MODELLING E-BUSINESS SECURITY USING BUSINESS PROCESSES

S. Nachtigal
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
Email: s.nachtigal@rhul.ac.uk

C. J. Mitchell
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
Email: c.mitchell@rhul.ac.uk

Keywords: e-business, information security model, business process, information flows, perimeter security

Abstract: Organisations (enterprises, businesses, government institutions, etc.) have changed their way of doing business from a traditional approach to embrace e-business processes. This change makes the perimeter security approach inappropriate for such organisations. The well-known and widely used security mechanisms, including cryptography-based tools and techniques, cannot provide a sufficient level of security without being a part of a comprehensive organisational approach/philosophy. This approach must be different from the current dominant approach, i.e. perimeter security, and must focus on different organisational components. In this paper we suggest a process security approach, and describe ongoing research with the aim of developing an e-business security model based on this new, process security, approach.

1 INTRODUCTION

The way in which business is conducted is going through a very significant change. E-business, a new and different way of running a business, is a subject of growing importance both for the business and the academic world.

The business world has adopted information technology since the very early stages of computer history. From mainframes, through minicomputers, PCs and LANs, to WANs and EDI — all these technologies (combining hardware, software, databases and telecommunications) provide a company with the means to enhance its internal operations. Information technology has changed significantly since the introduction of computers, while these technology changes have impacted business practice to a great extent (Oz, 2000). In value chain/supply chain terms, information technology has helped to improve the efficiency of company supply chains (Poirier and Bauer, 2001); WANs and EDI were the first technologies adopted to improve external operations by providing communications with the business environment (mostly suppliers), and actually extending the supply chain.

In today's technology intensive reality, the opportunity of adding value to the firm's supply chain can be achieved by making more and more business functions 'electronic'. In technological terms, this is achieved by introducing increasing numbers of information systems and information technologies *into* enterprise business processes and *between* business processes. In other words, this is achieved by networking the business functions inside the organisation, and between the organisation and its environment. The Internet infrastructure and Internet-based technologies make it possible for organisations to perform all business connections electronically — not just with suppliers and customers, but also with financial institutions, government bodies, potential suppliers, potential customers, partners, competitors, etc. Use of Internet-based technologies implies the existence of a Web-site as a means of enabling electronic business (Poirier and Bauer, 2001).

In practice, it is possible to transform the supply chain to an electronic form either partly or completely, while operating as an e-business organisation. By doing so, the traditional supply chain becomes a supply network. More than that, by introducing advanced information technologies into the supply chain, the supply chain becomes, according to Porter's model (Porter, 1980), a value chain — i.e., a value network or electronic value network.

Given the above discussion, in this paper (and in the research it is related to) an e-business (e-biz) organisation is defined as:

a 'Business that performs its supply chain activities by means of Internet-based Information Technologies through integration, cooperation and interaction of its and others supply chain participants' webs, and by doing that actually creates a ***Portals Value Network*** (PVN).'

(It should be emphasised that the research described below distinguishes between the terms 'e-business' and 'e-commerce'. Since we have already defined the term 'e-business', the distinction should be clear: the term 'e-commerce' refers only to the activities of buying /selling products. Hence e-commerce is just a part of e-business. The subject of concern here is 'e-business').

Based on our definition, from a business point of view, e-business is the integration of processes, systems and enterprises, while from a technological point of view, e-business is the collection and integration of IT concepts and tools. E-business means that the entire enterprise becomes an e-enabled organisation. The e-biz approach to performing business transactions implies using information technologies (especially communication technology) throughout the business supply chain. In fact the electronic supply chain might be different for each organisation that practices e-business — depending on the number and type of organisations that the company has business relationships with. New threats and problems arise while using Internet technology in general, and especially when a company adopts the e-biz mode. E-biz involves performing business interactions (in other words, transmitting documents, i.e. data flow) between organisation portals by means of Internet technology.

Academic research, while interacting with the business world, contributes to mutual efforts to solve field problems. In the case of e-biz, both business and academia are challenged to provide solutions, since e-biz is relatively new, and also very beneficial for various aspects of modern life. As an integration of business and technology, e-biz faces significant difficulties and problems. This paper describes ongoing research related to probably the most significant of these problems, namely security.

