GUIDELINES FOR REDUCING AUDIT RISK IN AN E-COMMERCE ENVIRONMENT WITH SPECIFIC REFERENCE TO VALIDITY

by

DEON STOLTZ

Short Dissertation

Submitted in partial fulfilment of the requirements for the degree

MASTER OF COMMERCE

in

COMPUTER AUDITING

in the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

at the

RAND AFRIKAANS UNIVERSITY

STUDY LEADER: PROF. A DU TOIT

JOHANNESBURG
NOVEMBER 1999

DECLARATION

I declare that this short dissertation hereby submitted to the Rand Afrikaans University for the degree of Master of Commerce, except to the extent acknowledged in the text, is my own unaided work and has not been submitted previously for any degree to any other university.

DEON STOLTZ

ACKNOWLEDGEMENTS

All honour to God

INDEX

OPSOMMING

RIGLYNE OM OUDIT RISIKO TE BEPERK IN 'n E-HANDEL OMGEWING MET SPESIFIEKE VERWYSING NA GELDIGHEID

DEUR

DEON STOLTZ

OPSOMMING VAN DIE SKRIPSIE INGEDIEN VIR DIE GRAAD
MAGISTER COMMERCII IN REKENAAROUDITERING
IN DIE
FAKULTEIT EKONOMIESE EN BESTUURWETENSKAPPE
AAN DIE
RANDSE AFRIKAANSE UNIVERSITEIT

STUDIELEIER: PROF. A DU TOIT

JOHANNESBURG
NOVEMBER 1999

RIGLYNE OM OUDIT RISIKO TE BEPERK IN 'n E-HANDEL OMGEWING MET SPESIFIEKE VERWYSING NA GELDIGHEID

Die doel van hierdie opsomming is om die agtergrond, metodiek en gevolgtrekking van die navorsing weer te gee. Die opsomming is onder die volgende hoofde uiteengesit.

1. **Probleemomskrywing en doel van hierdie navorsing**
2. **Navorsingsmetodiek**
3. **Omvangsbeperking en uitsluitings**
4. **Resultate**
5. **Gevolgtrekking**

1. Probleemomskrywing en doel van hierdie navorsing

Ontwikkeling op die tegnolgiese gebied het die afgelope dertig jaar teen so 'n fenominale tempo plaasgevind dat ons, ons nou inderdaad in die inligtingsera bevind. Hierdie inligtingsera is die gevolg van die toeganklikheid van inligting wat voortspruit uit die tegnologiese vordering en ontwikkeling. Een van hierdie tegnologiese ontwikkelinge is elektroniese-handel (e-handel).

E-handel word moontlik gemaak deur 'n wye verskeidenheid van tegnologiese infrastrukture. Die infrastrukture sluit in rekenaarstelsels, bedryfstelsels, databasisse, netwerke, en web bedieners om maar 'n paar te noem. Hoewel hierdie infrastrukture help om e-handel te bevorder, dra dit egter ook by tot nuwe risiko's.

Die blote feit dat elektroniese transaksies via 'n onveilige medium soos die Internet geskied, is genoeg om kriminele aktiwiteite aan te spoor. Die gevolg van die kriminele aktiwiteite in 'n e-handel omgewing is die risiko van ongeldige transaksies. Vir die ouditeur beteken hierdie kriminele aktiwiteite 'n toename in oudit risiko.

Die doel met hierdie skripsie is eerstens, om risiko's en risiko areas te identifiseer in 'n e-handel omgewing en dan tweedens, om 'n kontrolelys daar te stel wat vir die rekenaarouditeur as riglyn kan dien, om hierdie risiko's aan te spreek, in sover dit betrekking het op die oudit doelwit van geldigheid.

2. Navorsingsmetodiek

'n Literatuurstudie is uitgevoer op bestaande gesaghebbende literatuur, wat insluit gepubliseerde en ongepubliseerde werke sowel as die Internet. Deur die inligting te gebruik wat uit hierdie bronne verkry is, is 'n kontrolelys saamgestel om as riglyn te dien tydens die oudit van geldigheid in 'n e-handel omgewing.

