ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/220627549

A Review of Information Security Issues and Respective Research Contributions

Article *in* ACM SIGMIS Database · February 2007

DOI: 10.1145/1216218.1216224 · Source: DBLP

CITATIONS
203

READS
3,100

2 authors:

Mikko Siponen
University of Jyväskylä
155 PUBLICATIONS **7,153** CITATIONS

SEE PROFILE

Harri Oinas-Kukkonen
University of Oulu
230 PUBLICATIONS **4,948** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project

Prevent Metabolic Syndrome View project

Project

Cyber Trust -project View project

All content following this page was uploaded by Harri Oinas-Kukkonen on 06 November 2015.

The user has requested enhancement of the downloaded file.

A Review of Information Security Issues and Respective Research Contributions

Mikko T. Siponen
University of Oulu

Harri Oinas-Kukkonen
University of Oulu

Abstract

This paper identifies four security issues (access to Information Systems, secure communication, security management, development of secure Information Systems), and examines the extent to which these security issues have been addressed by existing research efforts. Research contributions in relation to these four security issues are analyzed from three viewpoints: a meta-model for information systems, the research approaches used, and the reference disciplines used. Our survey reveals that most information security research has focused on the technical context, and on issues of access to IS and secure communication. The corresponding security issues have been resolved by using mathematical approaches as a research approach. The reference disciplines most commonly reflected have been mathematics, including philosophical logic. Based on this analysis, we suggest new directions for studying information security from an information systems viewpoint, with respect to research methodology and research questions. Empirical studies in relation to the issues of security management and the development of secure IS, based on suitable reference theories (e.g., psychology, sociology, semiotics, and philosophy), are particularly necessary.

ACM Categories: K.6.5

Keywords: Computer Science

Introduction

The importance of information security has increased due to the increased utilization of computers and the Internet. Not surprisingly, there are now several journals and a large number of annual conferences and workshops dedicated to the security aspects of information systems (IS) and computing. These include contributions by computer scientists, cryptologists, electrical and computer engineers and IS scholars. However, these contributors often have very different views on the key information security problems and their respective solutions. Furthermore, we see that scholars belonging to a certain discipline, such as computer science, cryptology, computer engineering or IS, often seem to have a poor awareness of the contributions made by researchers in other disciplines. This leads to fragmentation in the field of information security, which has two implications. First, scholars in different disciplines may end up trying to reinvent the wheel. Second, we can see that addressing security problems holistically requires interdisciplinary efforts.

Given such diversity in the information security field, it is surprising to find that few research efforts have been devoted to interdisciplinary research, analyzing contributions to information security without limiting the analysis to a particular discipline (e.g., computer science, IS or cryptology). Such studies are needed in order to see the "big picture", to make sense of the field, to see what previous research work has emphasized and identify those areas where the need for future work is greatest. Previous review articles have focused on specific aspects of information security, such as access control models (e.g., Castano et al., 1995; Sandhu, 1993), cryptographic solutions (e.g., Menezes et al., 1999) and methods for designing secure IS (e.g., Baskerville, 1998; 1993; Backhouse & Dhillon, 2001; Dhillon, 1997). Due to the lack of a wide-ranging review on information security contributions, it is necessary to study *how and to what extent information security issues have been covered by previous research and what research approaches and reference disciplines have been used by prior research*. To do this, we need to select appropriate conceptual tools from the literature that will help us to make sense of and categorize the existing research efforts. These are a *meta-model for IS*, *research approaches* and *reference disciplines*.

We surveyed the information security literature up to early 2000[1]. We did not limit this analysis to specific conferences or journals, in order to get a rich picture of information security research efforts, including the different research approaches taken and reference disciplines employed. However, inevitably some studies lie beyond the scope of this analysis, namely those involving educational questions and ethical analysis. Such studies do not fall into particular security issues (access, secure communication, security management, development of secure IS).

The paper is organized as follows. The second section presents the analytical framework for study of the issues surrounding information security. In section three, information systems security research is analyzed from the selected viewpoints. The fourth section discusses the key findings. Finally, the paper is concluded with a summary of the contributions of this research.

A Framework for the Study and Information Security Issues

Definitions

In seeking an appropriate vehicle for the organization and categorization of the contributions on information security, we found the following set of questions useful for educational purposes and reasons of clarity.

- Access to IS: How can people's access to information be controlled?
- Secure communication: How can secure communication between people be ensured?
- Security management: How should information security be managed?
- Development of secure IS: How should an IS be developed in order to be secure?

Before selecting these four issues, we conceptually tested and tried several other potential issues. For example, we first endeavoured to sketch a detailed list of information security issues. This preliminary list of issues included: how to authenticate the subjects; how to develop and express security policies and security guidelines; how and what to audit; how to organize backup, recovery and contingency management; how to prevent other unwanted flow of information; how to achieve physical and tamper-proof security; how to create secure environments with respect to executable codes; how to create secure programming languages; how to validate and test code; how to organize key management and solve certificate authority questions; how to maximise end-user commitment towards organizations' security objectives and policies.

While testing these issues conceptually, we realized that it was difficult, if not impossible, to craft a detailed list of information security issues that would cover everything. Also, with such a detailed list there would be a risk that the list would be biased towards some sub-area of information security, or towards certain disciplines. To avoid this problem, we decided to increase the level of abstraction and provide only four high-level information security issues: access to IS, secure communication, security management, and development of secure IS. Increasing the level of abstraction helps to make the security issues more inclusive. We find that these issues are appropriate and instrumental for educational purposes and reasons of clarity (cf., Iivari et al., 2001) and for studying the extent of information security research in a variety of areas. We see that these issues represent an abstraction of information security contributions. This means that security contributions can be mapped out according to these four issues, and vice-versa.

[1] Information systems, computer science and management science publications (journals, conferences, books, workshops) were analyzed. The key idea was to cover security topics widely, irrespective of their publication forum. In cases where several papers tackled the same topics similarly, we selected the key papers (based on our subjective judgment) – "criterion 1". In fact, this is the strength of the paper. Often review articles are based on "A" level, or the top 10-20, journals. As a result, such review studies may first lack a representative view of the field and, second, lack potential studies that have not yet matured to the "A" level. Additionally, studies in "A" journals are assumed to be ones that are already most well-known in the field.

"How should an IS be developed and managed?" is a key question in the field of IS (Hirschheim et al., 1996). Hence, from an IS perspective, the respective security aspects ("How should information security be managed?" and "How should an IS be developed in order to be secure?" should be relevant. We see that there are also two issues, access to IS and security of communication, that encompass various solutions by information security researchers[2]. Hence, we see these security issues as relevant for the study.

Different types of information security requirements may be associated with these information security issues. The following three requirements are widely agreed to be important, irrespective of the tradition of information security from which they emanate (e.g., Baskerville, 1988; Parker, 1998): information should not be modified by unauthorized subjects (*integrity*); information should be available to authorized subjects when required (*availability*); improper disclosure of information should be detected and prevented (*confidentiality*). We also note that electronic commerce has increased the need to ensure that in trading or contracts one cannot afterwards deny an action (e.g., signing a contract) that one has carried out (*non-repudiation*).

The association of these four requirements with information security issues is useful for practitioners and scholars to aid examination of how various security solutions address these four security issues, and to perceive the extent to which the existing information security research covers the security issues.

The issue of *access to IS* encompasses the means used to control subjects' access (e.g., read and write access) to objects requiring information security, such as files, directories, tuples or relations (Sandhu, 1993). The goal is to guarantee that the requirements of integrity, availability and confidentiality of security objects are not compromised. "Security subjects" refers to active information entities, e.g., processes and humans. For example, authentication, which refers to a process of ensuring that subjects are really the subjects they claim to be (Needham, 1989), belongs to this issue. The objective of authentication is to ensure that information is not modified by unauthorized subjects (integrity), it is available only to authorized subjects (non-disclosure), and that individuals cannot deny an action that they have carried out (non-repudiation). Authentication ensuring non-repudiation is especially important in enabling electronic business so that people can make valid contracts.

Access to IS also includes the prevention of all unwanted flows of information between objects and subjects, including any flows of information that could be used to attain nformation which needs to be secure. This issue also includes so-called covert channels and the avoidance of the inference problem, irrespective of the source, from deliberate social engineering attacks (where human faults or weaknesses are used to carry out such an attack) to Trojan horses. Denial-of-service is also a part of this. In this case an unwanted, albeit authorized, process of dwindling takes place in the resources of the IS.

Confidentiality, availability, integrity and non-repudiation constitute the main requirements for *secure communication*. In an act of communication, the aim may not be to hide the act itself (this may be impossible); but the context of that act of communication needs to be confidential or untouched (integrity). Data communication channels, e.g., local networks, can also be regarded as security objects and therefore, following our classification, protection against the tapping of a network belongs to the issue of access to IS.

Security management refers to a means of maintaining secure IS in organizations, including IS planning and evaluation. This also includes the questions of key, backup, recovery and contingency management. Confidentiality, availability, integrity and non-repudiation are the requirements for security management.

The issue of *development of secure IS* encompasses questions such as how to collect different security requirements, how to express and model different security requirements, and how to ensure that an IS meets the given requirements. Testing is also part of this issue. Checklists and various studies on security policies are considered under the issue of security management as these do not offer any means of identifying or modelling security requirements, but rather provide predefined security management principles. Confidentiality, availability, integrity and non-repudiation make up the requirements for the issue of development of secure IS.

Analytical Framework

We have found several potential frameworks from the IS literature with which information security issues and their respective research contributions can be

[2] For example, a reviewer suggested that the issue of secure communication ("How can secure communication between people be ensured?") may be seen as a field of communication security, while the issue of access to IS ("How can people's access to information be controlled?") might be seen as the field of computer security. While most of the research contribution in relation to access, for example, is advanced by communication security researchers, this disciplinary classification is not used in this study. However, this reviewer's view demonstrates how relevant and expressive the issues of secure communication and access to IS are.

analyzed. Dhillon (1997), Dhillon and Backhouse (2001) and Hirschheim et al. (1996) have analyzed existing methods in the light of four sociological paradigms, Iivari (1989) has scrutinized IS development methods from the viewpoint of a meta-model for IS, while Iivari (1991), Iivari and Hirschheim (1996), and Iivari et al. (1998) have analyzed IS development methods in the light of research methods, the organizational role of IS and research objectives. Of these, *meta-model for IS*, *research approaches* and *reference disciplines* (Figure 1) were regarded as excellent candidates for excellent candidates for viewpoints from which to carry out the research objectives of this study for the following reasons. These viewpoints have not been used to analyze security contributions in an interdisciplinary manner. For example, Burrell-Morgan sociological paradigms have been used to analyze information security contributions (Dhillon, 1997; Dhillon & Backhouse, 2001). And yet, these viewpoints have the potential to yield valuable information. Reference disciplines (Lyytinen, 1987) and research approaches are seen as useful in interdisciplinary analysis studies in the field of IS (Iivari, 1991; Iivari & Hirschheim, 1996; Lyytinen, 1987). Indeed, one of the key issues of IS research throughout its history has been the selection and use of suitable research methods and reference disciplines (Banville & Laundry, 1989; Iivari, 1991; Lyytinen, 1987). Hence, we assume that pointing out the reference disciplines and research methods used in information security research is of use to future research. Both of these help in perceiving the reference disciplines and research methods which have been used, and in examining which issues merit the application of alternative reference disciplines and research methods. The same goes with the meta-model. According to (Hirschheim et al., 1996; Iivari & Koskela, 1987; Iivari, 1989; Lyytinen, 1987), three domains are fundamental to the field of IS: the organizational, the conceptual and the technical. Accordingly, IS scholars have classified IS research into these domains (Hirschheim et al., 1996; Iivari, 1989; Lyytinen, 1987). Hence, we assume that these three domains, forming the meta-model for IS (Iivari, 1989), are also useful in classifying information security contributions. These three viewpoints presented in Figure 1 are examined next.

