framework. As the results of this study several shortcomings were recognized, including: The different SIS design approaches cover the different levels of IS, but lack the comprehensiveness needed; most of the approaches for designing SIS are difficult to integrate in ISSD methods; existing SIS design approaches do not assist the autonomy of developers; new ISSD methods spring up occasionally, however, considering the trend of current SIS design approaches, security approaches always come a few steps behind ISSD methods.

The shortcomings detected were addressed by putting forth a framework describing barriers preventing alternative SIS design approaches from more effectively addressing these lapses, and a meta-notation, for adding security into ISSD methods, was presented. Then the solution presented was tested in a practical setting using action research. While further research and practical experience are needed, the experience gained from the action research intervention demonstrates that the proposed meta-notation was relevant, feasible and easy to embed in normal ISSD in a real life setting.

References

Abrahamsson P (2002) The role of commitment in software process improvement. Acta Universitatis Ouluensis A 386, Oulu University Press.

Abrams MD & Podell HJ (1995) Local area networks. In: Abrams MD, Jajodia S & Podell HJ (eds) information security: an integrated collection of essays. IEEE Computer Society Press, Los Alamitos, CA.

AFIPS (1979) Security: checklist for computer center self-audits. AFIPS, USA.

Anderson R (1993) why cryptosystems fail. Communication of the ACM 37: 32-44.

Anderson R (1999) How to cheat at the lottery (or, massively parallel requirements engineering). Procedings of the Annual Computer Security Applications Conference (ACSAC99), Phoenix, AZ, p XIX–XXVII.

Armstrong H (2000) Managing information security in healthcare – an action research experience. Proceedings of the Sixteenth Annual Working Conference on Information Security, Beijing, China, p 19-28.

Avison D, Baskerville R & Myers M (2001) Controlling action research projects. Information Technology and People 14: 28-45.

Avison D & Fitzgerald G (1991) Information systems practice, education and research. Information Systems Journal 1: 5-17.

Backhouse J & Dhillon G (1996) Structures of responsibilities and security of information systems. European Journal of Information Systems 5: 2-10.

Badger TG (2000) Action research, change and methodological rigour. Journal of Nursing Management 8:201-207.

Barnes BH (1998) Computer security research: a British perspective. IEEE Software 15: 30-33.

Basili VR. (1996) The role of experimentation in software engineering: past, present and future. In the Proceedings of 18th International Conference on Software Engineering (ICSE18), Berlin, Germany, p 442-449.

Basili VR & Lanubile F (1999) Building knowledge through families of experiments. IEEE Transactions on Software Engineering 25: 456-473.

Baskerville R. (1988) Designing information systems security. John Wiley Information Systems Series, Chichester, UK.

Baskerville R (1989) Logical controls specification: an approach to information system security. In: Klein H & Kumar K (eds) systems development for human progress. North-Holland, Amsterdam, p 241-255.

Baskerville R (1991) Risk analysis: an interpretative feasibility tool in justifying information systems security. European Journal of Information Systems 1: 121-130.

Baskerville R. (1992) The developmental duality of information Systems security. Journal of Management Systems 4: 1-12.

Baskerville R (1993) Information systems security design methods: implications for information systems development. ACM Computing Surveys 25: 375-414.

Baskerville R (1994) Research directions in information systems security. International Journal of Information Management 14: 85-387.

Baskerville R, Levine L, Pries-Heje J, Ramesh B & Slaughter S (2001) How Internet software companies negotiate quality. IEEE Computer 34: 51-57.

Baskerville R & Pries-Heje J (1999) Grounded action research: a method for understanding IT in practice. Accounting, Management and Information Technologies 9: 1-23.

Baskerville R & Pries-Heje J (2001) Racing the E-bomb: how the Internet is redefining information systems development methodology. In: Fitzgerald B, Russo N & DeGross J (eds) Realigning Research and Practice in IS development: the social and organizational perspective. Kluwer, New York, p 49-68.

Baskerville R & Wood-Harper AT (1996) A critical perspective on action research as a method for information systems research. Journal of Information Technology 11: 235-246.

Baskerville R & Wood-Harper AT (1998), Diversity in information systems action research methods. European Journal of Information Systems 7: 90-107.