3. Omvangsbeperking en uitsluitings

Die grootste risiko met betrekking tot e-handel transaksies is die geldigheid van die transaksies. Gevolglik fokus die skripsie op die geldigheid van elektroniese transaksies en die invloed op oudit risiko en meer spesifiek kontrole risiko. Geen een van die ander oudit doelwitte is in hierdie skripsie aangespreek nie.

Die twee hoofvorme van e-handel is elektroniese data uitruiling (EDI) en Internet gebaseerde e-handel. Die skripsie fokus uitsluitlik op Internet gebaseerde e-handel. Die kontrolelys is opgestel vanuit die veronderstelling dat die stelsel wat geoudit word gebruik maak van die SSL en die SET protokol sowel as keerwalle.

4. Resultate

Vier areas is geïdentifiseer wat beveilig moet word om 'n veilige e-handel omgewing daar te stel:

- Die kliënt self;
- Die data wat in transito is;
- Die e-handel bediener; en
- Die bediener sagteware

Die toegangsroete van 'n e-handel transaksie soos uiteengesit in figuur 1 is saamgestel. Die figuur dien as riglyn vir die kontrolelys soos vervat in hoofstuk vier van die skripsie.

5. Gevolgtrekking

E-handel transaksies groei teen 'n fenominale tempo en daar is geen twyfel dat dit net 'n kwessie van tyd is voordat e-handel 'n huishoudelike naam sal wees. E-handel is hier om te bly, die tegnologie rondom e-handel mag dalk in die toekoms verander, maar elektroniese transaksie sal daar altyd wees, dit is gerieflik en dit is maklik.

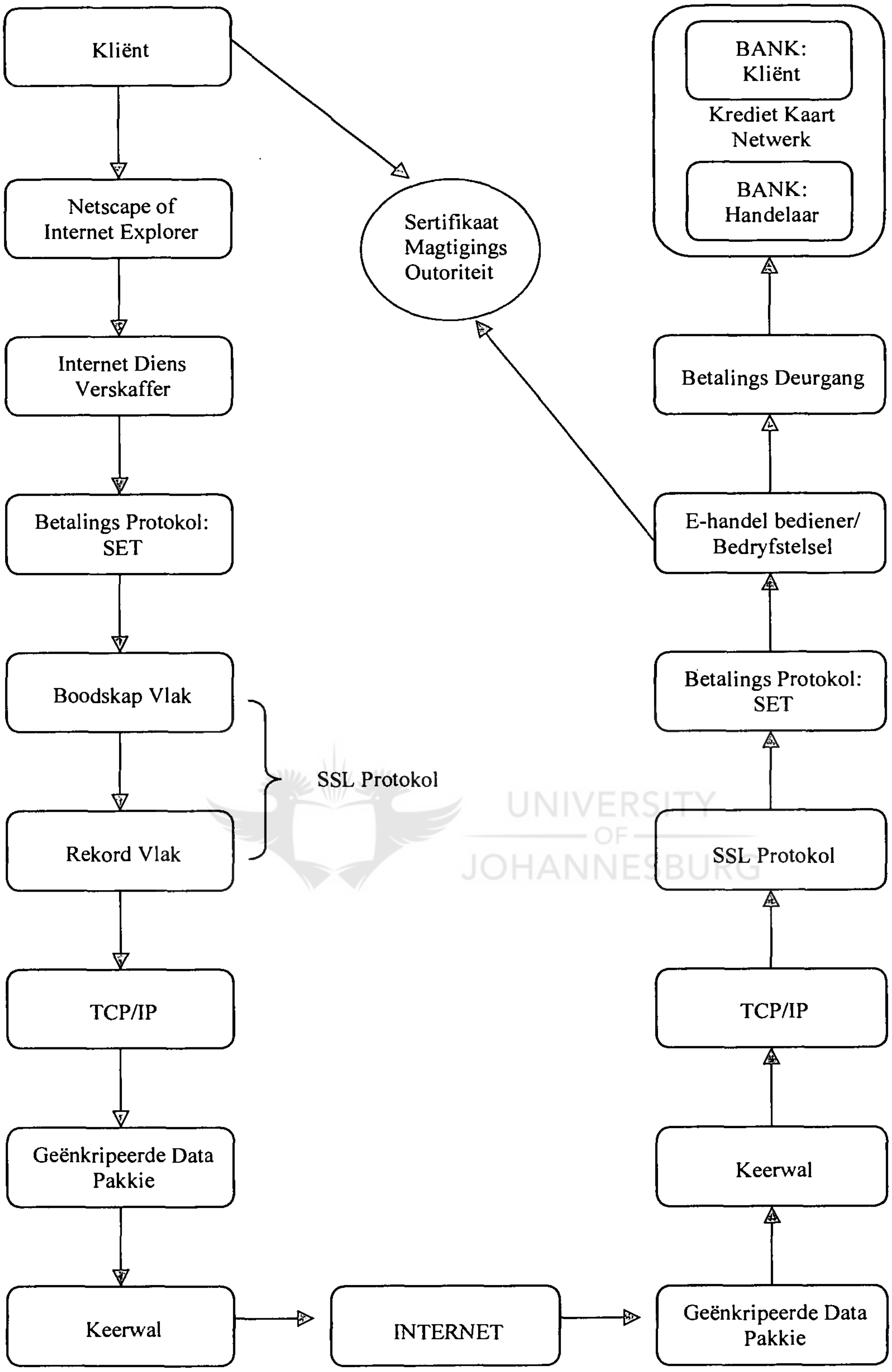
In 'n e-handel omgewing is dit 'n kwessie van tegnologie word gebruik om tegnologie te oudit. Tot die mate wat die rekenaarouditeur daardie tegnologie kan verstaan en kan toepas moet hy daarvan gebruik maak, andersins moet gebruik gemaak word van kundiges soos vereis deur SAOS 620 – Gebruik van die werk van kundiges. Dit is dus van kardinale belang dat die rekenaarouditeur op hoogte bly van nuwe tegnologiese ontwikkelinge en verwikkelinge in die IT-industrie.

