A framework for electronic commerce security

L. LABUSCHAGNE
Department of Computer Science
Rand Afrikaans University
PO Box 524, AUCKLAND PARK 2006, South Africa
E-mail: LL@na.rau.ac.za
Tel: +27 (0)11 489-3335
Fax: +27 (0)11 489-2138

Key words: "Electronic commerce", "information security", "Internet security", "risk", "risk analysis", “information security services”, “decision table”, “security architecture”.

Abstract: This paper suggests a framework that can be used to identify the security requirements for a specific electronic commerce environment. The first step is to list all the security requirements for an electronic commerce environment in general. Next, all participants need to be identified. This is followed by the breaking down of the transactions into different autonomous actions. These actions are then mapped onto the participants involved, which serve as a model for the electronic commerce environment. This information is then used to identify the security requirements for a secure electronic commerce environment. The security requirements, in turn, are then used to develop the security architecture, consisting of appropriate security procedures and mechanisms and policy.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

1. INTRODUCTION

It is clear from many electronic commerce surveys that information security is the number one concern for both merchants and clients [ERNS99]. Despite this, electronic commerce is growing by leaps and bounds and every day sees the emergence of more and more virtual organisations. Current literature suggests a five-stage approach to establishing an electronic commerce environment, made up of the following [ERNS98]:

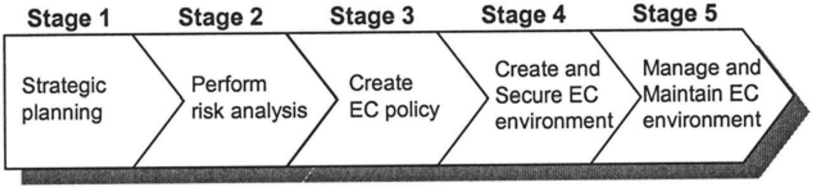

Figure 1. Stages in electronic commerce

This paper focuses on the second stage of this approach, namely risk analysis, and suggests a framework that can be applied to an electronic commerce environment to deliver an ideally suited set of security requirements. The following is a brief discussion on the different approaches to risk analysis.

2. CURRENT RISK ANALYSIS PRACTICES

There are two different ways to approach risk analysis in an electronic commerce environment. The first is through the use of conventional risk analysis methodologies, such as CRAMM [CENT96] or Marion2000 [BUCS98], that are currently used in Europe and South Africa. The second is through the use of an international security standard and the measurement of how well the environment compares to it. Following, a brief discussion on both.

2.1 Conventional risk analysis methodologies

Most conventional risk analysis methodologies are based on three security requirements, namely, confidentiality, integrity and availability. This has been established as an accepted approach for many years. This approach works well and has enjoyed the support of many security professionals. With the advent of open, distributed networks, some additional security requirements were identified. These new security requirements were grouped together in what became known as security standards.

2.2 Security standards

One of the better-known international security standards is ISO 7498-4, otherwise known as *"Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model"* [IBM95]. This standard is based on five security requirements, namely identification and authentication, authorisation, confidentiality, integrity and non-repudiation. These five security requirements are widely accepted as a baseline security standard. This might, however, not be enough when it comes to electronic commerce using the Internet. Other standards available are, for example, the BS7799 (British Standard) and Generally Accepted Principles and Practices for Securing Information Technology Systems (NIST).

Following, a brief discussion on the proposed framework for electronic commerce security requirements.

3. ELECTRONIC COMMERCE SECURITY REQUIREMENTS

With the advent of the Internet and especially electronic commerce, additional security requirements have, once again, been identified. These security requirements are a combination of both conventional risk analysis and security standards with some additional requirements. The electronic commerce security requirements are listed below:

Identification and authentication - The ability to uniquely identify a person or entity and to prove such identity

Authorisation - The ability to control the actions of a person or entity based on its identity

Confidentiality - The ability to prevent unauthorised parties from interpreting or understanding data

Integrity - The ability to assure that data has not been modified accidentally or by any unauthorised parties

Non-repudiation - The ability to prevent the denial of actions by a person or entity

Availability - The ability to provide an uninterrupted service

Privacy - The ability to prevent the unlawful or unethical use of information or data

Auditability - The ability to keep an accurate record of all transactions for reconciliation purposes

This list is by no means comprehensive and can be extended to include other security requirements more specific to an industry. Furthermore, other security requirements, like proper information security policies and procedures, can also be added. The following figure shows the origin of the security requirements and how they fit together to form the electronic commerce security requirements:

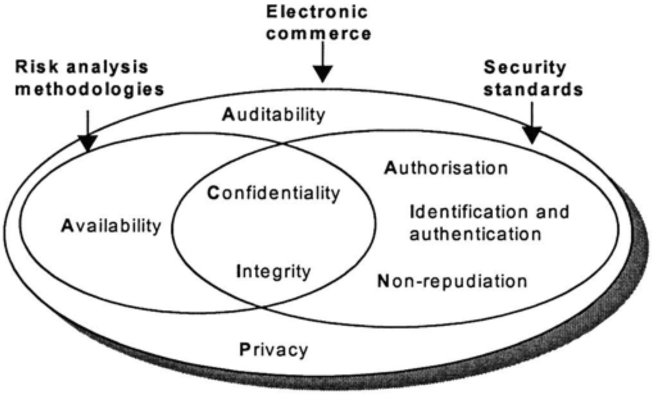

Figure 2. Security requirements for electronic commerce environment

Using these eight security requirements as the basis for the proposed electronic commerce security framework, the following section explains where these security requirements fit into a typical electronic commerce environment.

4. ELECTRONIC COMMERCE ENVIRONMENT

This paper simplifies the electronic transaction process that forms the centre of electronic commerce so as to illustrate the proposed security requirements framework. Following is a diagram illustrating an electronic commerce environment where a client wishes to buy a product from a merchant [MACG96]:

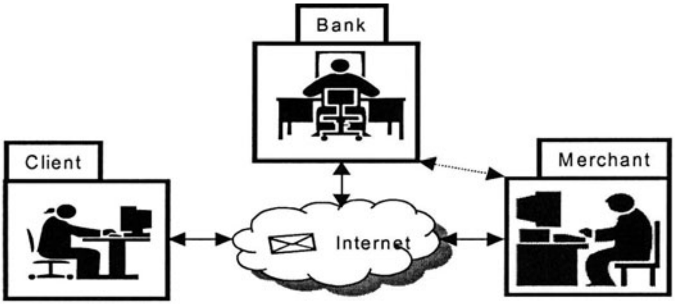

Figure 3. Electronic commerce environment

In figure 3, there are three participants to any electronic transaction, namely the client, the merchant and the bank. All transactions take place via the Internet between these three participants. For the sake of simplicity, issues such as taxation and legislation across geographical borders do not form part of this discussion, although they are very important.

Four spheres can be identified from figure 3, each with its own unique security requirements based on the electronic commerce requirements discussed in section 3. In the context of this article, a sphere is defined as an independent entity consisting of a person, information technology, or both. The spheres are indicated below:

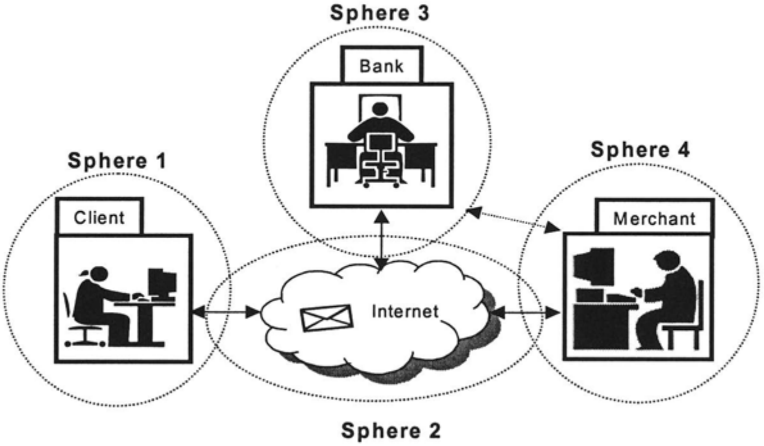

Figure 4. Spheres within electronic commerce environment

Following, a brief description of each sphere:

A. Sphere 1 – Client

The client can be any user on the Internet. It is therefore difficult, even impossible, to determine or assume that a client has any security mechanisms in place. The only assumption that can be made is that the majority of users use browsers that support digital certificates and SSL, although this does not mean that the users know of, or understand how to use this built-in functionality.

The nature of electronic commerce is such that the majority of Internet users should be viewed as potential clients and should therefore not be prevented or hindered in any way from partaking in an electronic transaction. The main benefit of electronic commerce is that it provides the opportunity to trade in a global market place.

B. Sphere 2 – Internet

The Internet is viewed as a network of networks without any single entity taking responsibility for any security on it or accountability for any losses suffered. It is seen as the infrastructure that facilitates global communication and, therefore, electronic commerce. The Internet, from its humble beginnings, does not exist to protect any of the participants, but rather to enable or facilitate the connection between different participants.