The breadth of IS can be understood with the help of *a meta-model for IS* (Iivari, 1989). In this study, a meta-model for IS (Iivari, 1989) is utilized in order to explore the scope of different security solutions. This meta-model is based on a commonly agreed separation between three levels of abstraction or domains for an IS (Hirschheim et al., 1996; Iivari & Koskela, 1987; Iivari, 1989; Lyytinen, 1987):

1. The *organizational* level defines the organizational role and context of the IS (Hirschheim et al., 1996; Iivari, 1989). Since information security, at least from an IS viewpoint, is concerned with protecting information and the system processing it, information security should (in addition to technical issues regarding computer security) be concerned with human processors, including their behavioural aspects (Baskerville, 1989, p. 244). Organizational security policies are examples of organizational-level solutions.

2. The *conceptual or language* level defines an implementation-independent specification for the IS (Hirschheim et al., 1996; Iivari, 1989). Different techniques for modelling security constraints are examples of conceptual-level security solutions.

3. The *technical* level defines the technical implementation for the IS (Hirschheim et al., 1996; Iivari, 1989). For instance, the various encryption algorithms are technical-level solutions.

Since the meta-model for IS is based on commonly agreed levels (Hirschheim et al., 1996; Iivari & Koskela, 1987; Iivari, 1989; Lyytinen, 1987), it shows which aspects of information systems are covered by different security solutions.

The study of *research approaches* aims to reveal which research strategies are used to develop the existing information security solutions (Figure 1). For example, a question such as "Are the methods, techniques and principles validated empirically or conceptually?" can be answered by inference from the research approach used. Several classifications of IS research methods exist, including Galliers and Land (1987), Iivari (1991), Järvinen (2000), Nunamaker et al. (1991) and March and Smith (1995). When selecting an appropriate research method classification, we realized that it was necessary to select a research method classification that classifies research approaches or strategies, as well as research methods. The concept "research approach" operates at a higher level of abstraction than that of "research method", which means that one research approach can be addressed by means of several research methods. In this study, it is useful primarily to analyze research approaches rather than research methods. This is because it is common to information security studies that they do not reveal the exact research methods applied, while we can always interpret the research approach used. We therefore selected Järvinen's classification (2000) because it primarily classifies research approaches (Figure 1).

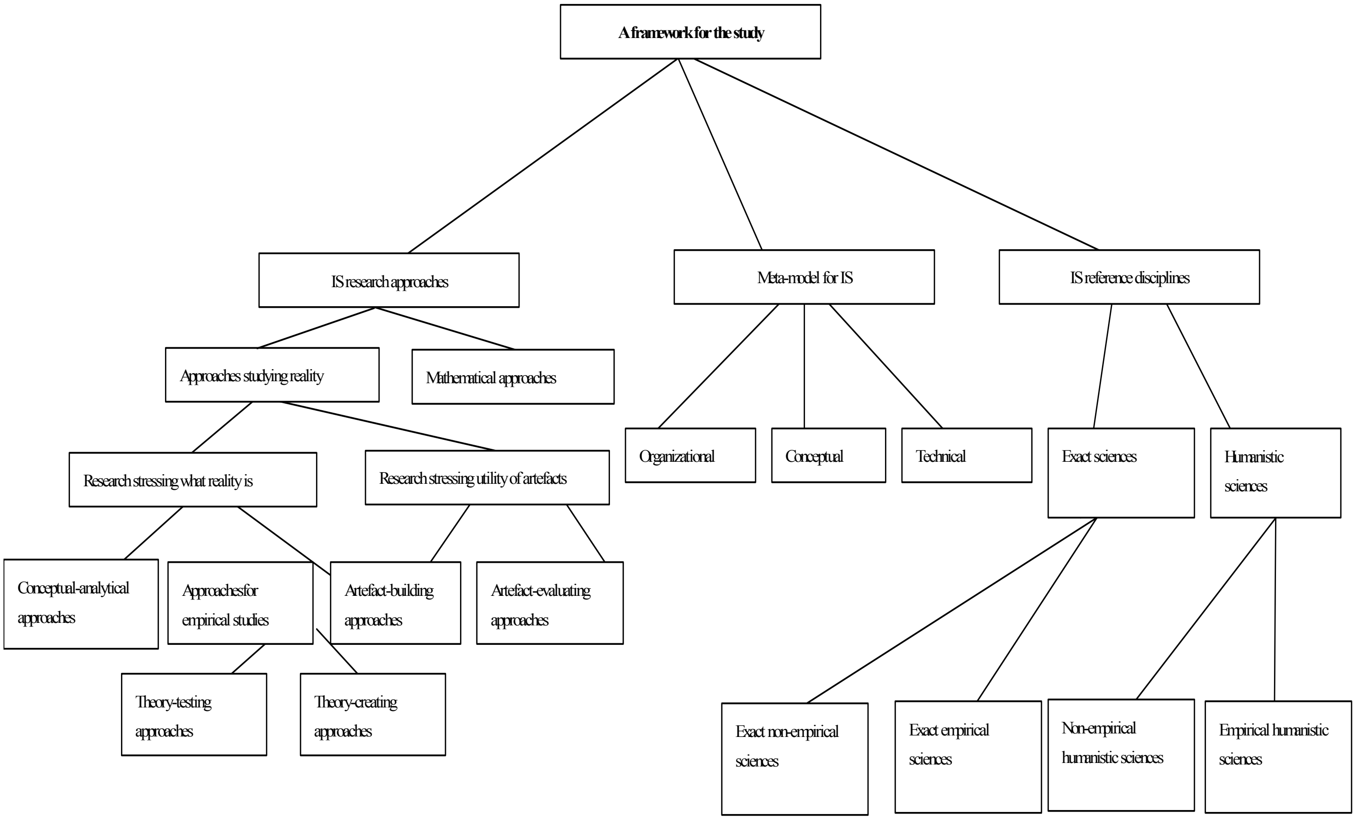
A framework for the study
IS research approaches
Meta-model for IS
IS reference disciplines
Approaches studying reality
Mathematical approaches
Organizational
Conceptual
Technical
Exact sciences
Humanistic sciences
Research stressing what reality is
Research stressing utility of artefacts
Conceptual-analytical approaches
Approaches for empirical studies
Artefact-building approaches
Artefact-evaluating approaches
Theory-testing approaches
Theory-creating approaches
Exact non-empirical sciences
Exact empirical sciences
Non-empirical humanistic sciences
Empirical humanistic sciences

Figure 1. A framework for the study

Following Järvinen (2000), IS research approaches are first divided into "approaches studying reality" and "mathematical approaches". Approaches studying reality are subdivided into "approaches stressing what reality is" and "research stressing utility of artefacts" (Figure 1). 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". In our interpretation, research utilizing philosophical logic (sometimes referred to as logical modelling) is classified under mathematical approaches.

Researchers should be aware of the theoretical underpinnings of IS (e.g., Dhillon & Backhouse, 2001; Hirschheim et al., 1996; Iivari et al., 1998; Lyytinen, 1987). Pointing out the *reference disciplines* reflected is one way to achieve this aim (Lyytinen, 1987). IS researchers have utilized several contributing or reference disciplines, from mathematics to sociology, psychology and philosophy (Lyytinen, 1987). Following Lyytinen (1987), disciplines contributing to IS may first be 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, linguistics, 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.

Information Security Research Contributions

In the following analysis, the research contributions with respect to access to IS, secure communication, security management and development of secure IS are first placed in terms of the levels, and second, classified in terms of security requirements.

The contributions related to access to IS cover technical, conceptual and organizational levels.

The contributions of secure communication to this issue mainly concern the technical context with a few works at the conceptual level. There are also solutions that cover both technical and organizational levels within secure communication.

The contributions related to security management only concern the organizational and technical levels. As well as the solutions dealing with either technical or organizational levels, there are also works in the security management category which cover both organizational and technical levels.

Contributions concerning the development of secure IS cover all three levels: technical, conceptual and organizational.

Access to IS

Technical Level

At the technical level, the most notable contributions to the method of authentication include passwords (Denning, 1992) and token-based authentication, i.e., authentication using special-purpose devices, such as smart-cards (e.g., Chang et al., 1993; Hendry, 1997). In these cases, mathematics is used as the reference discipline, and mathematical approaches are used as the research approach.

Availability issues related to authentication has been recognized (Gong, 1993). The question of how to authenticate subjects has also been studied in distributed systems (Woo & Lam, 1992), in relation to mobility (Molva et al., 1994), and with respect to GSM (Bookson, 1994; Rahnema, 1993). Needham (1989) and Simmons (1988) have also studied authentication in general.

Password mechanisms are a technical-level contribution, and these can be classified as i) traditional passwords (where users are able to choose a password); ii) system-generated passwords, iii) passphrases, iv) cognitive passwords and v) associative passwords (Zviran & Haga, 1993; Jobush & Oldehoeft, 1989). Technical-level contributions include password schemes (e.g., Chang & Hwang, 1991) and password authentication protocols to defend against certain attacks (e.g., Gong, 1995; Kwon & Son, 1998). To control the security of token-based authentication from physical attacks, known as tamper-proofing, a few solutions exist (Anderson & Kuhn, 1996). Authentication protocols, after verification of the identities of participants, may also be used in achieving an agreement upon a session key. In such cases, these are often referred to as key distribution protocols (Gong, 1993). We have found that all these contributions concerning access to IS at a technical level encompass the requirements of confidentiality, availability, integrity and non-repudiation.