Die grootste risiko area in ‘n e-handel omgewing is die data in transito. In die verband is twee protokols geïdentifiseer nl. die SSL protokol en SET protokol.

SET beveilig die betalings informasie, d.w.s die kredietkaartnommer, deur gebruik te maak van kriptografie . SSL verskaf ‘n veilige kommunikasie kanaal tussen web klient en web bediener deur gebruik te maak van digitale sertifikate en beskerm so die bestelling se besonderhede.

Dit is dus moontlik om die geldigheid van elektroniese transaksies te bevestig deur gebruik te maak van die nuutste tegnologie en sagteware wat beskikbaar is.

Ter opsomming verskaf hierdie kontrolelys ‘n riglyn aan die rekenaarouditeur, wat as basis dien tydens die oudit van die geldigheids-doelwit in ‘n e-handel omgewing. Na gelang van verandering in tegnologie behoort die kontrolelys dienooreenkomstig aangepas te word.



Figuur 1 Toegangsroete van 'n e-handel transaksie soos aangepas (Loshin, 1997:21-24) (Bierer, 1994:55)(Garfinkel, 1997: 418)(Drew, 1998:26) (Ghosh, 1997:104).

SYNOPSIS

1. PROBLEM DESCRIPTION AND OBJECTIVE OF THIS SHORT DISSERTATION
2. RESEARCH METHODOLOGY
3. SCOPE AND LIMITATIONS
4. RESULTS
5. CONCLUSION

1. PROBLEM DESCRIPTION AND OBJECTIVE OF THIS SHORT DISSERTATION

The Internet itself was not designed with security in mind. As e-commerce makes use of the Internet, this lack of security has a direct impact on the risks associated with e-commerce as well as the validity of e-commerce transactions.