Bishop M, Cheung S & Wee C (1997) The threat from the net [Internet security]. IEEE Spectrum 34: 56-63.

Björck F (2001) Implementing information security management systems. In: Eloff J, Labuschagne L, Solms R & Dhillon G (eds) Advances in information security management and small systems security. Kluwer Academic Publisher, Norwell, MA, p 197-211.

Blum FH (1955) Action research- a scientific approach? Philosophy of Science 22: 1-7.

Boehm BW (1976) Software engineering. IEEE Transactions on Computers 25: 1226-1241.

Bollinger TB & McGowan C (1991) A critical look at software capability evaluations. IEEE Software 8: 25-41.

Booysen HAS & Eloff JHP (1995) A Methodology for the development of secure Application Systems. Proceeding of the 11th IFIP TC11 international conference on information security, South Africa, p 255-269.

Boudreau M-C, Gefen D, Straub DW (2001) Validation in information systems research. MIS Quarterly 25:1-24.

Brinkley DL & Schell RR (1995) Concepts and terminology for computer security. In: Abrams MD, Jajodia S & Podell HJ (eds) information security: an integrated collection of essays. IEEE Computer Society Press, Los Alamitos, CA, p 40-97.

BS7799 (code of practice for information security management) (1993) British Standard Institution. London, UK.

Burrell G & Morgan G (1979) Sociological paradigms and organizational analysis. Heinemann, London.

Calas MB & Smircich L (1999) Past postmodernism? Reflections and tentative directions. Academy of Management Review 24: 649-671.

Castano S, Fugini M, Martell G & Samarati P (1995) Database Security. ACM press, New York.

Chalmers AF (1999) What is this thing called science? Third edition, Open University Press, Buckingham, UK.

Chan MT & Kwok LF (2001) Integrating security design into the software development process for e-commerce systems. Information Management and Computer Security 9: 112-122.

Chokhani S (1992) Trusted products evaluation. Communications of the ACM 35: 64-76.

Chua WF (1986) Radical developments in accounting thought. Accounting Review 61: 583-598.

Cullinane D (1999) Electronic commerce security. In: Krause M & Tipton HF (eds) Handbook of information security management. Auerbach, Boca Raton, FL, p 219-236.

Datapro (1992) datapro reports on information security international. Datapro Information Services Group. Delran, NJ.

Davis GB (1999) A research perspective for information systems and example of emerging area of research. Information Systems Frontiers 1: 195-203.

Davis GB (2000) Information systems conceptual foundations: looking backward and forward. Proceedings of the IFIP WG 8.2.Working Conference, Aalborg, Denmark.

Davis BC & Ylönen T (1997) Working group report on Internet/Intranet security. Proceedings of the Sixth IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. IEEE Computer Society Press, Los Alamitos, CA, p 305-308.

Dean D, Felten EW & Wallach DS (1996) Java security: from HotJava to Netscape and beyond. Proceedings of the 1996 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, Los Alamitos, CA, p 190-200.

Denning P, Comer D, Gries D, Mulder M, Tucker A, Turner AJ & Young P (1989) Computing as a discipline: final report of the task force on the core of computer science. Communications of the ACM 32: 9-23.

Dhillon G (1997) Managing information systems security. MacMillan Press LTD, London, UK.

Dhillon G & Backhouse J (2000) Information system security management in the new millennium. Communications of the ACM 43: 125-128.

Dhillon G & Hosein I (2001) Formal methods and secure systems development. Proceedimgs of the Information Resources Management Association conference, Toronto, Canada.

Dhillon G & Backhouse J (2001) Current directions in IS security research: toward socio-organizational perspectives. Information Systems Journal 11: 129-156.

Diffie W (1988) The first ten years of public-key cryptography. Proceedings of the IEEE 76: 560-577.

Dobson J (1990) A Methodology for analysing human and computer related issues in secure systems. Proceedings of the Sixth IFIP International Conference on Computer Security and Information Integrity, Espoo, Finland.

Ellmer E, Pernul G & Kappel G (1995) Object-oriented modeling of security semantics. Proceedings of the 11th Annual Computer Society Applications Conference (ACSAC'95).

Eloff MM & Solms SH (2000a) Information security management: a hierarchical framework for various approaches. Computers and Security 19: 243-256.