Most of the contributions concerned with ensuring that subjects can have access to objects (e.g., files) are at the technical level. Such techniques include Access Matrix, Mandatory Access Control policies, Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) policies. Brief overviews of these techniques are provided by McLean (1990), Sandhu (1993), Sandhu and Samarati (1994), and Boswell (1995). Access Matrix, according to Lampson (1971), differs from DAC and MAC in that the objective of Access Matrix is not to provide any particular access policies, whereas DAC and MAC do provide them. These access control models encompass the requirements of confidentiality and integrity as follows.

MAC is concerned with the integrity (e.g., the Biba model) and/or confidentiality of information (e.g., BLP model, Jajodia and Sandhu model). MAC policies are concerned with the flow of information, while DAC policies are not (and therefore pave the way for a Trojan horse, or similar attacks aimed at leaking information to unauthorized parties, for instance). Also, in the case of MAC, the clearances are set and controlled by security personnel (not users).

With DAC the flow of information is controlled by users: users can grant rights to other users. AM provides an easily understandable manner of representation for many policies, particularly DAC policies. The limitations of AM were recognised by Harrison et al. (1976), and consequently several improved models to overcome such problems have been developed, including Sandhu (1988), Sandhu (1992), Dacier and Deswarte (1994). Role-Based Access Control models also consider groups as a set of subjects (see Sandhu et al., 1996; Sandhu, 1998). Excluding AM, they do not offer any means to model or identify subjects, objects, etc., and therefore they remain at the technical level only. These security models are not at the conceptual level since they are mainly used to technically validate the proposed solutions, and do not provide modelling tools for the modelling of organizational and conceptual level aspects.

Access control lists provide a more efficient implementation of AM. Although they are implementation-independent solutions, they remain at the technical level only. With regard to flows of information from objects, there are several information-flow control models (including non-interference models, e.g., Ryan & Schneider, 1999). These, greatly influenced by information theory, are also at the technical level, using mathematics as a reference discipline and building their research approaches upon mathematical approaches. The so-called lattice models, which are based on the mathematical structure of lattices, are cases in point, although some models referred to as lattice policies do not contain any information-flow models. Information-flow models include Denning (1976), Jacob (1991); see Foley (1991), Sandhu (1993), Castano et al. (1995). The other research contributions at a technical level include memory protection of operating systems (see, e.g., Castano et al., 1995), and database integrity issues (e.g., Castano et al., 1995; Notargiacomo, 1995, Jajodia et al., 1995) covert channel (e.g., Kemmerer, 1983; Kemmerer & Porras, 1991; Moskowitz & Kang, 1994; Millen, 1999).

The issue of how to control subjects' ability to access objects in the area of web information systems has been studied from the point of view of hypermedia and hypertext. This research has concentrated on technical access control and policy models (Diaz et al., 1997; 1998; Fernandez & Nair, 1998). These solutions are aimed at ensuring the requirements of confidentiality, integrity, availability and non-repudiation. The reference discipline used is philosophical logic and the research approach is based on mathematical approaches.

Anti-virus techniques are aimed at guaranteeing the requirements of confidentiality, integrity and availability. They try to ensure that no malicious subjects (processes in this case) can obtain access to objects. Cohen defined a computer virus as a program that can spread itself to other programs and cause harm (Cohen, 1984). Nowadays one may refer broadly to "malware", including viruses, worms, Trojan horses, time bombs, and spy-software. Anti-virus (or anti-malware) techniques operate at the technical level. Such anti-virus techniques can be classified as i) scanners, which can only detect known viruses or their close relatives; ii) checksum-based, e.g., checking integrity checksums, iii) traps, e.g., detecting suspicious activities; iv) built-in self tests; v) program vaccination ; and vi) multiversion programming (Cohen, 1991; Lee et al., 1997). These anti-virus techniques can be divided into two categories with respect to their working environment: scanners operating in gateways, for example scanning attachments from incoming e-mail, and on-access virus scanning, i.e., taking place at the workstation level (Hruska, 1997). Bishop (1991), Cohen (1991) and Spafford (1998) provide overviews of viruses, and Bontchev (1996) discusses macro viruses and their prevention.

In order to control different digital goods, such as pictures and programs, particularly after their distribution, the question of image security has been brought up. Contributions with respect to watermarking are a case in point, ranging from digital images (Voyatzis & Pitas, 1999) and 3D objects (Yeo & Yeung, 1999) to real-time video applications (Busch et al., 1999). A practical overview of watermarking is provided by Craver and Yeo (1998). Steganography, although similar to watermarking (Anderson & Petitcolas, 1998; O'Sullivan et al., 1998), is discussed under communication security. These contributions are aimed at ensuring non-repudiation.

Auditing[3], in the sense of discovering security violations, can be carried out manually or automatically, off-line or on-line. The key problem for an audit is determining what information should be collected to perform the audit, i.e., how and what to audit. Auditing involves the requirements of integrity, availability, confidentiality and non-repudiation. A system that carries out an automated audit is referred to as intrusion detection (Sandhu & Samarati, 1996). The contribution of intrusion detection systems are at the technical level, including Threshold-based, Anomaly-based, Rule-based, State-transition (Ilgun et al. 1995), and Model-based reasoning (Garvey & Lunt, 1991). Such techniques can also be classified as either i) passive, i.e., those which only collect and possibly process the collected data; and ii) active, i.e., they also automatically perform counteractions, such as deleting processes or closing user accounts. The reference discipline reflected is mathematical logic, while the research approach used is based on mathematical approaches. These contributions encompass the requirements of confidentiality, integrity, availability and non-repudiation.

Firewalls (in the simplest sense, filters which filter incoming and/or outgoing traffic on a network operating between an organization and the outside world) are also aimed at preventing unauthorized access or denial-of-service attacks on a network, particularly the Internet. Such solutions are at the technical level. Firewalls are traditionally classified as packet-filtering (packets are dropped or allowed on the basis of their source and/or destination, using IP address, ports, etc.), circuit gateways, and application gateways (filtering on an application-by-application basis); see Bellovin and Cheswick (1994), Wack and Carnahan (1995) and Lodin and Schuba (1998). The research approach used is that of conceptual analysis. These studies try to fulfil the requirements of confidentiality, integrity and non-repudiation.

[3] Auditing is also used as a synonym for testing and validating the security of IS, i.e., to see whether the security mechanisms are working as required.

Conceptual Level

Access Matrix (Lampson, 1971) offers a manner in which to present subjects and objects at the conceptual level. Access Matrix is aimed at ensuring the requirement of confidentiality and integrity of computer systems. It is utilized to illustrate which users/processes (security subjects) have access to which security objects. There are a few conceptual-level contributions providing conceptual tools with respect to the modelling of access control policies, including Wood et al. (1979) and Baldwin (1990).

Organizational Level

Biometrical authentication has been studied at an organizational level (e.g., Miller, 1994; Lawton, 1998). Bio-sciences and psychology are used as reference disciplines and the research approaches utilized include conceptual analysis and empirical theory-testing research. We found that all the information security contributions with respect to access at an organizational level deal with the requirements of integrity, availability, confidentiality and non-repudiation.

The existing organizational-level contributions concerning access to IS seek to maximize users' intent to follow security guidelines. The contributions attempt to ensure the users' commitment to the organizations' security policy based on a) extrinsic deterrence as in Straub (1990), where criminology is used as a reference discipline, and b) non-deterrence motivational factors as in Spurling (1995), McLean (1992), Siponen (2000a), Spruit (1998), and Thompson and Solms (1998), where conceptual analysis is used as a research approach. Spruit has used psychology as a reference discipline, and Siponen (2000a) has used philosophy and psychology as reference disciplines. The role of ethics as a means of ensuring security has been considered by Kowalski (1990), Leiwo and Heikkuri (1998) and Siponen (2000b), all of whom use conceptual analysis, and codes of ethics have been considered by Harrington (1996) using conceptual analysis and empirical, theory-testing research. The aim of these contributions is to ensure that the requirements of integrity, availability and confidentiality are met. Also non-repudiation can be seen to be behind these contributions. It can be seen that employees are responsible for fulfilling their security mission. For example, consider a case where the improper following of a security procedure by an employer results in a security violation. Given that the employee has been assigned to act in the role (and she/he has agreed to it), the employee cannot then deny that it was his/her role responsibility to prevent the violation and follow the guidelines properly.

The question of how to authenticate users by means of passwords has also been studied at the organizational level. In this area of research, scholars have explored the problem of how the process of remembering passwords could be made easier for users. In the search for such cognitive passwords, psychology has been used as a reference discipline and the relevance of cognitive and associative passwords has been considered through empirical theory-testing studies (Zviran & Haga, 1990; Podd et al., 1996).

Secure Communication

Technical and Organizational Levels

Cryptographic techniques are often divided into (1) asymmetric techniques, where correspondents can communicate 'securely' without sharing a secret key (also known as public-key cryptography) and (2) symmetric techniques, where every pair of correspondents, i.e., receiver and sender, needs to share a secret key (also know as private-key cryptography), a category developed by Simmons (1979). Many cryptosystems and/or protocols enriched by cryptography use both of these techniques (hybrid systems). There are also mobile communication systems, such as GSM, which aim at providing anonymity/confidentiality/authentication (Bookson, 1994; Rahnema, 1993). Digital signatures, which are mainly based on asymmetric (public-key) cryptography, are aimed at ensuring information integrity and non-repudiation. In the case of digital signatures, the aim of non-repudiation is to provide evidence for juridical purposes, the objective being that the signer of the message cannot categorically deny that s/he has signed the message[4]. Law is used as the reference discipline. While cryptographic techniques remain at the technical level, non-repudiation objectives are at the organizational level.

A schema for distributing private documents based on Java applets is outlined in Dymond and Jenkin (1999). A taxonomy for key recovery encryption systems has been proposed by Denning and Branstad (1998). The research approach used is conceptual analysis. The main concern for these techniques is to address the requirement of non-repudiation. These contributions encompass the following security requirements: confidentiality, integrity and non-repudiation.

Symmetric algorithms include DES, Blowfish, IDEA, RC2, RC4, and RC5. The IP security protocol (IPSec), which consists of cryptographic techniques, is an approach to secure communication on the

[4] See Brown (1994) for the legal aspects of digital signatures.

Internet and is described by Stackpole (1999) and, in the light of cryptanalysis, by Bellovin (1997). Secure mobile IP is considered by Inoue et al. (1997). The security aspects of virtual private networks are described by Baukari and Aljane (1996) and Bell (1993) on the technical and organizational levels. Intranet security is considered by Collins (1998) on the organizational and technical levels. Mathematics, in particular cryptology, is used as a reference discipline in these solutions. These solutions are aimed at ensuring confidentiality and integrity.

Asymmetric techniques include RSA, ElGamal, and DSS. These solutions encompass the requirements of confidentiality and non-repudiation.

Table 1 shows communication security solutions.

