International Journal of Business Management and Research
Vol.1, Issue.1 (2011) 11-27

ACCOUNTABILITY AS AN OBJECTIVE FOR SECURITY REQUIREMENTS OF E-BUSINESS PROCESS

[1]S.Gopi Krishna, [2]Dr.R.Siva Ram Prasad

[1]Professor & Head, Dept. of CSE Narasaraopeta Engineering Collge, Narasaraopet, AP, India, gks24@rediffmail.com [2]Research Director, Dept. of CSE Acharya Nagarjuna Univeristy Guntur, AP, India
raminenisivaram@yahoo.co.in

ABSTRACT

This paper presents an open framework for the analysis of security requirements of business processes in electronic commerce. The most important dimensions of the framework are security objectives (confidentiality, integrity, availability, and accountability), the phases of and the places/parties involved in the process. The approach is of open nature so that it can be adapted to the heterogeneous needs of different application scenarios. The discussion of business processes illustrates the capacity and potential of the framework.

General Terms : Security, E-Business

Keywords: E-Commerce, Security, Algorithms, Accountability.

1. INTRODUCTION & LITERATURE SURVEY

Over the last years enterprises and individuals have started to conduct business over computer networks, especially the Internet. This development is commonly summarized as electronic business (e-business). Zwass [1] defines e-business as business connections, which make use of electronic media. One of the major characteristics is that partners do not necessarily have to know each other prior to their business interaction [2].

Despite its wide use and opportunities, e-business has not grown to its full potential – one of its most important obstacles being the lack of adequate security measures as well as difficulties to specify adequate security requirements. An abundance of research about security in e-business can be found in literature.

The framework for security requirements of e-business processes (EBPs) proposed in this article. The dimensions are the security objectives and the places of an e-business transaction. This article adds other dimensions, viz., the phase of an EBP.

Wang and Wulf [3] propose a general framework for security measurement in computer systems. Compared to our framework, they neglect the process dimension.

Herrmann and Pernul [4] [5] argue that security requirements vary with the perspective taken. They identify different perspectives (informational, functional, dynamic, and organizational) which are closely related to the different elements of a workflow specification. In comparison with our approach, the authors focus on legal issues such as intellectual property, legal bindings, and privacy.

This article introduces a framework to structure security requirements of an EBP. Since information security is a very broad topic, we concentrate on security objectives, which have a precise definition and meaning. Security is often associated only with confidentiality of data, especially by non-security experts. Our framework takes into account all relevant security objectives such as the availability of data and systems, which is very important because of the distributed nature of e-business.

Since there is a high diversity concerning structure and nature of EBPs, we work on a high level of abstraction and identify four phases, which all EBPs have in common. The division used in this article originated with Schmid [6]. A further discussion will follow in Section 2.3. We will show that security

requirements of EBPs are dependent of three different factors, also referred to as dimensions:

– security objectives,

– place and party of the EBP and

– the different phases of the process

2. DIMENSIONS OF FRAMEWORK

Figure 1 illustrates the idea of dimensions for the analysis of security requirements; additional dimensions will be identified and contrasted later on. The framework allows for a structured analysis of security in EBPs since a matrix can be used to illustrate the different dimensions. Security measures can be arranged in this matrix according to the security requirements. The remainder of this paper has the following structure: Section 2 discusses the dimensions of our framework. Section 3 applies the framework to a sample business scenario of a virtual shopping mall. A discussion of the results, open questions and related work follows in Section 4, before future research areas conclude this paper.