Eloff MM & Solms SH (2000b) Information security: process evaluation and product evaluation. Sixteenth Annual Working Conference on Information Security, Beijing, China, p 11-18.

Ferraiolo K & Sachs JE (1996) Distinguishing security engineering process areas by maturity levels. Proceedings of the 9th Annual Canadian Information Technology Security Symposium, Ottawa, Canada.

Finne T (1995) The Information security chain in a company. Computers and Security 15: 297-316.

Fitzgerald KJ (1995) Information security baselines. Information Management and Computer Security 3: 8-12.

Fitzgerald KJ (1993) Risk analysis: ten years on. Information Management and Computer Security 1 5.

Foley SN (1991) A Taxonomy for information flow policies and models. Proceedings of the 1991 IEEE Computer Security Symposium on Research in Security and Privacy, IEEE press, Los Alamitos, CA, p 98-108.

Frisinger A (2001) Improving the protection of assets in open distributed systems by use of X-ifying risk analysis. Proceedings of the IFIP TC11 16th International Conference on Information Security, Paris, France, p 293-304.

Gadamer H-G (1989) Truth and method. 2nd rev. ed., Sheed and Ward, London, UK.

Galliers RD & Land FF (1987) Choosing appropriate information systems research methodologies. Communication of the ACM 30: 900-902.

Galliers RD & Swan J (1997) Against structured approaches: information requirements analysis as a socially mediated process. Proceedings of the Thirtieth Hawaii International Conference on System Sciences, IEEE Computer Society Press, Los Alamitos, CA 3: 179-187.

GASSP (1999) Generally accepted system security principles (GASSP). IS Security 8: 27-77.

Guarro SB (1987) Principles and procedures of the LRAM approach to information systems risk analysis and management. Computer and Security 6: 493-504.

Habermas J (1984) The theory of communicative action – reason and the rationalisation of society (Vol I), Beacon Press, Boston, MA.

Habermas J (1987) The theory of communicative action – the critique of functionalist reason (Vol II), Beacon Press, Boston, MA, USA.

Halliday S & Badenhorst K & von Solms R (1996) A business approach to effective information technology risk analysis and management. Information Management and Computer Security 4: 19-31.

Hare RM (1963) Freedom and reason. Oxford University Press, Oxford, UK.

Hare RM (1964a) The Promising game. Revue Internationale de philosophie 70: 398-412.

Hare RM (1964b) Adolescents into adults. In: Hollins TCB (Ed) Aims in Education. Manchester University Press, UK. Reprinted in: Hare RM (eds) Essays on Religion and Education, Oxford University Press, UK, 1998.

Hare RM (1975) Autonomy as an educational Idea. In: Brown SC (ed) Philosophers Discuss Education. Macmillan, London, UK. Reprinted in: Hare RM (eds) Essays on Religion and Education, Oxford University Press, UK, 1998.

Hare RM (1976) Value education in a pluralist society: a philosophical glance at the humanities curriculum project. Proceedings of the Education Society of Great Britain. Reprinted in: Hare RM (ed) Essays on Religion and Education, Oxford University Press, UK, 1998.

Hare RM (1986) A reductio ad absurdum of descriptivism. In: Shanker S (ed) Philosophy in Britain Today, Croom Helm, London, UK, p. 118-136. Reprinted in: Hare RM (eds) Essays in Ethical Theory. Oxford University Press, Oxford, UK, p 113-130.

Hare RM (1999) Foundationalism and coherentism. In: Hare RM (ed) Objective Prescriptions and other Essays. Oxford University Press, Oxford, UK, p 115-125.

Hefner R (1997) A process standard for systems security engineering: development experiences and pilot results. Third IEEE International 1997 Software Engineering Standards Symposium and Forum, Emerging International Standards (ISESS 97), IEEE Computer Society Press, Los Alamitos, CA, p 217-221

Herrmann G & Pernul G (1998) Viewing business-process security from different perspectives. In the proceedings of the Eleventh International Bled Conference on Electronic Commerce. Bled, Slovakia.

Herrmann G & Pernul G (1999) Viewing business-process security from different perspectives. International Journal of electronic Commerce 3: 89-103.

Hirschheim R (1985) Information systems epistemology: an historical perspective. Proceedings of the IFIP WG 8.2. Working Conference on Research methods in information systems. Elsevier Science Publisher, Amsterdam.