Although IPv6 was implemented successfully in many test environments, IPv4 is currently the predominant Internet protocol. Unfortunately IPv4 does not have any of the security functionality contained within IPv6 [LABU00]. For this reason, the security of a message cannot be assumed.

C. Sphere 3 – Bank

For the sake of simplicity, this framework assumes inter-banking transactions to be the norm, i.e. different banks do business with one another. This sphere regards the inter-network of banks as a unit, rather than each bank as a separate entity. The banking sphere includes other financial organisations such as credit card and digital cash or e-cash companies.

The purpose of the banking sphere is, firstly, to validate and authorise transactions and, secondly, to honour them. The principle involved is similar to what is used by SET *(See [SET00] for a detailed explanation of the SET protocol).*

D. Sphere 4 – Merchant

The merchant wants to sell products or services to the client and therefore accepts the responsibility for securing the transaction so that all participants are prepared to partake in the transaction. The merchant must, therefore, provide assurance that an electronic transaction can be made safely and securely and that risk has been minimised to an acceptable level for all participants.

For the sake of simplicity, the electronic business environment, which includes knowledge management and workflow, is not included in the proposed framework, although it would be possible to apply the framework to this environment.

At this point, the participants and the relationship between them have been described. The next step is to analyse and break down the transaction into smaller, autonomous actions that together form a complete electronic transaction [BADE94]. A typical electronic transaction consists of the following actions as shown in figure 5 below:

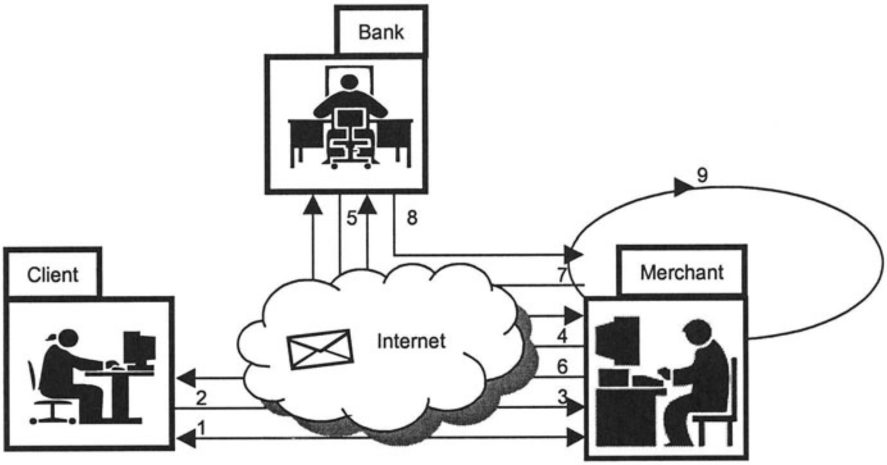

Figure 5. Autonomous actions contained within electronic transaction

A client uses the Internet to find and connect to a merchants' website (action 1). The client browses the website and decides on a purchase. An electronic transaction is initiated by the client by providing both order and payment information (action 2). Order and payment details are sent to the merchant using the Internet as communication medium (action 3).

Upon receiving the order and payment information, the merchant establishes a connection with the bank to verify the payment details (action 4). The bank checks the executability of the transaction and a reply is returned to the merchant (action 5). If the transaction is executable, that is the client has sufficient funds available, the merchant returns acknowledgement to the client before honouring the transaction (action 6). Upon completion of the transaction, payment instruction is sent to the bank (action 7). The bank honours the payment and returns proof of having done so (action 8)

The merchant uses transaction information to establish trends and do budgeting and business planning (action 9). This transaction can be broken down into more detailed actions if required. For the sake of simplicity, this article refrains from doing so.

A decision table can then be used to assist in the identification of the necessary security requirements for the electronic commerce environment discussed above [PRES97]. Following is an example of what such a decision table would look like based on the above scenario and a brief discussion on the steps to develop such a decision table:

Table 1. Decision table

		Step 3 Actions									
	Spheres	**A1**	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**	**A8**	**A9**	
Step 2	Client	X	X				X				**Step 4** **Mapping**
	Internet	X	X	X							
	Merchant	X			X	X	X	X	X	X	
	Bank				X	X		X	X		
	Security requirements										
Step 1	Identification and authentication	X	X		X			X			**Step 5** **Security framework**
	Authorisation					X		X			
	Confidentiality		X	X	X		X	X	X		
	Integrity		X	X	X		X	X	X		
	Non-repudiation		X		X		X	X	X		
	Availability				X						
	Privacy	X								X	
	Auditability					X	X	X	X		

Step 1 consists of listing all the security requirements that must be satisfied as discussed in section 2.3. *Step 2* consists of listing the spheres that have been identified. Only the four spheres shown in figure 3 are used. *Step 3* consists of listing the actions that make up a transaction. The seven actions identified are used in the decision table. *Step 4* maps the actions onto the spheres identified in *step 2*. Not all actions will include all the spheres. *Step 5* identifies the security requirements for a specific action. This information is then used to determine how it can be implemented within the relevant sphere.