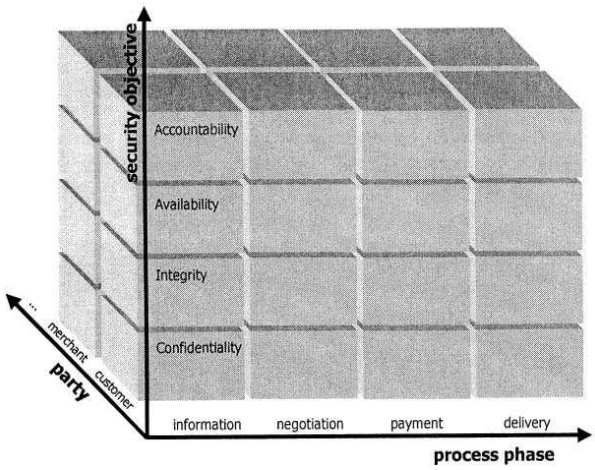

Fig.1 Dimensions of the framework Organized in a matrix

Our framework analyzes security using several dimensions such as security objectives, parties/places and phases of the EBP under consideration. Each of these dimensions consists of so-called *elements,* e.g. the dimension *phase comprises* four elements, and one of these elements is the *negotiation phase.* The purpose of this section is to describe the major dimensions of our framework and identify the elements relevant for every dimension. Please note that the framework is designed to be open, i.e. it can be adjusted through adding or removing dimensions and/or elements. In our opinion the dimensions discussed in Sections 2.1, 2.2 and 2.3 are the most important and influential ones in an e-business setting. Section 2.4 discusses further dimensions, which could be used to extend our framework

2.1 Security Objectives

The term *security objective* defined in [7] as "a processing or communication service that is provided by a system to give a specific kind of protection to system resources" or — with more emphasis on communication In [8] — as "a service, provided by a layer of communicating open systems, which ensures adequate security of the system or of data transfer". Therefore, security objectives are the goals that are to be achieved, while security services are means to achieve these goals. Traditionally, when talking about data security, three security objectives are addressed: confidentiality, integrity, and availability [4]. To better suit the needs of e-business with all its legal aspects, more security objectives have been identified recently, the most important one being **accountability**.

Confidentiality describes the state in which data is protected from unauthorized disclosure, e.g. a loss of confidentiality occurs when the content of a communication or a file is disclosed.

Integrity means that the data has not been altered or destroyed, which can be done accidentally (e.g. transmission errors) or with malicious intent (e.g. sabotage).

Availability refers to the fact that authorized persons can access data and systems within an appropriate period of time. Reasons for loss of availability may be attacks or instabilities of the system.

Accountability: If the accountability of a system is guaranteed, the participants of a communication activity can be sure that their communication partner is the one he or she claims to be. Thus, the communication partners can be held accountable for their actions.

Note that the four objectives are of different nature. While confidentiality and integrity are mainly about data, availability is primarily associated with computer systems and secondarily with the data of the system. Accountability is used in connection with subjects and data.

The lack of accountability makes the Internet vulnerable to numerous attacks, including prefix hijacking, route forgery, source address spoofing, and DoS flooding attacks.

Besides the four objectives stated above, others have been identified – like **unobservability** and **authenticity**. Nonetheless, our selection is not a random one, since all security objectives can be described in terms of the classical three. Unobservability, e.g., can be regarded as confidentiality concerning the circumstances of a communication, whereas accountability may be expressed as integrity of data defining the sender or recipient of a communication. Because of its high importance for e-business, accountability was included in our list of security objective. A reason to restrict the framework to four objectives was to keep its granularity on a manageable level. In this paper, we define *security mechanisms* (or *security measures*) as software, hardware, organizational procedures, protocols, or algorithms, which are used to increase the level of one or more security objectives. Digital signatures, for example, are used for accountability and integrity, whereas a backup server room is a measure to increase availability. *Security requirements* of an EBP express the importance of the different security objectives, e.g. the need for

confidentiality may be high in one setting while availability will be rated high in another.

2.2 Places/Parties

Electronic commerce (e-commerce) is a subset of electronic business (e-business). While e-business focuses on the support of business between two or more partners through information technology (IT) with the overall objective to increase the efficiency of the underlying business processes, e-commerce is only about trade relationships using IT support [9]. Concerning the parties involved, Gaugler [10] differentiates four categories of e-business:

- Business-to-Business (B2B),
- Business-to-Consumer (B2C),
- Business-to-Public (B2P),
- Public-to-Consumer (P2C).

Under certain circumstances, more than two parties can be involved in an e-business setting. Examples of parties not mentioned above are:

Certification Authorities for the establishment and maintenance of public key infrastructures needed for digital signatures

Trusted Third Parties (such as notary services, lawyers or courts) in case of legal disputes between the trading partners.