Hirschheim R & Klein HK (1989) Four paradigms of information systems development. Communications of the ACM 32: 1199-1216.

Hirschheim R, Klein HK & Lyytinen K (1995) Information systems development and data modelling: conceptual and philosophical foundations. Cambridge University Press, UK.

Hirschheim R, Klein HK & Lyytinen K (1996) Exploring the intellectual structures of information systems development: a social action theoretic analysis. Accounting, Management and Information Technologies 6: 1-64.

Hirschheim R, Iivari J & Klein HK (1997) A comparison of five alternative approaches to information systems development. Australian Journal of Information Systems 5: 3-29.

Hitchings J (1995) Achieving an integrated design: the way forward for information security. Proceedings of the IFIP TC11 11th international conference on information security, South Africa, p.269-383.

Hitchings J (1996) A Practical solution to the complex human issues of information security design. Proceedings of the 12th IFIP TC11 international conference on information security.

Hopkinson JP (2001) Security standards overview. Proceedings of the Second Annual International Systems Security Engineering Conference, Orlando, FL.

Humphrey WS (1988) Characterizing the software process: a maturity framework. IEEE Software 5: 73-79.

Hutchinson W & Warren M (2000) Using the viable systems model to develop an understanding information system security threats to an organisation. Proceedings of the 1st Australian Information Security Management Workshop, Deakin University, Geelong, Australia.

Iivari J & Kerola P (1983) A Sociocybernetic framework for the feature analysis of information systems design methodologies. In: Olle TW, Sol HG & Tully CJ (eds) Information Systems Design Methodologies: A Feature Analysis, North-Holland, Amsterdam, p 87-139.

Iivari J & Koskela E (1987) The PIOCO model for IS design. MIS Quarterly 11: 401-419.

Iivari J (1989) Levels of abstraction as a conceptual framework for an information system. In: Falkenberg ED & Lindgreen P (eds) Information System Concepts: An In-depth Analysis. North-Holland, Amsterdam, p. 323-351.

Iivari J (1991a) Object-oriented information systems analysis: a framework for object identification. Proceedings of the Twenty-Fourth Annual Hawaii International Conference on System Sciences. IEEE Computer Society Press, Los Alamitos, CA II: 205-218.

Iivari J (1991b) A paradigmatic analysis of contemporary schools of IS development, European Journal of Information Systems 1: 249-272.

Iivari J & Hirschheim R (1996) Analyzing information systems development: a comparison and analysis of eight IS development approaches. Information Systems 21: 551-575.

Iivari J, Hirschheim R & Klein HK (1998) A paradigmatic analysis contrasting information systems development approaches and methodologies. Information Systems Research 9: 164-193.

Iivari J, Hirschheim R & Klein HK (2001) A dynamic framework for classifying information systems development methodologies and approaches. Journal of Management Information Systems 17: 179 – 218.

Isakowitz I, Bieber M & Vitali F (1998) Web information systems. Communication of the ACM 41: 78–80.

IT baseline protection manual (1996) BSI, Germany.

ITSEC (1991) Commission of the European communities, information technology security evaluation criteria, provisional harmonised criteria: version 1.2. Office for Official Publications of the European Communities, Luxembourg, June.

Jaaksi A (1998) Our cases with use cases. Journal of Object-Oriented Programming 10: 58-65.

Jajodia S & Sandhu RS (1995) Towards a multilevel secure relational data model. In: Abrams MD, Jajodia S & Podell HJ (eds) Information security: an integrated collection of essays. IEEE Computer Society Press, Los Alamitos, CA, p 461-492.

James HL (1996) Managing information systems security: a soft approach. Proceedings of the Information Systems Conference of New Zealand. IEEE Society Press, Los Alamitos, CA.

Janczewski L (2000) Managing security functions using security standards. In: Janczewski L (ed) internet and intranet security management: risks and solutions, Idea Group Publishing, USA, p 81-105.

Jenkins MA (1985) Research methodologies and MIS research. Proceedings of the IFIP WG 8.2. Working Conference on Research methods in information systems. Elsevier Science Publisher, Amsterdam, p 103-117.

Johnson BM (1995) Why conduct action research? Teaching and Change 3: 90-115.

