Chapter 7
Related Work

The previously relevant work accomplished in this field is discussed in this chapter. The e-business information security is reviewed and discussed. This review focuses on the work of e-business security models and more specifically on the approach suggested here are the increasing problems with perimeter security and the business process and information flow security approach.

7.1 Perimeter security

In the main context of such security which is providing the boundary to the security aspect of a business environment, there is a growing general awareness of the failings of the perimeter security approach. There has been relatively little published research on other approaches. Professional groups have called for an alternative approach, under the banner of de-parameterization. A variety of approaches have been proposed to enable de-parameterization to be achieved. Simmonds [201] explains the concept as a set of business-driven solutions within a framework that can be mixed in order to address business needs without a hardened perimeter. This approach is not a single solution, but a way of thinking [201]. Stanton [225] continues with this shift in thinking, and explains that de-parameterization is not about getting rid of boundaries, but instead involves re-aligning and refocusing them. The author suggests the ‘inside outside security’ approach, rather than a ‘one size fits all’ approach. Instead of a single hard fence around a soft centre, an organisation should protect core functions and processes with internal partitions and boundaries. This kind of approach is supported by the basic principles of security management, namely deciding on what is crucial for the business processes, and focusing on their security [225]. Services Oriented Architecture, a major current trend in information technology needs to be supported by a new security model. The model proposed by Sluiter is implemented in three phases, namely-

- Preparation
- Reorganisation
- Opening up

Also business partners in e-business information system need to implement adequate security in order to interact with each other. The difficulties in securing the modern environment are not just technology-related but outdated legal constraints preventing information sharing when it is most needed, cultural factors, poor standards compliance, ‘phishing’ attacks affecting people's trust in online transactions, together with the technological obstacles that still remain. All these issues need to be addressed, although the main focus is put on access control.

7.2 Business process security
Discussed in chapter 3 that e-business is the subject of a huge volume of ongoing research. Some of this research relates to e-business information security, and just a small part of the latter relates to the security of the business process and/or information flows. Very little research relates to the security of the business logic. Other work [140] has identified the security requirement of electronic processes. A discussion of e-business process modelling [226] offers the building blocks required for e-business automation, and notes that the fragmentation of security requirements is the biggest challenge for Web services.

The vast majority of existing research on business process security focuses on workflow control. In the last few years there has been a growing interest in research on workflow in general, and on information security in particular. Specifying a workflow system involves defining procedures in terms of tasks, the users that should perform the and the interactions between tasks that impose constraints on task execution. Hence, a workflow is a combination of tasks or logical steps in a business process, while accompanying constraints define the limitations on tasks that are performed by people. The usual approach to the protection of business processes is based on the Separation of Duty principle. Separation of Duty is designed to ensure that staffs that perform critical organisational tasks are not able to commit fraud. Certain separation of duty specifications can result in three types of anomaly, and suggest a constraint specification language to specify the inter-instance constraints i.e. an instance is generated when the workflow is executed. The workflow security model of Wainer et al. [130] makes use of Role-Based Access Control to control access to the tasks making up a workflow, while the focus of the model is on the selection of users to perform the workflow tasks. Although the model was developed for a traditional type of business, and not specifically for an e-business organisation, we mention the model here as an illustration of business process security-related research.

A suggest approach that supports Business Process Reengineering in order to improve security and integrity. This work was discussed previously in chapter 3, section 3.14.2, in the context of e-business security requirements. The authors consider security and integrity as two separate issues and propose a framework for business-process re-engineering in order to improve security and integrity. A three layered architecture for business process specification is suggested. A security infrastructure for both business processes and workflow management is developed, and the types of security requirements necessary for such an infrastructure are identified. Also, business processes and their security semantics are discussed from five different perspectives, and the effects of security constraints on the various perspectives are analysed. Leyman et al [77] focus on the relation between web services and business processes and on the elements essential for suitable standards has been suggested as a means of analysing e-business process security. Anderson et al. [24]
propose the use of model checking technology for the design and assurance of e-business processes. The term ‘assurance’ implies a measure of confidence that a security policy is enforced properly [224]. The problems in the information systems that support e-business, compounded by rapid development and system complexity in the e-business environment, have the potential to harm businesses.