Banks or **credit card companies** if special electronic payment systems (e.g. electronic cash or SET [11]) are implemented.

Each of the parties involved in e-commerce may have a different conception of security in an e-business Process (EBP). In the extreme these requirements may even contradict each other. Example: On the one hand a customer of an online trader wants his personal data such as address, shopping preferences, and credit card number to be kept confidential and deleted after the transaction is completely settled. On the other hand the online trader might be

tempted to use these data for marketing purposes or even sell the personal data of its customers to a web marketing company to increase his revenue.

The above considerations clearly show the need to include the dimension *parties* in our security framework. In a sample scenario that will follow in Section 3 we will restrict ourselves to a B2C example with two parties: customer and merchant.

2.3 Phases of an EBP

Next to security objectives and parties we will include different phases of an EBP in our framework. It is intuitively clear that the security aspects change during the execution of an EBP. E.g. the integrity of prices for products on a web page is important in an early stage, while accountability is an integral component of payment.

Since EBPs are heterogeneous, we have to find a process model that is suitable for most processes in e-business. To be manageable, this model will be on a high level of abstraction. Such a general model has been introduced by Schmid [8] who identifies three phases:

1. During the **information phase** the parties try to find partners, compare them, clarify their trade relation, and specify the products to be exchanged. These actions are not legally binding.
2. In the **contracting phase** the parties decide on their partners according to their decision criteria and work out and sign a contract about their trade relation.
3. Finally, in the **delivery phase** payment and delivery is done and eventually a new transaction is prepared.

The three phases are supposed to be executed in chronological order. Unfortunately, the delivery phase proves to be too coarse for the analysis of security requirements, since the delivery phase combines payment and delivery,

which clearly have different security requirements. Therefore, we extend the model of Schmid to the following four phases:

– information

– contracting

– payment

– delivery

Please note that the chronological order of the last two phases depends on the type of EBP. Next to a sequential order – such as prepaid payment systems using coupons or electronic cash and pay-after systems using credit cards – a parallel execution is possible, which is also know as pay-now systems. As mentioned above and as will be shown in the sample scenario in Section 3, security requirements and mechanisms vary according to the phases.

Figure 2 gives an (incomplete) overview of security mechanisms that may be used in the four different phases. Since typically in an EBP the information and telecommunication systems on the company's side are more complex and numerous, research has focused on this area. Damm *et al.* [12] give an overview

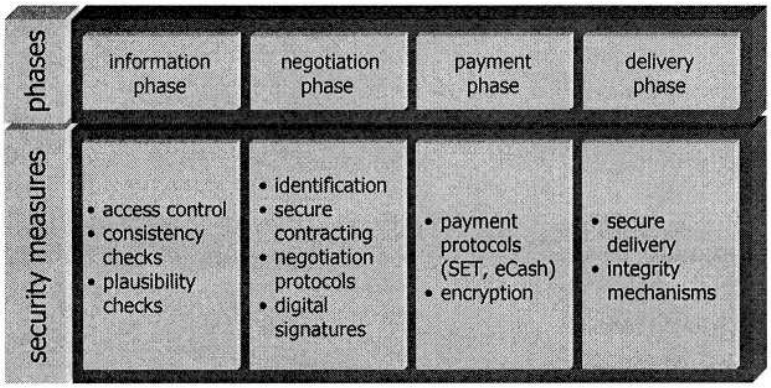

Figure 2: Security mechanisms and measures in the different phases of an EBP

2.4 Additional Dimensions

Next to the dimensions discussed above, there are other ones, which have an effect on security in an EBP. Manchala [13] identifies the **monetary height** of the transaction and the **shopping history** of the consumer as factors relevant for trust in e-commerce. Clearly, these factors are possible dimensions for our framework, too. A company might activate additional security mechanisms for a customer if this customer has had problems with paying goods in the past or if the customer orders goods of an exceptionally high value. Alternatively, if the shopping history of a customer has shown his trustworthiness the security mechanisms may be lowered.