Technique	Confidentiality	Integrity	Non-repudiation
Message Encryption	1		
Digital signatures		2	1
Steganography	1		
Watermarking			1
Hash		1	

Table 1. The existing set of solutions to communication security and the security requirements thereof

In Table 1, the numbers indicate the importance of the requirement, in rank order. For example, the primary aim of a message encryption is confidentiality. Message encryption concerns the process of encrypting and decrypting messages such as e-mail messages. Digital signatures, steganography and watermarking are briefly discussed below. Hash functions take a text (e.g., a message or a program) as an input and produce an output called hash output or simply hash. It has relevance for digital signatures (in the case of digital signatures, a message is hashed and only the hash value of the message is signed) and message integrity (for more, see Menezes et al., 1999).

At the technical level several protocols have been developed for the Internet environment based on symmetric, asymmetric or hybrid cryptography. Secure socket layer (SSL), a general purpose protocol developed by Netscape for communicating securely over the Internet, and PGP, for encrypting electronic mail, are cases in point with respect to hybrid systems (Garfinkel & Spafford, 1997). PGP (version 8.1) is an application program and protocol for encrypting electronic mail by using IDEA, RSA and MD5 algorithms. It (version 8.1) is a hybrid system, using both asymmetric (e.g., RSA) and symmetric (IDEA) encryption. It is available as a stand-alone application as well as integrated in certain e-mail programs. Such techniques attempt to maintain confidentiality (i.e., prevent unauthorized disclosure of information), integrity (prevent unauthorized modification of the information), authentication and/or non-repudiation. Other such systems include S/MIME, which is an extension of the MIME standard which allows users to encrypt e-mail messages by user-specified encryption (Garfinkel & Spafford, 1997), PCT (developed by Microsoft to overcome some of the weaknesses of SSL version 2.0), which is also a transfer layer security protocol (and therefore similar to SSL and TLS), S-HTTP, a protocol providing encryption and signatures as an extension to HTTP. There are also protocols/systems for transmitting payments (based on credit cards, cheque or cash) over the Internet including SET, CyberCash, NetCash, SEPP, and FirstVirtual. These are all on the technical level. A mathematical approach is used as the research approach to develop these techniques and the reference disciplines reflected are mathematics, particularly cryptology. These techniques are aimed at ensuring confidentiality, integrity and non-repudiation. Message digest or check value techniques such as SHA, MD4, and MD5 are primarily used to provide integrity in communication.

On the technical level, steganography, i.e., covered writing - “the science” of hidden communication - has also attracted the interest of scholars (Jamil, 1999). The aim of digital steganography is the transmission of secret messages (any message that can be presented as a bit stream) by embedding the messages into digital images, videos, etc (Johnson & Jajodia, 1998). The limits of steganography are discussed by Anderson and Petitcolas (1998). Three techniques have tackled anonymity in the Internet environment: mixer (Chaum, 1981), crowds (Reiter & Rubin, 1998) and proxy (Rubin & Geer, 1998). By using these techniques, the receiver organization (e.g., a shopping mart) cannot trace the original IP-address. The research approaches used are conceptual analysis and mathematical approaches. The reflected reference discipline is cryptology. These contributions are aimed at maintaining the requirement of confidentiality. The main reference discipline is mathematics, in particular cryptology, and the research approach is based on mathematical approaches.

Conceptual Level

The only conceptual-level contribution within secure communication is proposed by Rieß (1991), who puts forward a technique for modelling security in distributed systems. This is at the conceptual level mainly aimed at ensuring confidentiality and integrity.

Security Management

Technical Level

The consistency aspects of security policies are analyzed by Cholvy and Cuppens, (1997). Eckert (1995) has considered the matching of security policies to the needs of applications. They have used mathematics as a reference discipline. Internet security issues have been addressed by using intelligent agents (Zeng et al. 1997). Security management issues concerning virtual private networks have been put forward (Baukari & Aljane, 1996). These contributions at the technical level encompass the following security requirements: confidentiality, integrity, availability and non-repudiation.

Both Organizational and Technical Levels

The following solutions encompass both organizational and technical levels. The questions of key management with respect to keys used for encryption and decryption (e.g., key generation, registration and certification authorities, key distribution, key backup/recovery/escrow, key replacement or key update, key revocation, key termination) are explored on the organizational and technical levels. Key management refers to the managing of keys used for cryptographic techniques. Cryptographic systems need a key – a secret number which performs the same function as a key in the case of a physical lock - to decrypt or encrypt the message. Key management ensures the requirements of integrity, availability, confidentiality and non-repudiation. Non-repudiation with respect to key management is an important factor paving the way for electronic commerce. These contributions utilize conceptual analysis and mathematical approaches, and mathematics is used as the reference discipline. Contributions include Ford and Baum (1997), and Fumy and Landrock (1993).

Organizational Level

Several checklists (Wood et al., 1987; Moulton & Moulton, 1996) and management standards (BS7799, 1993; GMITS, 1996; ITSEC, 1991) have been laid down. Since these checklists suggest actions or protection mechanisms that organizations should implement, but do not provide any help towards capturing or expressing security requirements, they are classified under "management" rather than "development". These are at the organizational level only. An information security planning methodology has been suggested by Straub and Welke (1998). This framework is at the organizational level; it uses criminology as a reference discipline and is based on empirical theory-testing research – action research in particular.

There also exist several studies on information security policy, such as on requirements for key escrow policies (e.g., Denning & Baugh, 1996), Internet security (Lichtenstein, 1997), and security policies generally: Sterne (1991), Lindup (1995), Abrams and Moffett (1995), Clark and Wilson (1987), and Anderson (1996) for clinical IS. These studies present a variety of predefined security policies. Furthermore, Pounder (1997) goes through the European Union information security proposals, Sanderson and Forcht (1996), Walter (1993) and Wood (1996) stress the importance of security policies, and Dhillon (1997) presents meta-analyses of the meaning of the concept of security policies and related concepts. Moreover, sets of security requirements for more restricted domains include frameworks for network security (Falk & Trommer, 1998), security management in mobile-phone communications (Chan et al., 1993) and the security management aspects of workflow environments (Valia & Al-Salqan, 1997). These contributions at the organizational level encompass the following security requirements: confidentiality, integrity and non-repudiation.

The question of how to construct security guidelines for the end-user is considered by Siponen (2000c), taking philosophy as the reference discipline. Non-formal polices for object-oriented systems have also been considered (Lupu & Sloman, 1997; Yialelis et al., 1996). A conceptual-level framework for policy modelling is put forward by Dobson and McDermid (1989). All these authors have adopted conceptual analysis as their research approach. These studies try to fulfil the requirements of confidentiality, integrity, availability and non-repudiation.

Contingency management has been considered by Smith and Sherwood (1995) and Parker (1998). In addition, security guidelines concerning security aspects of outsourcing have been discussed (Lindgreen et al., 1997). In these cases, no reference disciplines or research approaches have been applied.

Development of Secure IS

Technical Level

Technical-level questions with respect to how to develop secure IS include programming security at the end of the development process. Most of the contributions in the current literature in this area are related to the Internet. Secure GCI/API programming and ActiveX security aspects are discussed by Garfinkel and Spafford (1997) and Ghosh (1998). Java's security features are described by Gong (1997). The weaknesses of Java's (sandbox) security model are considered by Sterbenz (1996), and an improved approach is described by Zhong and Edwards (1998). In addition to these, the security weaknesses of safe-Tcl, including suggested improvements, are given in Gritzalis and Iliadis (1998). Blocking Java applets with the help of a firewall is considered by Martin et al. (1997). Java-related security problems using Netscape Navigator and Microsoft Internet Explorer browsers have been explored by Dean et al. (1996). The security aspects of code distribution in the Internet environment are explored by Zhang (1997). A secure architecture for mobile software agents in the Internet environment is set forth in Vogler et al. (1997). The security issues surrounding mobile agents in general are considered by Karjoth et al. (1997). The security of CORBA is explored by Kyeongbeom et al. (1997). All contributions with respect to secure programming are at the technical level. Röhm et al. (1999) proposed an implementation-oriented language for modelling secure business transactions. Philosophical logic is the reference discipline reflected. Conceptual analysis and a mathematical approach are used as research approaches.

Conceptual Level

A few contributions on the identification and modelling of security requirements exist, including Dubois and Wu (1996), methodologies by Koning (1995) and Bemardi et al. (1994), as well as a methodology for network security (Eloff & Nel, 1992). These methods provide conceptual-level support and use conceptual analysis as the research approach.

There are methods (including modelling techniques), which provide conceptual-level support for developing secure IS. These include Baskerville (1989), Dobson (1991), Pernul (1992), Hitchings (1996), Booysen and Eloff (1995), Pernul et al. (1998) and Ellmer et al. (1995). They provide structural or object-oriented notations for modelling security aspects. In addition, methods and approaches for modelling and analyzing the confidentiality and integrity requirements of business processes have been presented (Herrmann & Pernul, 1999; Röhm et al., 1998). These methods for designing secure IS have used conceptual analysis, artefact-building and evaluation, and empirical research (both theory-creating and testing) as research approaches. Only one of these, Dobson (1991), has used a particular reference discipline: philosophy of language.

Organizational Level

The issue of how to express and model security requirements at the organizational level has been studied (Hitchings, 1996; Backhouse & Dhillon, 1996; James, 1996; Dhillon, 1997; Thomas & Sandhu, 1994). The research approach taken is that of conceptual analysis, and Backhouse and Dhillon (1996) and Dhillon (1997) have used philosophy of language as the reference discipline.

Various versions of risk analysis techniques have traditionally been used in trade-offs between security, usability, other requirements, costs etc. These include Custance (1996), Bennett and Kailay (1992), and Tarr and Kinsman (1996). The research approaches utilized vary from conceptual analysis to mathematical approaches, and in the latter case, mathematics is used as the reference discipline. Moreover, methods for identifying threats have been described by Stacey et al. (1996), and a model for estimating the cost of hazards by Ekenberg et al. (1995). Development standards such as the System Security Engineering Capability Maturity Model (SSE-CMM, 1999a; 1999b) and the Common Criteria also provide answers to these questions.

The meeting of (military) security requirements, and existing security models/policies have been considered by Kolstad and Bowles (1991), and the harmonization of security requirements by Leiwo et al. (1999). Both are at the organizational level, and both use mathematics as the reference discipline and conceptual analysis and mathematical approaches as research approaches.

The testing of information security has been considered within the organizational context by Ceraolo (1996). A testing methodology for intrusion detection systems has also been put forward (Puketza et al., 1996). Several evaluation criteria (a technical assessment of a system's or product's security properties in order to view whether they satisfy the evaluation requirements), including TCSEC, ITSEC and the Common Criteria have been proposed (Abrams & Podell, 1995; Eloff & von Solms, 1998). These criteria are at the organizational level: they elaborate certain criteria that systems or products should satisfy.