2 THE MAIN PROBLEM OF E-BIZ ORGANISATIONS

The uniqueness, and the danger, in e-biz is its 'openness' to the environment, and the various connections and communication channels with the external world. As a result of that 'openness', an enterprise that practices e-biz is exposed to a wide range of threats, i.e. factors that expose the enterprise to a danger of suffering from loss, both tangible (e.g. monetary loss) and non-tangible (e.g. reputation).

An e-biz process is subject to all the benefits and disadvantages that the technologies imply. The vast majority of the technology-related disadvantages are information security related — while performing a process by means of IT, threats such as sensitive (business and private) information disclosure and theft, industrial espionage, electronic fraud, business failures due to technological (hardware, software or communication) failures, viruses, spyware, adware, phishing, DDoS, impersonation should be considered. The harm to an enterprise may come from different sources and by different means— the attacks could include technology-based tools and methods as well as social engineering methods.

As IT becomes more and more user-friendly, it also becomes much more accessible by a wider population. The potential sources of security threat sources are becoming more technology-literate and sophisticated. Although the threats are growing, countermeasures are being constantly improved, and new techniques are being applied to secure corporate business information; currently, security countermeasures include hardware and software-based tools and also powerful cryptographic mechanisms. So, there are increases both in the technological sophistication of the attackers and in protection methods and power.

However, attackers continue to look for alternative methods of accessing corporate information. This has given rise to different kind of threats, based on social engineering methods, that in the vast majority of cases have nothing to do with information technology abuse.

Corporate information systems security has been dominated by 'traditional' security considerations for many years. According to the traditional information security model, security is achieved by providing a security perimeter, designed to protect the company's boundaries from the external world (Kis, 2002). The vast majority of existing business information systems have been, and are still being, designed and built according to the perimeter security paradigm. The goal is to prevent malicious/non-authorised users and applications from accessing the company and its various business functions. A wide variety of tools and mechanisms have been (and are still being) developed to support corporate security based on this perimeter security approach.

In this approach, information systems security is provided on the basis of a trust hierarchy, by which the internal users (i.e. the company's employees) are automatically assigned a maximal level of trust, while everyone trying to enter the business from the external world is assigned a minimal level of trust, if at all. This approach has a number of shortcomings, including the basic assumption that employees can be trusted (according to CSI's 2004 statistics, at least

66% of all security incidents are due to employee actions, performed either deliberately or by error (CSI, 2005)). Moreover, the concept of 'closed borders' fits LAN and/or WAN based activities, but does not fit so well to Internet-based business operations, and breaks down completely once one considers mobile and wireless access to corporate networks.

The traditional business models for information systems security are thus no longer appropriate, and fit neither the new organisational environment nor the new organisational security needs. The old approach does not distinguish between different applications with different levels of sensitivity running in the business. The different mobile devices, which are potentially widely used in e-biz activities, are at great risk and could not been given a high trust level, even if the users are trusted employees. The other problem is the absence of a standard security infrastructure in the form of end-to-end protocols: "it is too easy to steal or tamper with the devices, and the digital keys are stored at gateways rather than on the device" is a familiar refrain.

Indeed, we note certain recent developments regarding application security — some commercial security companies have made a declaration on their new products for application security, while distinguishing between different security needs based on different sensitivity levels. However, there is still no solution for the security needs resulting from business transactions performed via the Internet between the portals of different participants within the PVN community. An e-biz company must give access to its internal various business functions to the external business world, in order for e-biz to work. A comprehensive security solution for such a company must combine both internal and external information security. The task of providing security to the information systems of such a business mainly involves providing security for the information transmitted between the company and the other participants of a specific PVN that enables specific e-biz transactions.

This novel task has arisen from the very definition of an e-biz company, and means that e-biz is primarily concerned with protecting information flows. As a result, in this paper we focus purely on the information flows between a company and its PVN participants; we analyse the security requirements resulting from such flows in order to obtain an information systems security model appropriate to e-biz business needs.