Järvinen P (1997) The new classification of research approaches. In: Zemanek H (eds): The IFIP Pink Summary - 36 years of IFIP. IFIP, Laxenburg, Austria, p 124-131.

Järvinen P (2000), Research questions guiding selection of an appropriate research method. Proceedings of the 8th European Conference on Information Systems (ECIS 2000), Vienna, Austria.

Kahn DA (1996) The codebreakers: the story of secret writing. Scribner, New York.

Kaliski B (1993) A survey of encryption standards. IEEE Micro 13: 74-81.

Kant I (1993) The moral law: groundwork of the metaphysic of morals. Routledge, London, UK.

Karyda M, Kokolakis S & Kiountouzis E (2001) Redefining information systems security: viable information systems. Proceedings of the IFIP TC11 16th International Conference on Information Security (IFIP/SEC'01), Paris, France, p 453-468.

Klander L (1997) Hacker proof: the ultimate guide to network security. Jamsa press, Las Vegas, NV.

Klein H & Lyytinen K (1985) The poverty of scientism in information systems. Proceedings of the IFIP WG 8.2. Working Conference on Research methods in information systems. Elsevier Science Publisher, Amsterdam, p 131-161.

Klein HK & Myers MD (1999), A set of principles for conducting and evaluating interpretive Field studies in information systems. MIS Quarterly 23: 67-94.

Klein HK & Myers MD (2001) A classification scheme for interpretive research in information systems. In: Trauth EM (ed) Qualitative Research in IS: Issues and Trends, Idea Group Publishing, Hersney, PA, p 218-239.

Kokol P (1996) Method engineering-a framework for improved computer based medical systems design. Proceedings of the Ninth IEEE Symposium on Computer-Based Medical Systems, IEEE Computer Society Press, p 41-46.

Kraus LI (1972) SAFE: security audit and field evaluation for computer facilities and information systems. AMACOM, NY.

Kumar K & Welke RJ (1992) Methodology engineering: A proposal for situation-specific methodology construction. In: Cotterman WW &. Senn JA (eds) Challenges and Strategies for research in systems development, Wiley, Chichester, UK, p 257-269.

Kuhn TS (1962) The structure of scientific revolutions. University of Chicago Press, USA.

Kuvaja P, Similä J, Krzanik L, Bicego A, Saukkonen S & Koch G (1994) Software process assessment & improvement - the BOOTSTRAP approach. Blackwell Publishers, Oxford, UK.

Kvale S (1983) The qualitative research interview: a phenomenological and a hermeneutical mode of understanding. Journal of Phenomenological Research 14: 171-196.

Lacity MC & Janson MA (1994) Understanding qualitative data: a framework of text analysis methods. Journal of Management Information Systems 11: 137-155.

Lakatos I (1970) Falsification and the methodology of scientific research programmes. In: Lakatos I & Musgrave A (eds) Criticism and the growth of knowledge. Cambridge University Press, UK, p 91-196.

Loose J (2001) A historical introduction to the philosophy of science. Fourth Edition, Oxford University Press, UK.

Lee AS (1989) A scientific methodology for MIS case studies. MIS Quarterly 13: 33-50.

Lee AS (1999) Rigor and relevance in MIS research: beyond the approach of positivism alone. MIS Quarterly 23: 29-33.

Lewin K (1949) Action research and minority problems. Journal of Social Issues: 2: 34-46.

Lyytinen K (1987) Two views on information modeling. Information and Management 12: 9-19.

Lyytinen K (1991) A taxonomic perspective of information systems development: theoretical constructs and recommendations. In: Boland RJ & Hirscheim RA (ed): Critical Issues in Information Systems Research, John Wiley and Sons Ltd, Chichester, UK.

Madabushi SVR, Jones MC & Price RL (1993) Systems analysis and design models revisited: a case study. Information Resources Management Journal 6: 26-39.

Mahmood MA (1987) System development methods - a comparative investigation. MIS Quarterly 11: 293-311.

Malouin JL & Landry M (1983) The miracle of universal methods in systems design. Journal of Applied Systems Analysis 10: 47-62.

March ST & Smith GG (1995) Design and natural science Research on Information Technology. Decision support Systems 15: 251-266.