Testing with respect to Java security, cryptographic systems and firewalls is discussed in Dima et al.

(1999). The research approach is that of conceptual analysis.

Discussion

In order to obtain a deeper understanding of the information security research contributions, their scope and respective contributions, certain information security issues (access to IS, secure communication, security management, and development of secure IS) were put forward. Four security requirements (integrity, availability, confidentiality, and non-repudiation) were associated with these issues. The results suggest that these security issues were relevant to an analysis of security contributions. The results of the analysis are summarized in Table 2.

The issues of access to IS and secure communication have been the subject of much attention from information security scholars. The issues of access to IS and communication have mainly been approached at the technical level using mathematical approaches (including logic) as a research approach and mathematics (including logic) as the main research discipline. While organizational-level contributions with respect to the issues of access to IS, security management and development of secure IS have been put forward, most of the contributions remain at the technical level. Moreover, there are studies exploring the issue of access using empirical theory-testing and conceptual analysis as research approaches, as well as a few attempts utilizing philosophy, psychology and criminology as reference disciplines.

Information security issue	Contributions				
	Organizational	Conceptual	Technical	Reference disciplines	Research approaches
Access to IS	Biometrical authentication, cognitive passwords, maximizing users' intent to comply with security policy (through deterrence and motivation means).	Access control matrix, modelling of access control policies	Authentication methods (passwords, token-based authentication), access control and information-flow control models, memory protection of operating systems, anti-virus techniques, watermarking, image security, audit/intrusion detection, firewalls	Mathematics and philosophical logic, bio-sciences, psychology, criminology, philosophy	Mathematical approaches (mathematical modelling), theory-testing research, conceptual analysis.
Secure Communication	Virtual private networks, Intranet security	Modelling security in distributed systems	Cryptographic techniques, including message encryption, digital signatures, steganography, watermarking, hash, virtual private networks, electronic cash, Intranet security, anonymity techniques	Mathematics (in particular cryptology), law	Mathematical approaches (mathematical modelling), conceptual analysis.
Security Management	Key management, creation of organizational security policies and guidelines, backup and contingency management, security checklist and management standards, security management methods, security of outsourcing		Key management, management of security policies, virtual private networks	Mathematics, law, criminology, philosophy	Mathematical approaches (mathematical modelling), conceptual analysis, empirical theory-testing research and theory-creating research.
Development	Risk management, security methods for developing secure IS, testing methods and methodologies.	Notations for modelling security semantics	Programming and programming language security	Mathematics, philosophy	Mathematical approaches (mathematical modelling), conceptual analysis, artefact-building and evaluating research, empirical theory-testing research and theory-creating research.

Table 2. The main research contributions found

The finding that information security research has concentrated on technical problems suggests some implications from an IS point of view. First, the introduction of technological solutions always raises the question of how motivated users are to adopt those solutions (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. For instance, cryptography-based solutions have been well researched (compared to non-technical security issues), but "key management policies" have attracted little interest, despite the fact that one of the main issues with respect to symmetric or asymmetric cryptography is clearly the issue of management. This means that cryptographic solutions, whether symmetric (one-key systems) or asymmetric (two-key systems), depend on successful key management (Davis & Ylönen, 1997).

Similarly, access control polices have attracted great interest among information security researchers. Access control polices are still unable to prevent leaks of information; in other words, access control polices do not prevent abusers from obtaining information from authorized users (at the organizational level) nor do they prevent authorized users from being able to spread top-secret information. Despite this weakness, little research has been carried out to tackle this issue at an organizational level.

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

Across all information security studies, and particularly meta-analyses, few overview studies are to be found. We believe that the neglect of interpretive reviews, including meta-studies, can be traced back to the predominant research interest of the security community: the interest in pragmatic research (Niiniluoto, 1990). This means results that can be quickly brought into practice are favoured. As far as critical studies are concerned, the communities of cryptologists and computer scientists in the field of computer security provide an exception. It seems that research which does not utilize mathematical approaches, but produces different procedures, principles, methods and other non-technical research results, is all too often uncritically accepted; or perhaps this kind of research does not receive enough interest from scholars.

Our study also shows that technical solutions are developed using mathematical approaches as the primary research approach. As the technical context focuses on presenting information in a form understandable by computers, mathematical and logical modelling are relevant research approaches. For the same reason, analytical philosophy and mathematics are pertinent reference disciplines at the technical level.

With respect to conceptual-level contributions, methods for the development of secure IS are found to prevail at this level. These information security development methods propose different notations for modelling security aspects of IS at the conceptual level. No particular reference discipline is adopted. These methods reflect developments in the areas of software engineering and IS development methods. The predominant research approaches are conceptual analysis. Hence, little is known about the strengths and problems associated with the utilization of the information security methods in organizations. More empirical theory-testing and theory-creating research is therefore needed in order to learn more about the usability and ease of use of the different methods for developing secure IS. Furthermore, the possible social-organizational implications of information security methods, when applied to organizations, should be studied. With respect to the theory-testing and theory-creating research approaches, the use of qualitative and interpretive research methodologies, including case and field studies (Cunningham, 1997) and action research (Baskerville & Wood-Harper, 1998), is welcomed.

We take the position that since the conceptual-level contributions are about modelling security-relevant entities and activities, philosophy of language and semiotics may be relevant contributory disciplines for methods for the development of secure IS in general and information security notations in particular.

As with the organizational context, the prevailing research approaches were found to be conceptual analysis and empirical research. The amount of empirical studies with respect to different issues continues to be sparse. Philosophy, psychology and criminology were utilized as reference disciplines. From an information security management viewpoint, further research is needed with respect to several issues. With respect to studies at an organizational level, the existing empirical research focuses mainly on the use of deterrence theory (based on criminology) to terminate security violations (e.g., Straub, 1990). Thus, while the role of deterrents have been studied extensively (Straub, 1990), the possibilities offered by non-deterrence motivational strategies based on psychology (motivation theories) and philosophy (theories of ethics) are still largely unexplored areas. In particular, empirical works are needed, examining how to ensure that users are committed to security policy by means of motivational strategies, including the use of rewards. The potential reference theories include Deci and Ryan (1985)'s intrinsic motivation, the theory of planned behaviour (TPB) by Ajzen (1991), and the technology acceptance model (Davis, 1989). Also with respect to non-deterrence motivational strategies, the potential offered by human morality with respect to the prevention of computer abuses and security violations (Siponen, 2001) should be explored in empirical studies. In this case, theories of ethics are the candidate reference theories, and both qualitative (e.g., survey) and quantitative studies (interviews) are welcomed.

Summary

This paper studied the key information security issues and respective research contributions. The information security contributions were analyzed from the viewpoints of a meta-model for IS, the research approaches employed, and the reference disciplines utilized. The analysis showed that information security research has focused primarily on technical issues. The main reference disciplines have been mathematics and philosophical or mathematical logic, and the most common research approach has been through mathematical approaches. Based on the findings, several implications for research were proposed. While the issues of access to IS and secure communications have been widely recognized, there is a great need for empirical studies on the development of secure IS and security management (using empirical theory-creating and testing, and utilizing qualitative and quantitative studies) based on appropriate reference theories (e.g., psychology, sociology, semiotics, and philosophy).

References

Abrams, M. D. and Moffett, J. T. (1995). "A Higher Level of Computer Security Through Active Policies," *Computer & Security*, Vol. 14, No. 2, pp. 147-157.

Abrams, M. D. and Podell, H. J. (1995). "Evaluation Issues," in Abrams, M.D., Jajodia, S. and Podell, H.J. (Eds.), *Information Security - An Integrated Collection of Essays*, Los Alamitos, CA: IEEE Computer Society Press.

Ajzen, I. (1991). "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, Vol. 50, pp. 179-211.

Anderson, R. (1996). "A Security Policy Model for Clinical Information Systems," *Proceedings of the 1996 IEEE Symposium on Security and Privacy*.

Anderson, R., and Kuhn, M. (1996). "Tamper Resistance - a Cautionary Note," *Proceedings of The Second USENIX Workshop on Electronic Commerce*, Oakland, California, pp. 18-21.

Anderson, R. J. and Petitcolas, F. A. P. (1998). "On the Limits of Steganography," *IEEE Journal on Selected Areas in Communications*, Vol. 16, Is.4, pp. 474-481.

Backhouse, J. and Dhillon, G. (1996). "Structures of Responsibilities and Security of Information Systems," *European Journal of Information Systems*, Vol. 5, No. 1, pp. 2-10.

Baldwin, R. W. (1990). "Naming and Grouping Privileges to Simplify Security Management in Large Databases," *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*.

Banville, C. and Landry, M. (1989). "Can the Field of MIS be Disciplined?" *Communications of the ACM*, Vol. 32, No. 1, pp. 48-60.

Baskerville, R. (1988). Designing Information Systems Security, Information Systems Series: John Wiley.

Baskerville, R. (1989). "Logical Controls Specification: An Approach to Information System Security," in Klein, H., and Kumar, K. (Eds.), *Systems Development for Human Progress*, Amsterdam: North-Holland.

Baskerville, R. (1991). "Risk Analysis: An Interpretative Feasibility Tool In Justifying Information Systems Security," *European Journal of Information Systems*, Vol. 1, Is.2, pp. 121-130.

Baskerville, R. (1993). "Information Systems Security Design Methods: Implications for Information Systems Development," *Computing Surveys*, Vol. 25, No. 4, pp. 375-414.

Baskerville, R. and Wood-Harper, A. T. (1998). "Diversity in Information Systems Action Research Methods," *European Journal of Information Systems*, Vol. 7, pp. 90-107.

Baukari, N. and Aljane, A. (1996). "Security and Auditing of VPN," *Proceedings of Third International Workshop on Services in Distributed and Networked Environments*.

Bell, R. (1993). "Virtual Private Networks - The Major Issues, Problems and Opportunities," *IEE Colloquium on Virtual Networking*.

Bellovin, S. M. (1997). "Probable Plaintext Cryptanalysis of the IP Security Protocols," *Proceedings of the 1997 Symposium on Network and Distributed Systems Security*.

Bellovin, S. M. and Cheswick, W. R. (1994). "Network Firewalls," *IEEE Communications Magazine*, Vol. 32, Is.9, pp. 50-57.

Bemardi, A., Rico, N., Cherkaoui, O., and Banfield, J. (1994). "Specification and Analysis of A Security Management System," *Proceedings of the IEEE Network Operations and Management Symposium*.

Bennett, S.P. and Kailay, M.P. (1992). "An Application of Qualitative Risk Analysis to Computer Security for the Commercial Sector," *Proceedings of the Eight Annual Computer Security Applications Conference*.