3 RELATED WORK

E-business (including e-commerce) is the subject of a huge volume of ongoing research. Some of this relates to e-business information security, and just a small part (with regard to information security) relates to business process and/or information flows. McLean (McLean, 1990) has developed a flow-based security model, FM, which is used as a standard for comparing with other security models. A new approach (Sabelfeld and Myers, 2003) was recently developed for specifying and enforcing information flow policies, since, according to the authors, standard security practices are not capable of enforcing an end-to-end confidentiality policy. Other work (Knorr and Rohrig, 2001) identifies security requirements of electronic processes. A discussion of e-business process modelling (Aissi et al., 2002) offers the building blocks required for e-business automation, while addressing the fragmentation of security requirements as the biggest challenge for Web services.

There is a growing general awareness of the failings of the perimeter security approach (especially for e-business). Professional individuals and groups (such as the Jericho Forum[1]) have called for an alternative approach, while suggesting a variety of solutions. The objective of this paper is to introduce such a new approach, namely a business-processes oriented security model, to e-business enterprise security. This new approach is based on an e-biz core characteristic of performing business functions by means of electronic data and information flows.

4 THE BUSINESS PROCESS

A process, as commonly defined, is the conversion/transformation of a certain entity (tangible or non-tangible) from one form to another while undergoing a series of actions (Laudon and Laudon, 1998). A *business process* can be defined as a certain sequence of activities that transforms inputs from different suppliers into outputs to selected customers (Smith and Fingar, 2003a).

Two universal macro-level modules are present in any business organisation, namely operations and management. The operations module is the most basic; without operations (i.e. processes) there is no management, and there is actually no organisation. No organisation is able to function as a vital active unit without properly performing its processes. A process can be described by mapping all the documents carrying the data relevant to the process. An e-biz process is based on a set of information/data flows that enable its existence. In practice, the only way to perform an e-biz process is to transmit documents over electronic channels, using the specific technologies making up the infrastructure that enables business communications.

[1] www.opengroup.org/jericho/

The existence of the company is dependent (in the case of e-biz) on the functionality of these electronic channels (e.g. the functionality of the Internet-related technologies) and the information they carry, while the importance of information quality and functionality is becoming a critical factor for all e-biz companies. Major parts of documents (if not all of them) include sensitive information; in any case, in order to ensure that the functionality of the business proceeds according to plan, all the business data and information (both transmitted and stored) should be protected. This leads us to a conclusion that for an e-biz company to function properly (and to function at all) its business processes have to be secured.

Smith and Fingar (Smith and Fingar, 2003a) distinguish three different characteristics related to business processes:

- *state* — the value of calculations performed, and the amount of information collected and generated during the execution of the process;
- *capability* — the activities and relationships of communications established between the participants at any stage of the process;
- *design* — the intentional characteristics of the process, put in place during the design of the process.

Smith and Fingar (Smith and Fingar, 2003a) use these process characteristics to link *business management* and *business technology*. Dynamics is a significant characteristic of a modern business — not just the process itself, but also the relationships between the processes and even the channels of executing the processes. A business process, as defined above, in practice occurs by transforming documents between stations involved in a specific series of actions in order to complete a specific mission. Documents contain data essential to perform each one of the procedural stages of a specific process. In other words, we use documents as a convenient way of carrying data.

Focusing on business process security appears to be a rational approach that complies with the most basic definition of 'organisation' in respect of its performance on a daily basis. Without processes there is no business, so providing security to an e-biz process simply enables the existence of such a business.

5 THE SECURITY MODELLING PROCESS

Existing security tools and mechanisms, developed upon the traditional perimeter security concept, and based on hardware and software products, including cryptography, are not sufficient since they do not relate to specific parameters that characterise the *business process*. This paper presents ongoing research that introduces a novel approach to securing business information systems by focusing on business processes.

An e-biz company must give access from the external business world to its internal various business functions, because only in that way can the e-biz mode be valid. A comprehensive security solution for such a company must combine both internal and external information security. The task of providing security for the information systems of such a business is mainly concerned with providing a security solution to the information transmitted between the company and the other participants of a specific PVN that enables specific e-biz transactions. This task is a new one that has been arisen from the definition of an e-biz company, and becomes the primary focus of e-biz security. As a result, the research described here will be limited to that task only; that is the information flows between the company and its PVN participants will be analysed in order to obtain an information systems security model appropriate to e-biz business needs.