The fact that business transactions are being performed online over this insecure medium, namely the Internet, is enough to encourage criminal activity. This criminal activity will ultimately result in invalid transactions, thereby influencing audit risk.

The objective of this short dissertation is firstly to identify the risks and risk areas in an e-commerce environment and secondly to develop a check-list that will assist the computer auditor when auditing validity in an e-commerce environment.

2. RESEARCH METHODOLOGY

A literature survey was conducted on existing authoritative textbooks and other literature available on e-commerce. With the information obtained from this research, a check-list was compiled to assist the computer auditor when auditing validity in an e-commerce environment.

3. SCOPE AND LIMITATIONS

Two main forms of e-commerce exist, the one is electronic data interchange (EDI) and the other is Internet based e-commerce. This short dissertation focused on Internet based e-commerce.

4. RESULTS

The four key areas that need to be secured in order to ensure a secure e-commerce environment were discussed. These four areas are:

- The Web client;
- Data in transit;
- Commerce server; and
- Operating system security.

The access path of an e-commerce transaction as set out in figure 1 was compiled from various sources. This access path serves as a guideline for the check-list as set out in chapter four of this short dissertation.

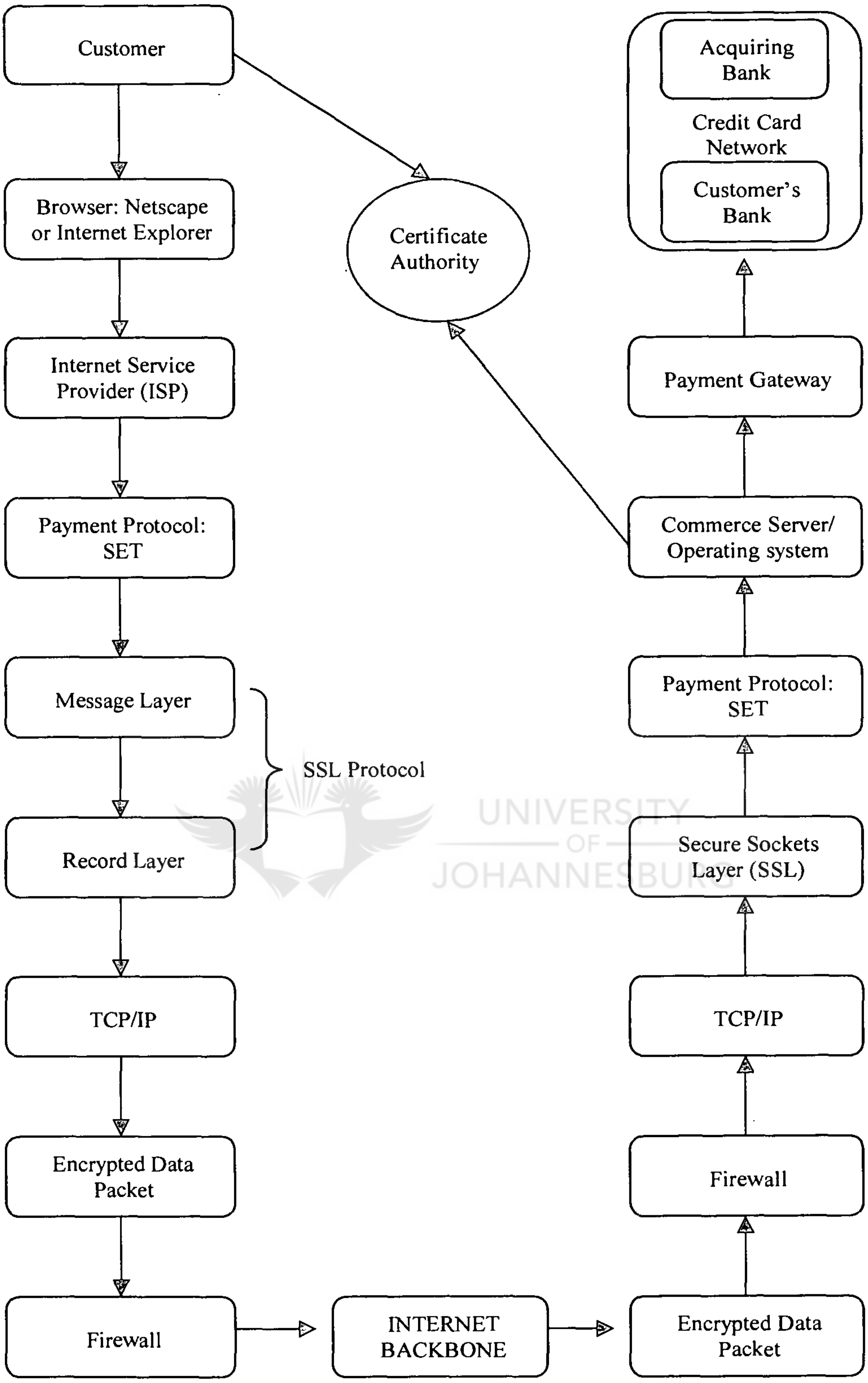


Figure 1. Access path of an e-commerce transaction as adapted (Loshin, 1997:21-24) (Bierer, 1994:55)(Garfinkel, 1997: 418)(Drew, 1998:26) (Ghosh, 1997:104)

5. CONCLUSION

From a business point of view, e-commerce presented the world with exciting new opportunities. However, along with these new opportunities came new risks.

In an e-commerce environment the auditor must use technology to audit technology. This can be done only by keeping abreast of the new developments in the IT industry.

In summary, this short dissertation provides a check-list to the computer auditor when auditing validity in an e-commerce environment. As technology changes, the check-list should be adapted accordingly.

CHAPTER 1
INTRODUCTION

CONTENTS PAGE

1.1 BACKGROUND

As the presence of the World Wide Web (WWW) becomes larger and more popular, many changes can be expected. Many of these changes have already begun to occur. Traditionally, people had to travel to a store, use mail or place telephone orders to purchase goods and services, but as the new millennium approaches, more and more people are starting to make use of the Internet to purchase these goods and services (Drew, 1998:2).