To use model checking, a user needs only describe the processes and property specifications using a high-level programming language. The model checker automatically translates these processes and property specifications into automata [283]. Model checking, argue Wang et al. in [181], is an appropriate answer to the limitations of testing and simulation methods, since model checking can go through all relevant states, addressing any given property. Model checking operates on logic, rather than on individual execution paths. Using model checking involves three main tasks, namely modelling of a system, specification of system properties, and verification to check whether the system model satisfies the required properties. The authors also discuss possible scenarios in which model checking might be effective, for example testing a Web catalogue with an advanced search interface. Such a catalogue can be tested with selective search patterns, but it is clearly impossible to try all possible query combinations. In their discussion of the importance of the e-process, Wang et al. [181] also present certain industrial developments relevant to secure e-process execution. Because of the importance of secure and reliable e-processes, say the authors, an e-process market has been established, offering off-the-shelf secure e-processes. Examples include Secure Electronic Transaction for securing online credit card payments, and the Inter Trust Digital Rights Management scheme, which claims to allow companies providing digital products to securely monitor customer usage of their products.

Wang et al. [181] give specific examples of the importance of secure e-process design, such as:

- Company management should have confidence that their e-processes will not give away free luxury products, unless planned;
- A digital music producer should have assurance that its digital assets can be managed securely.

An e-business organisation must consider the correctness of its e-processes and knowledge of internal control and assurance over e-business operations is essential for all the e-business participants, and even for society at large.

7.3 Security of Information flow

This concept was more than three decades old when protection of secret data from unauthorised parties took as prime concern to regulate the flow of information. The main aim was to protect confidential data in computing environments [249]. This approach was designed to regulate the
information flows in a system in order to prevent secret data from leaking to unauthorised parties. One of the best-known models from that period is Denning’s ‘Lattice Model of Secure Information Flow’ [64]. Based on the premise that security is enforced if no unauthorised flow of information is possible, Denning suggested restrictions `according to which the security of a system would not only be decidable, but simply so’. The suggested information flow model is defined by:

- A set of logical storage objects
- A set of processes
- A set of security classes
- An associative and commutative binary class combining operator
- A flow relation

The security requirements of this model can be formulated as follows. A flow model is secure if and only if execution of a sequence of operations cannot give rise to a flow that violates a specified flow relation [64]. Because of the transitivity property of the relation flow, if each individual operation is secure then the sequence of operations is also secure.

Because of the difficulties with providing security for information flows that exist to cause operations, Denning distinguishes between explicit and implicit information flows, dealing with them in a different way; the model thus also applies constraints to service processes in order to prevent information leakage. It seems that the model is designed to be applied to situations in which information can be classified as Secret, Top secret or Unclassified, etc.

Typical business organisations possess files/records for which only specific fields can be defined as ‘secret’ while others are not, but are still included in the same information flow. As a result, using the above classification is very problematic in a real business environment. Moreover, most seriously of all, the Lattice Model only addresses information confidentiality, not integrity, and integrity is of fundamental importance for an e-business process. Some of the research related to information-flow security deals with the property of non-interference and does not specifically address the e-business environment. Other work, [214], based on the non-interference property, introduces a security property to deal with the security of dynamic processes. According to the authors, Persistent BNDC, defined by the authors as a single equivalence check, ensures that no malicious attacker will be able to attack a system, even if the environment changes during its execution.

The real challenge for information-flow security is not about giving more precise definitions of non-interference, and/or implementing languages that support information-flow policies, but a series of goals such as[249]:

- The integration of information-flow controls with the existing infrastructure;
Not enforcing techniques that prevent all secret information-flows being seen, without any differentiation;

Managing complex security policies considers being the most important issue.

McLean [120] made a very important observation regarding information flow oriented research; all such work deals with sharing of information and not with the security of the information flow itself. The main focus of existing models is the flow of information between users, characterised by different levels of access to information, and how to prevent information flow from high-level users to low-level users. Hence, in some sense, all these models are access control models. The models cover the security of the end points of communication, but not the content and context of the information flow itself.

7.4 Summary

The majority of existing security work relevant to the focus of this thesis addresses the issue of user/employee access to the critical information of an organisation. Prior work is typically concerned with developing models and methodologies that enable access policies for specific users to be defined and enforced. Existing process-oriented security research is mainly concerned with the work-flow concept and workflow management systems. In fact, a workflow is not a business process, neither by definition nor in practice. The differences between workflows and business processes are also reflected in the research orientation. Workflow security research, as well as information flow security research, is mainly language-oriented. The vast majority of information flow security related research is associated with communication or computer-level technical aspects. [4,64,207,214,215,232]).

Information flows are treated according to Shannon's theory of information, and not specifically from a business perspective. There are certain important areas in the e-business security domain that appear to have been the subject of very little research. Areas such as e-business security design methods, e-business logic security, e-business security maintenance, and e-business forensics all appear to be underserved by current e-business security research. In the main part of this thesis we present a different approach to business process-based and information flow-based security.