As stated above, a process is associated with documents transmitted between the different stations of that process. This is why the best way to present a process is by presenting the information involved (i.e. that produced, transmitted and stored) in the process. The business processes could be identified by describing the business functions of which the processes are a part. However, when considering an e-biz process, there are number of rather unique features of this specific kind of a business process. Even the semantics of the widely used concept of workflow cannot be used for modeling the majority of e-biz processes, because of the great degree of mobility associated with e-biz activities (Smith and Fingar, 2003a). There is a formal theory of mobile processes, namely Pi-Calculus as developed by Milner. Most, if not all, processes are associated with the mobility feature — see (Milner, 1999) and (Smith and Fingar, 2003b).

The 'mobility' concept seems to be one of the most significant properties of e-biz process; it refers to the way information is exchanged among the participants in a process, and the changes in their relationships as the process evolves during execution. In fact, in the business environment, all the processes may/should be considered as mobile processes (Smith and Fingar, 2003a).

As stated before, an e-biz organisation runs its business differently to a traditional firm. Its business processes are an integration of sequences and sets of information flows. (The concept of analysing information flows has been used by McCumber in his McCumber Cube approach (McCumber, 2005), while dealing with *mapping information flow states* and introducing the concept of 3-states information existence).

This paper introduces a different direction for in-

formation flow analysis. In order to define the e-biz functions and processes, a detailed description of the well known traditional business functions and processes is performed. Any process is viewed as being comprised of a set (potentially a very complex one) of specific information flows. All the processes of the organisation, and the relevant information flows associated with them, are described, and the results are summarised by means of an *Information by Processes Table (IbPT)*.

In order to secure a business process, not only do its information flows need to be secured, but also all the data stores that serve these information flows. In order to operate properly, e-biz relies on a vast variety of data to support the organisation's activities. Besides all the business data and information stores, there are also stores (packages) of specific computer system data, needed for system execution or produced by the system.

All the processes, together with the associated information flows, databases and the set of various business (operational and management) parameters which characterise the processes, are evaluated and the final model is formulated. The relationships between the model components will be defined following the test phase of the research.

6 USING THE SECURITY MODEL

Organisations are constantly investing in information technology, and in business information systems security in particular. These security expenditures have constantly increased over the last few years (CSI, 2005). The expenditure is mostly on widely used security tools such as firewalls, antiviruses, VPNs, encrypted channels, etc. Although the tools are effective to a certain extent, there are objective shortcomings related to all existing security tools and mechanisms:

1. they solve just the technical side of the security problem;
2. the acquisition of those tools and mechanisms is not based on any analytical model, since corporate management is not supported by any such analytical model in their decision-making.

According to the traditional perimeter security approach, security tools are used in order *to protect organisations by preventing certain types of activities* (Holden, 2003) — which potentially results in a cumbersome and non-intuitive business environment for the employees. The security 'arms race' is a never-ending process, since the threats and risks are constantly growing, and the organisation management never knows how much security is enough to prevent unauthorised access into the business. The result, again, is the imposition of limitations on employee operational capabilities (e.g. they are forced to perform certain business operations in a particular, highly complex way, at certain hours, certain workstations, etc.).

The new approach suggested here, and the model which comes with it, is designed to *to enable business instead of prevent business* by abandoning the concept of borders (which are no longer relevant for an e-biz company) and providing decision makers with security measures based on business process specifications. This is a rational and, therefore, useful tool since the most important thing for the organisation is that its business processes are performed properly. The model will make possible the planning of both the business security measures and the security management process itself.

7 TESTING THE MODEL

Because of the nature of the discipline (information systems security) and the research target, it has been decided to apply a *heuristic case study* method in this research (Myers, 1997). Four different Case Studies will be performed, for the following reasons.

Any e-biz firm has to decide upon its business model, a new and different model to that applying to a traditional type of business. E-business models can be grouped and classified into two categories (Applegate, 2002) — the classification should be made on a basis of separation between two kinds of companies:

- *Digital businesses* — firms that are built and launched on the Internet;
- *Businesses that provide the platform upon which digital businesses are managed and operated.*

Gloor (Gloor, 2000) gives a more detailed classification of the models suggested by Malone (cited in (Gloor, 2000)). Malone distinguishes between four fundamentally different types of models for e-biz:

- *Creators* — producers of goods (physical or information) such as General Electric, Cisco, Dell, Microsoft, and on-line versions of newspapers.
- *Distributors* — companies that distribute and/or supply the goods, such as electronic shops for books or music (the most representative example is Amazon).
- *Brokers* — companies that act as intermediaries, such as on-line auctioneers, travel agencies (eBay, Netaction and Olsale, Thelastminute, the90minute), are examples of this type of e-biz.
- *Extractors* — these are companies that exist only on Internet, operate as portals, and whose business model is based on advertising revenue. Typical examples are Yahoo and Google.