Massey JL (1988) An introduction to contemporary cryptology. Proceedings of the IEEE 76: 533-549.

Masterman M (1970) The nature of a paradigm. In: Lakatos I & Musgrave A (eds) Criticism and the growth of knowledge. Cambridge University Press, UK, p 59- 89.

Mathieson K (1991) Predicting user intentions: comparing the technology acceptance model with the theory of planned behaviour. Information System Research 3: 173-91.

Mautner T (1996) A dictionary of philosophy. Blackwell Publishers Ltd, Oxford, UK.

McCutcheon G & Jung B (1990) Alternative perspectives on action research. Theory into practice XXIX: 144-151.

McDermid JA & Bennett KH (1999) Software engineering research: a critical appraisal. IEE Proceedings of Software 146: 179-186.

McDermott J & Fox C (1999) Using abuse case models for security requirements. Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC). IEEE Computer Society Press Los Alamitos, CA, USA, p 55-64.

McKay J & Marshall P (2001) The dual imperatives of action research. Information Technology and People 14: 46-59.

McLean J (1990) The specification and modelling of computer security. IEEE Computer. January 23: 9-16.

Menezes AJ, van Oorschot PC & Vanstone SC (1999) Handbook of Applied Cryptography. CRC Press, Boca Raton, FL.

Metaxopoulos E (1989) A critical consideration of the Lakatosian concepts: “mature” and “immature” science. In: Gavroglu K, Goudaroulis Y & Nicolacopoulus P (eds.) Imre Lakatos and theories of scientific change. Kluwer academic publisher, Dosdrecht, the Netherlands, p 203-214.

Mumford E (2001a) Action research: helping organizations to change. In: Trauth EM (ed): Qualitative Research in IS: Issues and Trends, Idea Group Publishing, Hersney, PA, p 46-77.

Mumford E (2001b) An advice for an action researcher. Information Technology and People 14: 12-27.

Murine GE & Carpenter CL (1984) Measuring computer system security using software security metrics. Proceedings of the 2nd IFIP International Conference on Computer Security (IFIP/Sec'84), Toronto, Ontario, Canada.

Necco CR Gordon CL & Tsai NW (1987) System analysis and design: current practices. MIS Quarterly 11: 461-476.

Nickles T (2000) Lakatos. In: Newton-Smith WH (eds) A Companion to the Philosophy of Science. Blackwell Publisher, Oxford, UK, p 207-212.

Niiniluoto I (1990) Science and epistemic values. Science Studies 3:1, p 21-26.

Niiniluoto I (1991) What's wrong with relativism. Science Studies 4: 17-24.

Niiniluoto I (1999) Critical scientific realism. Clarendon Library of Logic and Philosophy, Oxford University Press, Oxford.

Nunamaker JF, Chen M & Purdin TDM (1991) Systems development in information systems research. Journal of Management Information Systems 7: 89-106.

Oberg A (1990) Methods and meanings in action research: the action research journal. Theory into practice XXIX: 214-221.

Oinas-Kukkonen H, Alatalo T, Kaasila J, Kivelä H & Sivunen S (2001) Requirements for web information systems engineering methodologies. In: Rossi M & Siau K (eds) Information Modeling in the New Millennium, Idea Group Publishing, Hershey, PA.

O'Connell E & Saidian H (2000) Can you trust software capability evaluations? IEEE Computer 33: 28-35.

O'Leary DP (1997) Teamwork: computational science and applied mathematics. IEEE Computational Science and Engineering 4: 13-18.

Palmer SW Kliewer S & Sweat M (2000) Security risk assessment and electronic commerce: A cross-industry analysis. In: Janczewski L (ed) Internet and Intranet Security Management: Risks and Solutions, Idea Group Publishing, Hershey, PA p 5-27.

Pap A (1949) Elements of analytic philosophy. Macmillan, New York, USA.

Parker DB (1981) Computer security management, Prentice Hall, Reston, USA.

Parker DB (1998) Fighting computer crime - a new framework for protecting information. Wiley Computer Publishing, New York.

Parnas DL (1999) Software engineering programs are not computer science programs. IEEE Software 16: 19-30.

Paulk MC, Curtis B, Chrissis MB & Weber CV (1993) Capability maturity model. Version 1.1. IEEE Software 10: 18-27.