Bishop, M. (1991). "An Overview of Computer Viruses in a Research Environment," *4th DPMA, IEEE, ACM Computer virus and Security Conference*.

Bontchev, V. (1996). "Possible Macro Virus Attacks and How to Prevent Them," *Computers & Security*, Vol. 15, No. 7, pp. 959-626.

Bookson, C. (1994). "GSM Security: A Description of the Reasons for Security and the Techniques," *IEE Colloquium on Security and Cryptography*.

Booysen, H. A. S. and Eloff, J. H. P. (1995). "A Methodology for the Development of Secure Application Systems," *Proceeding of the 11th IFIP TC11 International Conference on Information Security*.

Boswell, A. (1995). "Specification and Validation of a Security Policy Model," *IEEE Transaction on Software Engineering*, Vol. 21, Is.2, pp. 63-68.

Brown, P. W. (1994). "Digital Signatures: Are They Legal for Electronic Commerce?" *IEEE Communications Magazine*, Vol. 32, Is.9, pp. 76-80.

BS7799 (1993). *British Standard Institution*, London, UK.

Busch, G., Funk, W., and Wolthusen, S. (1999). "Digital Watermarking: From Concepts to Real-Time Video Applications*," IEEE Computer Graphics and Applications*, Vol. 19, No. 1., pp. 25-36.

Castano, S., Fugini, M., Martell, G., and Samarati, P. (1995). *Database Security*, Boston, MA: Addison-Wesley.

Ceraolo, J. P. (1996). "Penetration Testing Through Social Engineering," *Information Systems Security*, Vol. 4, No. 4.

Chan, K. L., Kwong, S., and Longginnou, L. (1993). "Security Management on Mobile-Phone Communication," *Proceedings of the Computer, Communication, Control and Power Engineering*.

Chang, C. C. and Hwang, S. J. (1991). "Cryptographic Authentication of Passwords," *Proceedings of 25th Annual 1991 IEEE International Carnahan Conference on Security Technology*.

Chang, C. C., Hwang, R. J., and Buehrer, D. (1993). "Using Smart Cards to Authenticate Passwords," *Proceedings, Institute of Electrical and Electronics Engineers 1993 International Carnahan Conference on Security Technology*..

Chaum, D. (1981). "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communication of ACM*.

Cholvy, L. and Cuppens, F. (1997). "Analysing Consistency of Security Policies," *Proceedings of 1997 IEEE Symposium on Security and Privacy*.

Clark, D. D. and Wilson, D. R. (1987). "A Comparison of Commercial and Military Security Policies," *Proceedings of the 1987 IEEE Symposium on Security and Privacy*.

Cohen, F. (1984). "Computer Viruses - Theory and Experiments," *Proceedings of IFIP/SEC'84*.

Cohen, F. (1991). "Current Best Practice Against Computer Viruses," *Proceedings of 25th Annual 1991 IEEE International Carnahan Conference on Security Technology*.

Collins, B. (1998). "Designing Secure Intranets," *Computing & Control Engineering Journal*, Vol. 9, Is.4, pp. 185-192.

Computer Fraud & Security Bulletin (2000). Elsevier Advanced Technology.

Craver, C. and Yeo (1998). "Technical Trials and Legal Tribulations," *Communications of the ACM,* Vol. 41, No. 7, p. 45-54.

Cunningham, J. B. (1997). "Case Study Principles for Different Types of Cases," *Quality & Quantity*, Vol. 31, pp. 401-423.

Custance, N. D. E. (1996). "The Use of Baseline Measures in Risk Assessment," *Proceedings of the 30th Annual International Carnahan Conference on Security Technology. IEEE Computer Society Press*.

Cusumano, M. A. and Yoffie, D. B. (1999). "Software Development on Internet Time," *IEEE Computer*, Vol. 32, No. 10, pp. 60-69.

Dacier, M. and Deswarte, Y. (1994). "Privilege Graph: An Extension to the Typed Access Matrix Model," *Proceedings of the Third European Symposium on Research in Computer Security (ESORICS)*, Sringer-Verlag.

Davis, B. C. and 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.

Dean, D., Felten, E.W., Wallach, D.S., and Balfanz, D. (1996). "Java Security: Web Browsers and Beyond," *Proceedings of 1996 IEEE Symposium on Security and Privacy*, Reprinted in Denning, D.E., and Denning, P.J. (1998) (Eds), *Internet Besieged: Countering Cyberspace* Scofflaws, New York: ACM Press, pp. 241-269.

Deci, E. L. and Ryan, R. M. (1985). *Intrinsic Motivation and Self-Determination in Human Behavior*, New York: Plenum Press.

Denning, D.E, (1976). “A Lattice Model of Secure Information Flow,” *Communication of the ACM*, Vol. 19, No. 5, pp. 236-243.

Denning, P.J. (1992). “Passwords,” *American Scientist*, Vol. 80, pp. 117-120.

Denning, D.E and Baugh, W.E., Jr. (1996). “Key Escrow Encryption Policies and Technologies,” *Information Systems Security*, Vol. 5, No. 2, pp. 34-44.

Denning, D. E. and Branstad, D. K. (1998). *A Taxonomy for Key Recovery Encryption Systems. in Internet Besieged: Countering Cyberspace Scofflaws,* Denning, D.E. and Denning, P.J. (Ed.), New York: ACM Press, pp. 357-375.

Dhillon, G. (1997). *Managing Information Systems Security,* United Kingdom: MacMillan Press LTD.

Dhillon, G. and Backhouse, J. (2001). “Current Directions in IS Security Research: Toward Socio-organizational Perspectives,” *Information Systems Journal*, Vol. 11, No. 2.

Diaz, P, Aedo, A., and Panetsos, F. (1997). “Modelling Static and Dynamic Aspects of Hypermedia,” *Proceedings of the IEEE International Conference on Multimedia Computing and Systems ‘97*.

Diaz, P, Aedo, A., and Ribagorda, A. (1998). “A Security Model for the Design of Hypermedia Systems,” *Proceedings of the TC11 14th International Conference on Information Security (SEC’98)*.

Dima, A., Wack, J., and Wakid, S. (1999). “Raising the Bar on Software Security Testing,” *IT Professional*, Vol. 1, Is.3, pp. 27 - 32.

Dobson, J. (1991). “A Methodology for Analysing Human and Computer-Related Issues in Secure Systems,” in Dittrich, K., Rautakivi, S., and Saari, J. (Eds.), *Computer Security and Information Integrity*, Elsevier Science Publishers.

Dobson, J. E., McDermid, J.A., (1989), A Framework for Expressing Models of Security Policy. 1989 IEEE Symposium on Security and Privacy.

Dubois, E. and Wu, S. (1996). “A Framework for Dealing With and Specifying Security Requirements in Information Systems,” *Proceedings of IFP SEC’96*.

Dymond, P. and Jenkin, M. (1999). “WWW Distribution of Private Information with Watermarking,” *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences (HICSS-32)*.

Eckert, C. (1995). “Matching Security Policies to Application Needs,” *Proceedings of the IFIP TC11 Eleventh International Conference on Information Security, IFIP/SEC’95*.

Ekenberg, L., Oberoi, S., and Orci, I. (1995). “A Cost Model for Managing Information Security Hazards,” *Computers & Security*, Vol. 14, No. 8, pp. 707-717.

Ellmer, E., Pernul, G., and Kappel, G. (1995). “Object-Oriented Modeling of Security Semantics,” *Proceedings of the 11th Annual Computer Society Applications Conference (ACSAC’95)*.

Eloff, J. H. P. and Nel, A. J. (1992). “A Methodology for Network Security,” *Proceedings of the International Workshop on Advanced Communications and Applications for High Speed Networks*, IEEE Computer Society Press.

Eloff, J. H. P and von Solms, R. (1998). “Measuring the Information Security Level in an Organization,” *Proceedings of the Sixth Working Conference of Workgroup 11.1 and Workgroup 11.2 of Technical Committee 11*.

Falk, R. and Trommer, M. (1998). “Managing Network Security - a Pragmatic Approach,” *Proceedings of the Seventeenth IEEE Symposium on Reliable Distributed Systems.*

Fernandez, E.B. and Nair, K.R. (1998). “An Abstract Authorization System for the Internet,” *Proceedings of the Ninth International Workshop on Database and Expert Systems Applications*.

Foley, S.N. (1991). “A Taxonomy for Information Flow Policies and Models,” *Proceedings of the 1991 IEEE Computer Security Symposium on Research in Security and Privacy*.

Ford, W. and Baum, M. S. (1997). *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures & Encryption*, Upper Saddle River, NJ: Prentice Hall.

Fumy, W. and Landrock, P. (1993). “Principles of Key Management,” *IEEE Journal on Selected Areas in Communications*, Vol. 11, Is.5, pp. 785 - 793.

Galliers, R. D. and Land, F. F. (1987). “Choosing Appropriate Information Systems Research Methodologies,” *Communication of the ACM*, Vol. 30, No. 11, pp. 900-902.

Garfinkel, S. and Spafford, G. (1997). *Web Security & Commerce*, Sebastopol, CA: O’Reilly & Associates, Inc.

Garvey, T.D. (1992). “The Inference Problem for Computer Security,” *Proceedings of Computer Security Foundations Workshop V*.

Garvey, T. D. and Lunt, T. (1991). “Model-Based Intrusion Detection,” *Proceedings of the 14th National Computer Security Conference*, Washington D.C.

Ghosh, A. K. (1998). *E-Commerce Security: Weak Links, Best Defenses*, Hoboken, NJ: Wiley Computer Publishing.

GMITS (1996), Guidelines for the Management of IT Security, Part 1: Concepts and Models for IT Security. ISO/IEC TR 13335-1.

Gong, L. (1993). “Increasing Availability and Security of an Authentication Service,” *IEEE Journal on Selected Areas on Communication*, Vol. 11, Is.5, pp. 657-662.

Gong, L. (1995). “Optimal Authentication Protocols Resistant to Password Guessing Attacks,” *Proceedings of the Eighth IEEE Computer Security Foundations Workshop*, IEEE Computer Society Press.

Gong, L. (1997). “Java Security: Present and Near Future,” *IEEE Micro*, Vol. 17, Is.3, pp. 14-19.

Gove, R. A. (1999*). Fundamentals of Cryptography and Encryption. Handbook of Information Security Management 1999*, Krause, M., and Tipton, H.F. (Eds.), Boca Raton, FL: CRC Press.

Gritzalis, S. and Iliadis, J. (1998). “Addressing Security Issues in Programming Languages for Mobile Code,” *Proceedings of the Ninth International Workshop on Database and Expert System Applications. IEEE Computer Society Press*.

Harrington, S. J. (1996). “The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgements and Intentions,” *MIS Quartely*, Vol. 20, No. 3.