Also, customers might be concerned about paying a company if there are rumors about bankruptcy. Additionally, the different **sites** of an EBP can be used as another dimension. The following three sites are typical for a simple EBP because of its distributed nature:

– merchant's site,

– customer's site, and

– transmission way (the Internet).

This distinction has been used and analyzed in [14] and [15]. The security requirements on the transmission way may vary, e.g. the delivery of an electronic document is less demanding concerning the availability of the Internet than the broadcast/streaming of a movie or concert. Nevertheless, a customer or merchant will typically not have the means to change the structure of security mechanisms outside their domains – especially since many other parties such as network providers, telecommunication companies, hardware and software companies, etc. may be involved in between.

The **physical location** (such as address and country) of customer and merchant might be of interest, too. On the one hand an Internet user might have objections ordering goods from specific countries. On the other hand, an online

dealer might not be allowed to deliver goods to certain countries because of trade regulations.

The **type of process** has great impact on security requirements. The process of filling out an online questionnaire to obtain a free homepage raises less security questions than an online banking transaction such as a money transfer or the purchase of shares. Our framework is capable of structuring such differences.

Clearly, the **type of product** changes the security requirements. As we will show in the sample process, a book and online-video require different security mechanisms during the delivery phase.

To be precise, another dimension – the **data ownership** dimension – should be included in our framework. When talking about security objectives (e.g. confidentiality) at a specific party (e.g. merchant) it is not a priori clear whose data are under consideration. It could be the merchant's as well as the customer's data.

Nevertheless, usually the customer will give sensitive information such as credit card number and address to the merchant. In the remainder of this paper – especially in the sample scenario – we will restrict ourselves to the discussion of the three major dimensions *security objective*, *party*, and *phase* in order to keep the granularity of the framework on a manageable level. Other dimensions, which have been topic of this section, will be mentioned but not discussed in depth.

3. SAMPLE SCENARIO

This section shows how to apply our framework to a sample scenario. Röhrig, Knorr, and Noser [5] analyzed the security of M3L: the Mall of the Multimedia Labs (MML) at the Department of Information Technology, University of Zurich. M3L offers products and services of the department such as online courses, research papers, PhD theses, "musical objects", and services in the area

of automatic, additive fabrication (stereolithography). Müller [17] gives a detailed technical description of M3L.

In what follows the security requirements within shopping processes in the M3L will be analyzed. We concentrate on two parties (customer, merchant). The evaluation will include three values: *low*, *medium*, and *high.* Here, *low* means that the party concerned has no particular interest in this security objective; *medium* denotes that the party wants this security objective to be protected, while *high* indicates that this security objective is considered essential.

In the information phase a customer browses the content of M3L. Since the products offered are not customizable and the terms of business are pre-defined, the negotiation phase consists of putting the desired goods into the virtual "shopping cart" and ordering them by clicking the respective buttons of M3L's user interface. During the payment phase either credit card transactions or the SET (Secure Electronic Transactions, cf. [7]) payment system may be used. The delivery of goods can be done online, because most of M3L's products (e.g. music or online courses) are digital and can be sent over the Internet.

The security requirements for both parties of the business process (customer and merchant) during the four phases will be explored in the next paragraphs.

During the **information phase** the customer wants to find out whether the goods offered by M3L meet his demands and to compare them with the products of other shops. The data under consideration for the confidentiality and integrity therefore is the information contained in the M3L web pages. The customer will have low demands concerning the confidentiality of this data. Nonetheless, the data he collects is the basis for his decision to buy certain goods. Therefore, he wants them to be correct, i.e. of certain integrity. If he

cannot access the web site of M3L, he will visit other merchants; the availability of the M3L server is quite unimportant to him.

In case the customer wants to make use of the merchant's offer, he expects that the terms presented on the web site are the ones that apply when he purchases the goods; accountability is therefore important for him.