Perry WE (1985) Management strategies for computer security. Butterworth Publisher, Boston.

Pernul G (1992) Security constraint processing during multilevel secure database design. Proceedings of the 8th Annual Computer Security Applications Conference, San Antonio, TX, p 75-84.

Pernul G & Quirchmayr G (1994) Organizing MLS databases from a data modelling point of view. Proceedings of the 10th Annual computer Security Application Conference, Orlando, FL, p 96-105.

Pernul G, Tjoa AM & Winiwarter W (1998) Modelling data secrecy and integrity. Data and Knowledge Engineering 26: 291-308.

Pfleeger SH, Fenton N & Page S (1994) Evaluating software engineering standards. IEEE Computer 27: 71-79.

Pfleeger SH (1999) Albert Einstein and empirical software engineering. IEEE Computer 32: 32-37.

Plihon V & Rolland C (1997) Genericity in method construction. International Conference on Software Engineering, Hong Kong, p 302-311.

Popper K (1948) What can logic do for philosophy? Aristotelian Society, Supplementary Vol. XXII.

Popper K (1985) Scientific method. In: Miller D (ed) Popper Selections. Princeton University Press, USA, p 133-142.

Ramamoorthy CV (1976) Computer science and engineering education. IEEE Transactions on Computers 25: 1200-1206.

Ray C (2000) Logical positivism. In: Newton-Smith WH (ed) A Companion to the Philosophy of Science, Blackwell Publisher, Oxford, UK, p 243-256.

Rifkin S (2001) What makes measuring software so hard? IEEE Computer 18: 41-45.

Röhm AW, Pernul G & Herrmann G (1998) Modelling secure and fair electronic commerce. Proceedings of the 14th Annual Computer Security Applications Conference, Phoenix, AZ, p 155-164.

Röhm AW & Pernul G (1999) COPS: A model and infrastructure for secure and fair electronic markets. Proceedings of the 32nd annual Hawaii International Conference on Systems Sciences, Hawaii, HI.

Sanders PW, Furrell P & Warren MJ (1996) Baseline security guidelines for health care management. In: the SEISMED Consortium (eds) Data Security for Health Care: Volume 31: Management Guidelines, Baseline Security Guidelines for Health Care Management, p 82 - 107, IOS Press, The Netherlands.

Sandhu RS (1993) Lattice-based access controls. IEEE Computer 26: 9-19.

Sandhu RS & Samarati P (1994) Access control: principle and practice. IEEE Communications 32: 40-48.

Sandhu RS Coyne EJ, Feinstein HL & Youman CE (1996) Role-based access control models. IEEE Computer 29: 38-47.

Schein E (1987) Clinical perspective in fieldwork, Sage, Beverly Hills, CA.

Schwabe D & Rossi G (1998) An object-oriented approach to web-based application design. Theory and Practice of Object Systems 4: 207-225.

Schweitzer JA. (1982) Managing information security: a program for the electronic information Age. Butterworth, Boston, USA.

Scruton R (1995) A short history of modern philosophy. Second Edition, Routlege, London, UK.

Sharp H, Robinson H & Woodman M (2000) Software engineering: community and culture. IEEE Software 17: 40-47.

Sherwood J (1996) SALSA: a method for developing enterprise security architecture and strategy. Computers and Security 15: 501-506.

Siponen MT (2000) A conceptual foundation for organizational information security awareness. Information Management and Computer Security 8: 31-41.

Siponen MT (2002) A Paradigmatic analysis of six conventional approaches for developing and managing secure IS: implications for research and practice. Working Paper Series B 65, University of Oulu, Department of Information Processing Science, Finland.

Slooten van K (1996) Situated method engineering, Information resources management journal 9: 23-31.

Smart P (1973) The concept of indoctrination. In: Langford G & O'Connor DJ (eds) New Essays in the Philosophy of Education. Routledge and Kegan Paul, London, UK, p 33-46.

Smith GW (1989) The semantic data model for security: representing the security semantics of an application. Proceedings of the Sixth International Conference on Data Engineering, Los Angeles, CA, p 322-329.

Solms R (1996) Information security management: the second generation. Computers and Security 15: 281-288.

Solms R (1997) Can security baseline replace risk analysis? Proceedings of the IFIP TC11 13th International Conference on Information Security (SEC'97), Copenhagen, Denmark.