Harrison, M. A., Ruzzo, W.L., and Ullman, J.D. (1976). “Protection in Operating Systems,” *Communication of the ACM,* Vol. 19, No. 8, pp. 461-471.

Hendry, M. (1997). *Smart Card Security and Applications*, Norwood, MA: Artech House.

Herrmann, G. and Pernul, G. (1999). “Viewing Business-Process Security from Different Perspectives,” *International Journal of Electronic Commerce*, Vol. 3, No. 3, pp. 89-103.

Hirschheim, R., Klein, H. K., and Lyytinen, K. (1996). “Exploring the Intellectual Structures of Information Systems Development: A Social Action Theoretic Analysis, *Accounting, Management and Information Technologies*, Vol. 6, No. 1-2, pp. 1-64.

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, IFIP/SEC’96*.

Hruska, J. (1997). “Virus Detection,” *European Conference on Security and Detection (ECOS’97).*

Ilgun, K., Kemmerer, R. A., and Porras, P. A. (1995). “State Transition Analysis: A Rule-based Intrusion Detection Approach,” *IEEE Transaction on Software Engineering*, Vol. 21, No. 3, pp. 222-232.

Iivari, J. (1989). “Levels of Abstraction as a Conceptual Framework for an Information System,” In Falkenberg, E.D., and Lindgreen, P., (Eds), *Information System Concepts: An In-depth Analysis*., North-Holland, Amsterdam.

Iivari, J. (1991). “A Paradigmatic Analysis of Contemporary Schools of IS Development,” *European Journal of Information Systems*, Vol. 1, No. 4, pp. 249-272.

Iivari, J. and Hirschheim, R. (1996). “Analyzing Information Systems Development: A Comparison and Analysis of Eight IS Development Approaches,” *Information Systems*, Vol. 21, No. 7, pp. 551-575.

Iivari, J., Hirschheim, R., and Klein, H. K. (1998). “A Paradigmatic Analysis of Contrasting Information Systems Development Approaches and Methodologies,” *Information Systems Research*, Vol. 9, No. 2, pp. 164-193.

Iivari, J., Hirschheim, R., and Klein, H. K. (2001). “A Dynamic Framework for Classifying Information Systems Development Methodologies and Approaches,” *Journal of Management Information Systems*, Vol. 17 No. 3, pp. 179-218.

Inoue, A., Ishiyama, M., Fukumoto, A., and Okamoto, T. (1997). “Secure Mobile IP Using Security Primitives,” *Proceedings of the Sixth IEEE Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*.

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.

Jacob, J. (1991). “A Uniform Presentation of Confidentiality Properties,” *IEEE Transactions on Software Engineering*, Vol. 17, No. 1, pp. 1186-1194.

Jajodia S., Sandhu, R. S., and Blaustein B. T. (1995). “Solutions to the Polyinstantiation Problem,” in Abrams, M.D., Jajodia, S., and Podell, H.J. (Eds.), *Information Security, An Integrated Collection of Essays*, Los Alamitos, CA: IEEE Computer Society Press.

James, H. L. (1996). “Managing Information Systems Security: A Soft Approach,” *Proceedings of the Information Systems Conference of New Zealand*, IEEE Society Press.

Jamil, T. (1999). “Steganography: The Art of Hiding Information in Plain Sight,” IEEE *Potentials*, Vol. 18, Is.1, pp. 10-12.

Jobush, D. L. and Oldehoeft, A. E. (1989). “Survey of Password Mechanisms: Weaknesses and Potential Improvements, Part 1,” *Computers & Security*, Vol. 8, pp. 587-604.

Johnson, N. F. and Jajodia, S. (1998). “Exploring Steganography: Seeing the Unseen,” *IEEE* Computer, Vol. 31, No. 2, pp. 26-34.

Järvinen, P. (2000). “Research Questions Guiding Selection of an Appropriate Research Method,” *Proceedings of the 8th European Conference on Information Systems (ECIS 2000)*, Vienna.

Karjoth, G., Lange, D. B., and Oshima, M. (1997). “A Security Model for Aglets,” *IEEE Internet Computing*, Vol. 1, Is.4, pp. 68 - 77.

Kemmerer, R. A. (1983). "Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels," *ACM Transaction on Computer Systems*, Vol. 1, No. 3, pp. 256-277.

Kemmerer, R.A. andPorras, P.A. (1991). "Covert Flow Trees: A Visual Approach to Analyzing Covert Storage Channels," *IEEE Transactions on Software Engineering*, Vol. 17, No. 11, pp. 1166-1185.

Kolstad and Bowles (1991). "Security Requirements and Models in Open Systems," *Proceedings of the Twenty-Third Southeastern Conference on Systems Theory*.

Koning, W. and Fred. D. (1995). "A Methodology for the Design of Security Plans," *Computers & Security*, Vol. 14, No. 7, pp. 633-643.

Kowalski, S. (1990). "Computer Ethics and Computer Abuse: A Longitudinal Study of Swedish University Students," *IFIP TC11 6th International Conference on Information Systems Security*.

Kwon, T. and Son, J. (1998). "Authenticated Exchange Protocols Resistant to Password Guessing Attacks," *IEE Proceedings of Communication*, Vol. 145, Is.5.

Kyeongbeom, K., Youngkyun K., Youngkee S., and Soran, I. (1997). "A Software Platform for Secure Applications Based on CORBA," *Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems*.

Lampson, B. W. (1971). "Protection," *Proceedings of the 5th Annual Princeton Conference on Information Science and Information Systems*, Reprinted in ACM Operating System review, January 1974.

Lawton, G. (1998). "Biometrics: A New Era in Security," *IEEE* Computer, Vol. 31, No. 8, pp. 16 - 18.

Lee, J. S., Hsiang, J., and Tsang, P. H. (1997). "A Generic Virus Detection Agent on the Internet," *Proceedings of the Thirtieth Hwaii International Conference on System Sciences (HICSS'97)*.

Leiwo, J. and Heikkuri, S. (1998). "An Analysis of Ethics as Foundation of Information Security in Distributed Systems," *Proceedings of the 31st Hawaiian International Conference on System Sciences (HICSS-31)*, Hawaii.

Leiwo, J., Gamage, C., and Zheng, Y. (1999). "Harmonization of Information Security Requirements," *Informatica*, Vol. 17.

Lichtenstein, S. (1997). "Developing Internet Security Policy for Organizations," *Proceedings of the Thirtieth Hwaii International Conference on System Sciences*.

Lindgreen, E. R., Janus, H. R. D., Shahim, A., Hulst, G., and Herscberg, I. S. (1997). "Security When Outsourcing: Concepts, Constructs, Compliance," *Proceedings of the IFIP TC11 13th International Conference on Information Security (SEC'97).*

Lindup, K. R. (1995). "A New Model for Information Security Policies," *Computer & Security*, Vol. 14, No. 8, pp. 691-695.

Lodin, S. W. and Schuba, C. L. (1998). "Firewalls Fend Off Invasions from the Net," *IEEE Spectrum*, Vol. 35, Is.2, pp. 26-34.

Lupu, E. and Sloman, M. (1997). "A Policy Based Role Object Model," *Proceedings of the First International Enterprise Distributed Object Computing Workshop*, IEEE Computer Society Press.

Lyytinen, K. (1987). "A Taxonomic Perspective of Information Systems Development: Theoretical Constructs and Recommendations," in Boland, R.J., and Hirscheim, R.A. (Eds.), *Critical Issues in Information Systems Research*, Hoboken, NJ: John Wiley & Sons Ltd.

March, S. T. and Smith, G. F. (1995). "Design and Natural Science Research on Information Technology," *Decision Support Systems*, Vol. 15, pp. 251-266.

Martin, D. M., Rajagopalan, S., and Rubun, A. D. (1997). "Blocking Java Applets at the Firewall," *Proceedings of the 1997 Symposium on Network and Distributed System Security*, IEEE Computer Society Press.

Mathieson, K. (1991). "Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behaviour," *Information System Research*, Vol. 3, No. 2, pp. 173-191.

McLean, J. (1990). "The Specification and Modelling of Computer Security," *IEEE Computer*, Vol. 23, IS.1, pp. 9-16.

McLean, K. (1992). "Information Security Awareness - Selling the Cause," in Gable, G., et al. (Eds.), *Security and Control: From Small Systems to Large*, *Proceedings of the IFIP TC11 /SEC'92*, Singapore, pp. 27-29.

Menezes, A. J., van Oorschot, P. C. and Vanstone, S. C. (1999). *Handbook of Applied Cryptography*, Boca Raton, FL: CRC Press.

Millen, J. (1999). "20 Years of Covert Channel Modeling and Analysis," *Proceedings of the 1999 IEEE Symposium on Security and Privacy*.

Miller, B. (1994). "Vital Signs of Identity," *IEEE Spectrum*, Vol. 31, Is.2, pp. 22-30.

Molva, R., Samfat, D., and Tsudik, G. (1994). "Authentication of Mobile Users," *IEEE Network*, Vol. 8, Is.2, pp. 26-34.

Moulton, R. T. and Moulton, M. E. (1996). "Electronic Communications Risk Management: A Checklist for Business Managers," *Computer & Security*, Vol. 15, No. 5.

Moskowitz, I. S. and Kang, M. H. (1994). "Covert Channels – Here to Stay*?" Proceedings of the Ninth Annual Conference on Computer Assurance (COMPASS '94) Safety, Reliability, Fault Tolerance, Concurrency and Real Time, Security*.

Needham, R. M. (1989). "Authentication," in Anderson, T. (Ed.), *Safe & Secure Computing Systems*, Blackwell Scientific Publications, pp. 189-196.

Niiniluoto, I. (1990). "Science and Epistemic Values," *Science Studies*, Vol. 3, No. 1, pp. 21-26.

Notargiacomo, L. (1995). "Architectures for MLS Database Management Systems," in Abrams, M.D., Jajodia, S., and Podell, H.J. (Eds.), *Information Security, An Integrated Collection of Essays*, Los Alamitos, CA: IEEE Computer Society Press.

Nunamaker, J. F., Chen, M., and Purdin, T.D.M. (1991). "Systems Development in Information Systems Research," *Journal of Management Information Systems*, Vol. 7, No. 3, pp. 89-106.

O'Sullivan, J. A., Moulin, P., and Ettinger, J. M. (1998). "Information Theoretic Analysis of Steganography," *Proceedings of 1998 IEEE International Symposium on Information Theory*.

Parker, D. B. (1998). *Fighting Computer Crime - A New Framework for Protecting Information*, Hoboken, NJ: Wiley Computer Publishing.

Podd, J., Bunnell, J., and Henderson, R. (1996). "Cost-effective Computer Security: Cognitive and Associative Passwords," *Proceedings of the Sixth Australian Conference on Computer-Human Interaction*.