Because of the anonymous conditions under which communications networks operate, procedures must be developed that serves as a substitute for existing procedures used in face-to-face or mail and telephone order transactions, including the authentication of the card-holder by the merchant. There is also a need for the card-holder to authenticate that the merchant accepts Secure Electronic Transactions (SET) (SET Secure Electronic Transactions LLC, 1999).

Until recently, e-commerce referred primarily to electronic data interchange (EDI) and electronic messaging technologies that facilitated the exchange of information. During the last year or two, the term e-commerce has broadened to include business-to-business and business-to-consumer transactions conducted over the Internet and the World Wide Web (Ghosh, 1998: 1-2).

With business rushing to put everything from catalogues of their products to the details of internal accounts on the Internet, e-commerce is rapidly establishing itself as the hottest growth area in the industry (Ellison, 1999:103).

A survey done by Ernst & Young shows clearly that management has begun to view security as an enabler to doing business on the Internet. However, security-related problems are still having an adverse effect on progress. Many companies do not monitor systems activity, and therefore they are not aware of the activities taking place. Responses like this may help to explain companies' unwillingness to become involved in e-commerce (Ernst &Young, 1997:8).

Almost everything sold via the Internet is referred to as e-commerce, from the books sold by Amazon.com, to Dell computers, to the detailed account information and personnel files accessed via VPNs, intranets and extranets. The implications of business moving to the Internet are vast. One of these implications is exposure to new risks (Ellison, 1999:103) (Anon, 1999:28).

1.2 PROBLEM DESCRIPTION

New technologies are evolving everyday. Over the last 30 years, technology has moved so rapidly that we are now truly in the information age. One of these new technologies is e-commerce. Thanks to the Internet, much of the world has access to more information than ever thought possible. With the click of a mouse button, you can get the latest news on almost any topic, from important financial events to the latest security flaws in the latest released software. However, these new technologies bring new risks (Ernst &Young, 1997:4).