In table 1, action 1 shows that the merchant must be able to identify and authenticate a client sufficiently to conduct a transaction. This does not mean that the client must sacrifice all anonymity, but rather that the merchant works with a user profile. At the same time, the client wants privacy regarding the products being viewed. Privacy in this context refers to this information not being made available to other merchants. Action 3 requires the content of the message travelling across the Internet to remain confidential and unchanged. Action 6 requires the merchant to send an acknowledgement of the order and to ensure the confidentiality and integrity of this message. At the same time, the client wants assurance that the merchant cannot later deny the confirmation. It can also be seen in the table that the merchant needs to record the transaction properly for audit purposes.

By looking at the security requirements of each action, it is possible to identify the security mechanisms required to secure the electronic commerce environment. For action 1, the *identification and authentication* security requirement could mean that users have to register before being able to purchase products (repetitive high-value transactions) or that the nature of the transaction does not necessitate anything more than a user-supplied name (single low-value transaction). The client also needs to be informed of the merchants' policy regarding privacy, including what is being recorded and for what purpose.

The security requirements for action 3 might suggest that SSL be used for securing the communication session (single low-value transaction). This would not require the client to do anything as most browsers support SSL automatically. The merchant must, however, have SSL installed on the web server. Based on the nature of the product, (where a product may be very expensive, for example) the merchant may decide that the client should have a digital certificate before engaging in any transactions.

The security requirements for action 6 could be satisfied using SSL, although the acknowledgement needs to be digitally signed by the merchant also, to satisfy the non-repudiation security requirement on the clients' behalf (all transactions).

5. CONCLUSION

By using the above approach, it is possible to develop a security architecture that would be suitable for the merchants' electronic commerce environment. The suggested framework follows a structured approach that helps in identifying the relevant security requirements for all parties involved. By following this approach, it is more difficult to forget any security requirements or, on the other hand, have unnecessary security mechanisms in place that hinder, rather than promote, electronic transactions. A fine balance should be established between ease of use for the client and reduced risk for the merchant.

The framework suggested in this article is a means of analysing an electronic commerce environment to be able to develop a suitable security architecture. It is by no means a substitute for a proper risk analysis, but can be used successfully where the luxury of sufficient time for a comprehensive risk analysis is not available. It can therefore be seen as a preliminary risk analysis, or as a method to check the results from a comprehensive risk analysis.

The time-to-market for electronic commerce is substantially less than in the physical business domain. Because of this, a quicker way of identifying and solving information security problems is required.

6. REFERENCES

[BADE94] Badenhorst, K. P., A formal approach to the optimisation of information technology risk management, Thesis (Ph.D.)-Rand Afrikaans University, South Africa, 1994

[BUCS98] BUC S.A., "Marion 2000 – User's guide of Marion 2000", BUC S.A., Paris, France, 1998

[CENT96] Central Computing and Telecommunications Agency, *CRAMM Management Guide,* CCTA, UK, 1996

[ERNS98] Ernst & Young, Executive guide to eCommerce, Ernst & Young International, Release 1, September 1998

[ERNS99] Ernst & Young, E-commerce: 1999 Special report – Technology in financial services, SCORE retrieval file number J00226, 1999

[IBM95] IBM, Enterprise-wide security architecture and solution presentation guide, IBM Corporation, SG24-4579-00, Red Book Collection, November 1995

[LABU00] Labuschagne, L, A new approach to dynamic Internet risk analysis, Thesis (D.Com) - Rand Afrikaans University, South Africa, 2000, http://csweb.rau.ac.za/deth/acad/thesis/

[MACG96] Macgregor, R.S., Aresi, A. and Siegert, A., WWW.security - How to build a secure world wide web connection, Prentice Hall, ISBN 0-13-612409-7, USA, 1996

[PRES97] Pressman, R.S., Software engineering: a practitioner's approach – Fourth Edition, The McGraw-Hill Companies, Inc., ISBN 0-07-709-411-5, USA, 1997

[SET00] SET Secure Electronic Transaction LCC, The SET™ Specification, http://www.setco.org/set_specifications.html, 2000