Pernul, G. (1992). "Security Constraint Processing During Multilevel Secure Database Design," *Proceedings of the 8th Annual Computer Security Applications Conference*, IEEE Society Press.

Pernul, G. (1994). "Database Security," *Advances in Computers*, Vol. 38, Yovits, M.C. (Ed.), Academic Press.

Pernul, G. and Quirchmayr, G. (1994). "Organizing MLS Databases from a Data Modelling Point of View," *Proceedings of the 10th Annual Computer Security Applications Conference*, IEEE Society Press.

Pernul, G., Tjoa A. M., and Winiwarter, W. (1998). "Modeling Data Secrecy and Integrity," *Data & Knowledge Engineering*, Vol. 26, pp. 291-308.

Pounder, C. (1997). "First Steps Towards a European Union Policy on the Securing of Electronic Communications," *Computers & Security*, Vol. 16, Is.7, pp. 590-594.

Puketza, N. J., Zhang, K., Chung, M., Mukherjee, B., and Olsson, R.A. (1996). "A Methodology for Testing Intrusion Detection Systems," *IEEE Transactions on Software Engineering*, Vol. 22, Is.10, pp. 719-729.

Rahnema, M. (1993). "Overview of the GSM System and Protocol Architecture," *IEEE Communications Magazine*, pp. 92-100.

Reiter, M. and Rubin, A.D. (1998). "Crowds: Anonymity for Web Transactions," *ACM Transactions on Information and System Security*, Vol. 1, No. 1.

Rieß, H. P. (1991). "Modeling Security in Distributed Systems," in Dittrich, K., Rautakivi, S., and Saari, J. (Eds.), *Computer Security and Information Integrity*, Elsevier Science Publishers.

Rubin, A. W. and Geer, D. E. (1998). "A Survey of Web Security," *IEEE Computer*, September, pp. 34-41.

Ryan, P. Y. A. and Schneider, S. A. (1999). "Process Algebra and Non-interference," *Proceedings of the 12th IEEE Computer Security Foundations Workshop*.

Röhm, A. W., Pernul, G., and Herrmann, G. (1998). "Modelling Secure and Fair Electronic Commerce," *Proceedings of the 14th Annual Computer Security Applications Conference*.

Röhm, A. W., Herrmann, G., and Pernul, G. (1999). "A Language for Modeling Secure Business Transactions," *Proceedings of the IEEE Annual Computer Security Applications Conference (ACSAC'99)*.

Sanderson, E. and Forcht, K. (1996). "Information Security in Business Environments," *Computers & Security*, Vol. 15, Is.4, pp. 321-322.

Sandhu, R., Bhamidipati, V., Coyne, E., Ganta, S., and Youman, C. (1997). "The ARBAC97 Model for Role-Based Administration of Roles: Preliminary Description and Outline," *Proceedings of the Second ACM Workshop on Role-Based Access Control,* Fairfax, VA: ACM Press.

Sandhu, R. S. (1988). "The Schematic Protection Model: Its Definition and Analysis of Acyclic Attenuation Schemes," *Journal of the ACM*, No. 2, pp. 404-432.

Sandhu, R. S. (1992). "The Typed Access Matrix Model," *Proceedings of the 1992 IEEE Symposium on Research in Security and Privacy*.

Sandhu, R. S. (1993). "Lattice-based Access Controls," *IEEE Computer*, Vol. 26, No. 11, pp.9-19.

Sandhu, R. and Samarati, P. (1996). "Authentication, Access Control, and Audit," *ACM Computing Surveys*, Vol. 28, No. 1.

Sandhu, R. S., Coyne, E. J., Feinstaein, H .L., and Youman, C. E. (1996). "Role-based Access Control Models," *IEEE Computer*, Vol. 29, Is.2, pp. 38-47.

Sandhu, R. (1998). "Role-Based Access Control," *Advances in Computers*, Vol. 46, Academic Press.

Simmons, G. J. (1979). “Symmetric and Asymmetric Encryption,” *ACM Computing* Surveys, Vol. 11, No. 4, pp. 305-330.

Simmons, G. J. (1988). “A Survey of Information Authentication,” Invited Paper, *Proceedings of the IEEE*, Vol. 76, Is. 5, pp. 603-620.

Siponen, M. T. (2000a). “A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security*, Vol. 8, Is.1, pp. 31-41.

Siponen, M. T. (2000b). “On the Role of Human Morality in Information System Security: The Problems of Descriptivism and Non-descriptive Foundations,” *15th International Information Security Conference (IFIP TC11/SEC2000)*, Beijing, China.

Siponen, M. T. (2000c). “Policies for Construction of Information Systems’ Security Guidelines: Five Approaches,” *15th International Information Security Conference (IFIP TC11/SEC2000)*, Beijing, China.

Smith, M. and Sherwood, J. (1995). “Business Continuity Planning,” *Computers & Security*, Vol. 14, No. 1, pp. 14-23.

Spafford, E. G. (1998). “Computer Viruses,” in Denning, D. E., and Denning, P. J. (Eds.), *Internet Besieged: Countering Cyberspace Scofflaws*, New York: ACM Press, pp. 73-95.

Spruit, M.E.M. (1998). “Competing Against Human Failing,” *15th IFIP World Computer Congress. ‘The Global Information Society on the Way to the Next Millennium’. SEC, TC11*, Vienna.

Spurling, P. (1995). “Promoting Security Awareness and Commitment,” *Information Management and Computer Security*, Vol. 3 No. 2.

SSE-CMM (1999a). “The Model,” v2.0. http://www.sse-cmm.org.

SSE-CMM (1999b). “The Appraisal Method,” v2.0. http://www.sse-cmm.org.

Stacey, T. R., Helsley, R. E., and Baston, J. V. (1996). “Identifying Information Security Threats,” *Information Systems Security*, Vol. 5, No. 3 , pp. 50-59.

Stackpole, B. (1999). “An Introduction to IPSEC,” in Krause, M., and Tipton, H.F. (Eds.), *Handbook of Information Security Management*, Auerbach, pp. 387-399.

Sterbenz, A. (1996). “An Evaluation of the Java Security Model,” *12th Annual Computer Security Applications Conference*.

Sterne, D. F. (1991). “On the Buzzword ‘Security Policy’,” *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, Los Alamitos, CA: IEEE Society Press, pp. 219-230.

Straub, D. W. (1990). “Effective IS Security: An Empirical Study,” *Information System Research*, Vol. 1, No. 2, pp. 255- 277.

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

Tarr, C. J. and Kinsman, P. (1996). “The Validity of Security Risk Assessment,” *Proceedings of 30th Annual International Carnahan Conference on Security Technology*.

Thomas, R. K. and Sandhu. R. S. (1994). “Conceptual Foundations for a Model of Task-based Authorizations,” *Proceedings of the 7th IEEE Computer Security Foundations Workshop*, Franconia, NH.

Thomson, M. E. and von Solms, R. (1998). “Information Security Awareness: Educating Our Users Effectively,” *Information Management & Computer Security*, Vol. 6, No. 4, pp.167-173.

Valia, R. and Al-Salqan, Y. (1997). *Proceedings of the Sixth IEEE Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*.

Vogler, H., Kunkelmann, T., and Moschgath, M.L. (1997). “An Approach for Mobile Agent Security and Fault Tolerance Using Distributed Transactions,” *Proceedings of the 1997 International Conference on Parallel and Distributed Systems,* IEEE Computer Society Press.

Voyatzis, G. and Pitas, I. (1999). “Protecting Digital-image Copyrights: A Framework,” *IEEE Computer Graphics and Applications*, Vol. 19, No. 1, pp. 18-25.

Wack, J. P. and Carnahan, L. J. (1995). “Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls,” NIST Special Publication 800-10.

Walter, J. E. (1993). “Security in Unattended Computing Labs — Safeguarding Users As Well As Machines,” *Proceedings of the 21st Annual ACM SIGUCCS Conference on User Services*, San Diego, CA.

Woo, T. Y. C. and Lam, S. S. (1992). “Authentication for Distributed Systems,” *IEEE Computer*, January.

Wood, C., Summers, R.C., and Fernandez, E.B. (1979). “Authorization in Multilevel Database Models,” *Information Systems*, Vol. 4, No. 2, pp. 155-163.

Wood, C. C., Banks, W. W., Guarro, S. B., Garcia, A. A., Hampel, V. E., and Sartorio, H. P. (1987). *Computer Security: A Comprehensive Controls Checklist*, Hoboken, NJ: John Wiley & Sons.

Wood, C. C. (1996). “A Policy for Sending Secret Information Over Communications Networks,” *Information Management & Computer Security*, Vol. 4, No. 3.

Yeo, B. L. and Yeung, M. M. (1999). "Watermarking 3D Objects for Verification." *IEEE Computer Graphics and Applications*, Vol. 19, No. 1, pp. 36-46.

Yialelis, N., Lupu, E., and Sloman, M. (1996). "Role-Based Security for Distributed Object Systems," *Proceedings of the 5th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'96).*

Zeng, L., Wamg, H., Lee, M.K.O. (1997). "Multiple Intelligent Agent Supported Internet Security System: Issues, Current Solutions, and a Proposed Approach," *Proceedings of the 1997 IEEE International Conference on Intelligent Processing Systems (ICIPS'97).*

Zhong, Q. and Edwards, N. (1998). "Security in the Large: Is Java's Sandbox Scalable?" *Proceedings of the Seventeenth IEEE Symposium on Reliable Distributed Systems.*

Zhang, X. N. (1997). "Secure Code Distribution," *IEEE Computer*, Vol. 30, Is.6, pp. 76-79.

Zviran, M. and Haga, W. J. (1990). "User Authentication by Cognitive Passwords: An Empirical Assessment," *Proceedings of the 5th Jerusalem Conference on Information Technology, 1990. 'Next Decade in Information Technology',* IEEE Society Press.

Zviran, M. and Haga, W. J. (1993). "A Comparison of Password Techniques for Multilevel Authentication Mechanisms," *The Computer Journal*, Vol. 36, No. 3, pp. 227-237.

About the Authors

Mikko T. Siponen is Professor in the Department of Information Processing Science at the University of Oulu, Finland. He holds a Ph.D. in Information Systems, and a DSSc in applied philosophy. His research focus is on IS security and ethical aspects of IS. His research work has been published in journals such as JAIS, I&O, EJIS, CACM, IEEE IT Professional and ISJ.

Harri Oinas-Kukkonen is Professor in the Department of Information Processing Science at the University of Oulu, Finland. He has about 15 years of experience with various aspects of information systems and digital media in practice and research. His research interests lie in information systems development, including system design, hypertext functionality, electronic commerce, mobile hypermedia and collective IQ.

View publication stats