E-commerce is enabled by an infrastructure of technologies and services, many of which are also used to support other applications. The infrastructure includes computer systems, operating systems, databases, development tools, networks, Web servers and Web browsers. This large existing base of technology has made the rapid growth in Web-based e-commerce possible. Although this infrastructure is helping to enable e-commerce, it is also contributing to an increase in risk (Price Waterhouse, 1998:565) (Anon, 1999:28).

As Ghosh (1998:6) and Feghhi (1998:3) stated respectively: "The mere fact that business is being performed online over an insecure medium is enough to entice criminal activity to the Internet" and "All Internet communications are inherently unsecure and subject to eavesdropping and tampering. A dishonest user may masquerade as an authorized user of a system in order to carry out fraudulent activities".

Kamptan (1999) explains that the security of an e-commerce site can be compromised in many ways. There are numerous ways in which an attacker can access data that is being sent or received, including, but not limited to, the following:

- **Spoofing**

  The attacker (client) can fool the merchant's server into believing that the request or post that he is sending is from another site. This is known as IP and/or DNS spoofing. The merchant's server may respond, believing that the client (attacker) is "trusted", when in fact the client is not.

- **Sniffing**

  In some cases, it is possible for an attacker to snatch packets when they are being sent over the network, especially with the newer cellular modems and unsecured phone lines.

- **Traffic Analysis**

  Using sampling techniques on the packets or, more commonly, the server log files, an attacker can learn about the nature of the transactions processed by a site.

According to Garfinkel (1998:4), the World Wide Web is the fastest growing part of the Internet. Unfortunately, is also the part of the Internet that is most vulnerable to attack. Web servers make an attractive target for attackers for many reasons, one of them being electronic commerce.

Many Web servers are involved with commerce and money. These Web servers, or better known as commerce servers, have become a repository for sensitive financial information, making them an attractive target for attackers. The commercial services on these servers also make them targets of interest.

1.3 OBJECTIVE OF THIS RESEARCH

The objective of this short dissertation is firstly to identify the risks and risk areas associated with e-commerce, with specific reference to the validity of the transactions that are logged, and secondly to compile a check-list that will assist the computer auditor in ascertaining whether the controls and technologies implemented by management are adequate and up to date in order to reduce the risk of invalid transactions, thereby reducing the audit risk to an acceptable level.

1.4 SCOPE, LIMITATIONS AND EXCLUSIONS

Much has been written about e-commerce and lots more will in future be written about e-commerce. For the purposes of this short dissertation, some limitations and exclusions are applicable.

To assure end-users and businesses of privacy and confidentiality in online transactions, a number of technological solutions have been introduced. In any online activity, a number of software components will be utilised to handle a transaction – whether it is mail, file transfer, remote login or Web surfing. A failure in any one of these components may compromise the integrity of the entire transaction (Ghosh, 1998:xi).

Ghosh (1998:xii) explains that the human factor is most certainly always a weak point in the security of any computer system. However this short dissertation will focus on the technological issues in e-commerce that ensure valid transactions.

Four critical components make up almost any e-commerce transaction (Ghosh, 1998:xii):

- The client-side software;
- The data transaction protocols;
- The commerce server; and
- The operating system software.

This short dissertation will ignore the client-side and focus on the business-side of the four components, being the data transaction protocols, commerce server security and operating system security.

As this short dissertation deals only with the validity of e-commerce transactions, none of the other audit objectives are addressed in this document, i.e. completeness, accuracy and integrity. These audit objectives with respect to e-commerce require a research study of their own.

The two main forms of e-commerce are electronic data interchange (EDI) and Internet-based e-commerce. Internet commerce consists mainly of Web-based e-commerce (Price Waterhouse, 1998:554).

Internet commerce as the name suggests uses the Internet to manage and conduct a business transaction. Web commerce, a subset of Internet commerce, goes beyond using the Internet as a transport mechanism and assumes that the participants have Web access. For the purposes of this short dissertation, the focus will be placed on Internet-based e-commerce, ignoring electronic data interchange (EDI) (Price Waterhouse, 1998:556).