Solms R (1998) Information security management (3): the code of practice for information security management (BS 7799). Information Management and Computer Security 6: 224-225.

Solms R (1999) Information security management: why standards are important. Information Management and Computer Security 7: 50-58.

Sommerville I (1996) Software engineering. Fifth Edition, Addison-Wesley Publishers Ltd, USA.

Spruit M & Samwel PH (1999) Risk analysis on Internet connection. Proceedings of the IFIP TC11 WG11.2/WG11.2 Seventh Annual Working Conference on Information Management and Small Systems Security, Amsterdam, the Netherlands.

Spurling P (1995) Promoting security awareness and commitment. Information Management and Computer Security 3: 20-26.

SSE-CMM (1998a) The model. v2.0. Http://www.sse-cmm.org.

SSE-CMM (1998b) The appraisal method. v2.0. Http://www.sse-cmm.org.

Stacey TR (1996) Information security program maturity grid. Information Systems Security 5: 22-33.

Stohr EA & Konsynski BR (1992) Research approaches in ISDP. In: Stohr EA & Konsynski BR (eds) Information Systems and Decision Processes. IEEE Computer Society Press, Los Alamitos, CA, p 301-320.

Straub DW (1990) Effective IS security: an empirical study. Information Systems Research, 1: 255-276.

Straub DW & Welke RJ (1998) Coping with systems risk: security planning models for management decision making. MIS Quarterly 22: 441-464.

Strens R & Dobson J (1993) How responsibility modelling leads to security requirements, Proceedings of the 1992 and 1993 ACM SIGCAS New Security Paradigm Workshop, New York.

Stroll A & Popkin RH (1979) Introduction to Philosophy. Third edition, Holt, Rinehart and Winston, Inc., USA.

Summers RC (1997) Secure computing: treats and safeguards. McGraw-Hill, New York.

Susman GI & Evered RD (1978) An assessment of the scientific merits of action research. Administrative science quarterly 23: 582-603.

Thomas RK & Sandhu RS (1994) Conceptual foundations for a model of task-based authorizations. Proceedings of the 7th IEEE Computer Security Foundations Workshop, Franconia, NH, p 66-79.

Thomson ME & von Solms R (1997) An effective information security awareness program for industry. Proceedings of the WG 11.2 and WG 11.1 of the TC11 IFIP, Copenhagen, Denmark.

Thomson ME & von Solms R (1998) Information security awareness: educating our users effectively. Information Management and Computer Security 6: 167-173.

Tillotson JW (2000) Studying the game: Action research in science education. The Clearing House 74: 31-34.

Tremblay G (2000) Formal methods: mathematics, computer science or software engineering? IEEE Transactions on Education 43: 377–382.

Truex DP, Baskerville R & Klein HK (1999) Growing systems in an emergent organization. Communications of the ACM 42: 117-123.

Truex DP, Baskerville R & Travis J (2000) Amethodical systems development: the deferred meaning of systems development methods. Accounting, Management and Information Technology 10: 53-79.

Tryfonas T, Kiountouzis E & Poulymenakou A (2001) Embedding security practices in contemporary information systems development approaches. Information Management and Computer Security 9: 183–197.

Voas J (1999) Software quality's eight greatest myths. IEEE Software 16: 118-120.

Walsham G (1993) Interpreting information systems in organizations, Wiley, Chichester, UK.

Walsham G (1996) The emergence of interpretivism in IS research. Information Systems Research 6: 376-394.

Warman AR (1992) Organizational computer security policy: the reality. European journal of Information Systems 1: 305-310.

Weick KL (1999) Theory construction as disciplined reflexivity: tradeoffs in the 90's. The Academy of Management Review 24: 797-806.

Wood CC, Banks WW, Guarro SB, Garcia AA, Hampel VE & Sartorio HP (1987) Computer security: a comprehensive controls checklist. John Wiley and Sons, Chichester, UK.

Wynekoop JL & Russo NL (1997) Studying system development methodologies: an examination of research methods. Information Systems Journal 7:47-65.

Zhou D, Kuo JC, Older S & Chin SK (1999) Formal development of secure email. Proceeding of the 32nd Annual Hawaii International Conference Systems Sciences, Hawaii, HI.