The merchant, however, wants to present his offers to potential customers in a correct and easy-to-use manner. If the chance arises to find out more about the prospective buyers, he will do so. This might contradict the customer's aim to reveal as few personal data as possible. To allow for the customer to access a correct image of the merchant's offer, integrity is an important aim of the merchant. The same applies for the availability the M3L service, since the customer could easily use the offers of a competitor. Of course, this problem applies much more to Internet shops selling consumer goods (like books) that are also offered by competitors.

The security requirements of customer and merchant during the information phase are summarized in Table 1.

	Confidentiality	**Integrity**	**Availability**	**Accountability**
Customer	Low	High	Low	High
Merchant	Low	Medium	High	Medium

Table 1: Security requirements during the information phase

During the **negotiation phase,** a contract between the parties is made. This means, that the customer will have to reveal more personal information, which will make him more sensitive about confidentiality. Furthermore integrity and accountability of data concerning the contract are important for him, because it is his basis for agreeing to this contract. The availability of the M3L

server, however, will be of low importance for him, since he still has the opportunity to change his supplier.

For the merchant the confidentiality of the customer's data will be only as important as demanded by legal regulations (e.g. privacy laws). Integrity and accountability for him are at least as important as for his customer. Because he is aware that the customer can still change to a competitor's offer, the availability of his systems is a major concern. The security requirements of both parties during the negotiation phase are shown in Table 2.

	Confidentiality	**Integrity**	**Availability**	**Accountability**
Customer	high	high	low	High
Merchant	Medium	high	high	High

Table 2: Security requirements during the negotiation phase

During the **payment phase** the data necessary to pay the goods are transmitted to the merchant. If credit card payment is used, this means that the credit card number of the customer is sent over the Internet. For this reason the customer will have high requirements concerning the confidentiality of his data, whereas the integrity of the data is less relevant for him; in the worst case he would be obliged to send the data a second time. The same applies for availability; if a customer cannot send his payment information, it is only a nuisance since he will have to try another time. Accountability is ranked *high* as the customer wants to be able to prove that he has paid the goods he ordered.

For the merchant it is more important that the credit card number is transmitted in a correct than in a secret manner. Confidentiality will therefore be only his aim as it is used to gain this customer's trust, whereas the integrity will be of high importance for him. This is also the case for availability. If a customer cannot send his payment information, this means that the merchant will be paid to a later time, which results in loss of interest, or in the worst case

that the customer wants to break off the whole deal. Moreover, accountability during the payment phase is extremely important for him, since this helps him to prove that a payment was issued or not.

For both customer and merchant the security requirements during the payment phase are presented in Table 3.

	Confidentiality	**Integrity**	**Availability**	**Accountability**
Customer	high	medium	medium	High
Merchant	medium	high	high	High

Table 3: Security requirements during the payment phase

During the **delivery phase** the security requirements vary as to the kind of product that is delivered. In the M3L scenario these goods are either stream data (music or video) or files (research papers or PhD theses). In both cases the customer's requirements on confidentiality will be medium or low, since the data transmitted has already been published and does not reveal personal information. Of course, if somebody tracks the customer's online orders over a longer time, he gets a fairly good idea of the consumer's preferences. The customer's demands on integrity and availability will be quite high, since he wants to get exactly and without delay the product he ordered and paid for. The accountability will not be of high concern for him, because he is less interested in the originator of the good than the good itself.

During the delivery phase the merchant will have high demands on confidentiality.Since he earns money by selling the product, it is important for him that only the buyer can read it. For him the integrity of the data will be only as important as necessary for not annoying his customer. If the goods he is about to deliver consist of streaming data, the availability of the network and IT infrastructure will be very important for the merchant, since a failure might effect his future sales. In case research information is transmitted, availability is less important than in case of streaming video. As to accountability, it is

important for the merchant, that the customer cannot deny that he received the goods. A summary of security requirements during the delivery phase is shown in Table 4.