This classification is generic enough and, indeed, includes all kinds of organisations acting as an e-biz. Based on the discussions in previous sections, the next phase of this research with regard with development methodology will include the following:

1. The choice of four different e-biz firms, one for each of the following types of e-biz models:
   - creator;
   - distributor;
   - broker;
   - extractor.

   Each of these chosen companies will be used as a Case Study.
2. Each of the Case Studies will be analysed, covering the:
   - background;
   - full process description;
   - full information flow description;
   - relevant databases;
   - security analysis;
   - business issues (strategies, policies, etc.).
3. The data will be analysed (the structured data will be also processed) and discussed.
4. Based on the case study findings, a 'process security' model will be developed and formulated.
5. The model (models) will be implemented on the case study firms.

8 CONCLUSIONS

Although there is a wide range of technological security tools, there is still no solution for security needs resulting from the business transactions performed, via the Internet, between the portals of the participants making up the PVN community. Such a solution will potentially be very useful for organisations which practice e-business activity, as discussed above. Any e-biz organisation will be equipped with a tool (model) which will enable rational economic security investments.

Additional benefits will come in form of the information acquired during the research phases of testing the models, i.e. the data collected from the case studies. These could lead to additional possible research results. Initially, this data will be used to follow-up the case-study organisations in order to analyse the impact of the suggested model in the middle and long term.

Further, a map of business processes with the associated information flows, which will be one of the by-products of this research, could be a useful basis for analysing the actual need of various security tools and measures (in terms of types, amounts, goals, cryptographic strength, etc.), related to a specific business process rather than the whole corporation.

REFERENCES

Aissi, S., Malu, P., and Srinivasan, K. (2002). E-business process modeling: The next big step. *Computer*, 35(5):55–62.

Applegate, L. M. (2002). *E-Business Handbook*. The St. Lucie Press.

CSI (2005). *2004 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute.

Gloor, P. (2000). *Making the e-Business Transformation*. Springer-Verlag, London.

Holden, G. (2003). *Guide to Network Defense and Countermeasures*. Thomson Learning, Course Technology.

Kis, M. (2002). Information security antipatterns in software requirements engineering. Permission is granted to copy for the PLoP 2002 conference.

Knorr, K. and Rohrig, S. (2001). Security requirements of e-business processes. In Schmid, B., Stanoevska-Slabeva, K., and Tschammer, V., editors, *Towards the E-Society: First IFIP Conference on E-Commerce, E-Business, and E-Government; Zurich, Switzerland, Oct. 4-5, 2001*, pages 73–86. Kluwer Academic Publishers, Norwell, MA.

Laudon, K. C. and Laudon, J. P. (1998). *Information Systems and the Internet*. Dryden Press, 4th edition.

McCumber, J. (2005). *Assessing and Managing Security Risk in IT Systems*. Auerbach Publications.

McLean, J. (1990). Security models and information flow.

Milner, R. (1999). *Communicating and Mobile Systems*. Cambridge University Press.

Myers, M. D. (1997). Qualitative research in information systems. *MIS Quarterly*, 21(2):241–242.

Oz, E. (2000). *Management Information Systems*. Thomson Learning, Course Technology.

Poirier, C. C. and Bauer, M. J. (2001). *E-Supply Chain*. Berrett-Koehler Publishers, Inc.

Porter, M. (1980). *Competitive Strategy*. Free Press, USA.

Sabelfeld, A. and Myers, A. C. (2003). Language-based information-flow security. *IEEE Journal on Selected Areas in Communications*, 21(1):5–19.

Smith, H. and Fingar, P. (2003a). *Business Process Management: The Third Wave*. Meghen-Kiffer Press.

Smith, H. and Fingar, P. (2003b). Workflow is just a Pi process. Possibly available at www.bpm3.com/picalculus.