	Confidentiality	**Integrity**	**Availability**	**Accountability**
Customer	Medium	high	high	Medium
Merchant	High	medium	High(video) medium (paper)	High

Table 4: Security requirements during the delivery phase

4. CONCLUSIONS

This paper introduced an open framework for security of EBPs and applied this framework to a sample scenario. *Security objectives*, *parties*, and *phases* have been identified as the most important dimensions of the framework. Additionally, other dimensions have been discussed such as the shopping history and physical location of merchant and customer, type and the monetary height of the product. Our framework is of open nature, i.e. dimensions and/or elements of dimensions can be added or removed according to the characteristics of the EBP under consideration. Furthermore, the framework can be used as a basis for a quantification of security [3] [5] and risk analysis in EBPs. We stressed the open nature of our framework by giving a list of potential additional dimensions in Section 2.4. The focus of this paper has been on e-commerce environments. Other noncommercial areas have specific security requirements, which could be analyzed with our framework:

One important area of public life is administration and government. The use of information technology and the streamlining of processes in this setting have become known as electronic government. We plan to apply the

framework to processes in this area and hope to find and characterize differences to EBPs.

Another security-sensitive area is health care where process automation plays an important role in cost reduction [14]. Security is of paramount importance in this environment since – in the worst case – human life may be threatened if appropriate security mechanisms are not in place. Therefore, we think that the analysis of security requirements in health care processes is an important future research direction.

5. REFERENCES

1. Zwass, Vladimir. *Electronic Commerce: Structures and Issues.* International Journal of Electronic Commerce, 1(1):3-23, 1996.
2. Nabil, Adam R.; Yesha, Yelena (Eds.). *Electronicc ommerce: Current Research Issuesand Applications.* LNCS 1028, Springer, Heidelberg, 1996.
3. Wang, Chenxi; Wulf, William. *Towards a Framework for Security Measurement.* In:Proceedings of the 9th annual IFIP WG 11.3 Working Conference on Database Security, pp. 3-7, Lake Tahoe, CA, August 1995.
4. Herrmann, Gaby; Pernul, Günter. , *Viewing Security from Different Perspectives.* In:Proceedings of the 11th International Bled Electronic Commerce Conference, Slovenia,1998, pp. 89-103.
5. Herrmann, Gaby; Pernul, Günter. *Zur Bedeutung von Sicherheit in interorganisationellen Workflows.* WIRTSCHAFTSINFORMATIK, 39 (1997) 3: 217-224.
6. Schmid, B.: ,,*Elektronische Märkte.* Wirtschaftsinformatik 35(1993)5: 465-480.
7. Shirey, R.: *Internet Security Glossary.* Request for Comments 2828, May 2000.

8. ISO/IEC 7498-2. *Information Processing Systems – Open System Interconnection – Basic Reference Model – Part 2: Security Architecture.* 1989.

9. Bauknecht, Kurt. *Electronic Business — Potentiale, Rahmenbedingungen & Anwendungsfelder*. Unterlagen zum Fortbildungsseminar in Informatik, Institut für Informatik der Universität Zürich, 22.-23. September 1999.

10. Gaugler, Thomas. *Interorganisatorische Informationssysteme (IOS): Ein Gestaltungsrahmen für das informationsmanagement.* Dissertation, Institut für Informatik, Universität Zürich, 2000.

11. SET Secure Electronic Transaction Specification. Book 1: Business Description, Version 1.0, http://www.setco.org, 1997.

12. Damm, D.; Kirsch, P.; Schlienger, T.; Teufel, S.; Weidner, H.; Zurfluh, U. *Rapid Secure Development — Ein Verfahren zur Definition eines Internet-Sicherheitsknozeptes.* Institutsbericht Nr. 99.01, Institut für Informatik der Universität Zürich, Februar 1999.

13. Manchala, Daniel W. *E-Commerce Trust Metrics and Models.* IEEE Internet Computing,March/April 2000, pp. 36-44.

14. Knorr, Konstantin; Röhrig, Susanne. *Security of Electronic Business Applications –Structure and Quantification.* In: Proceedings of the 1st International Conference on Electronic Commerce and Web Technologies EC-Web 2000, Greenwich, UK, Sep. 2000, pp. 25-37.

15. Röhrig, Susanne; Knorr, Konstantin. *Towards a Secure Web-Based Healthcare Application.* In: Proceedings of the 8th European Conference on Information Systems, Vienna, July 2000, Vol. 2, pp 1323-1330.