1.5 DEFINITIONS AND METHODOLOGY

This dissertation deals with reducing **audit risk** in an **e-commerce** environment, with specific reference to **validity.** The appropriate keywords have been defined as follows:

1.5.1 Audit risk

"Audit risk is the risk that the auditor expresses an inappropriate audit opinion when the financial statements are materially misstated." Because of the limitations inherent in both the preparation and the audit of financial statements, it is not possible to eliminate audit risk completely (SAICA, 1996:par3).

1.5.2 E-Commerce

"Electronic commerce is defined as possessing all the following attributes:

- Direct electronic interaction between two computer applications (application-to-application) or between a person using a computer (typically a Web browser) and another application (typically a Web server).

- The interaction involves the completion of a specific transaction or part of a transaction.

- The transaction crosses enterprise boundaries, either between two businesses (business-to-business) or between a business and a consumer (business-to-consumer)" (Price Waterhouse, 1998:554).

Electronic commerce is also defined as:

- "The conduct of commerce in goods and services, with the assistance of telecommunications and telecommunications-based tools"(Clarke, 1998:1).

1.5.3 Validity

"The purpose of the validity check is to ensure that actions taken by the computer are valid actions. A valid action is one that conforms to a set of actions that are considered to be correct. The validity check compares each action with a set of valid actions to ensure that it is indeed valid" (Watne & Turney, 1990:242).

Due to the fact that a number of research topics and publications have been completed on validity as a control objective, no literature survey was carried out on this aspect. It is assumed that the research works published by Boshoff (1985, 1990) are correct.

In chapter two a literature survey was conducted on authoritative sources available on audit risk and how it relates to the audit objective of validity, with the emphasis on audit risk.

In chapter three a literature survey was conducted on authoritative books and Internet sources available on e-commerce, with the aim of explaining the technology used in e-commerce, in order to identify weaknesses that will influence the validity of e-commerce transactions.

1.6 RESEARCH APPROACH

The approach adopted in this short dissertation is to compile a check-list that will assist the computer auditor when dealing with the validity of e-commerce transactions.

This check-list was compiled from an audit perspective for use by the computer auditor and not for use by an e-commerce merchant who wishes to secure his e-commerce web site with respect to the validation of transactions.

This check-list was compiled to assist the computer auditor in evaluating the validity of transactions. The basis of this check-list depends on an understanding of e-commerce technology as explained in chapter three.

Chapter two expands on audit risk and validity and the effect that validity has on audit risk and more specifically on control risk. Chapter three discusses the access path of an e-commerce transaction and the technology used in e-commerce, based on the access-path as set out in figure 1.1. In chapter four, the check-list is presented.

1.7 SUMMARY OF RESULTS

The Internet is today a vast frontier of unknown elements, including new types of software and new discoveries of security flaws. The most secure technical solution to preventing attacks launched from the Internet is to unplug the network from the computer. This solution is however not viable in today's business climate.

In an e-commerce environment, the auditor must make use of technology to audit technology. This can be done only by keeping abreast of the new developments in the IT industry.

The risks that affect validity have been identified. These risks are set out in chapter two. Four risk areas have also been identified as specified by Ghosh (1998:3).

An access path of an e-commerce transaction as set out in figure 1.1 has been compiled from various sources. This access path serves as a basis for the check-list as set out in chapter four.

The different components of this access path are discussed in chapter three, giving the necessary background to obtain a clear understanding of the technology involved in the entire process of an electronic transaction and in securing an electronic transaction.

In chapter four, a check-list is compiled, serving as a guideline when auditing the validity control objective

1.8 CONCLUSION

There is no silver bullet when it comes to securing e-commerce transactions. All software components involved in the handling of e-commerce transactions over the Internet/World Wide Web must be equally secured.

The computer auditor can use the check-list as set out in chapter four when auditing the validity of e-commerce transactions. The objective of this short dissertation has therefore been met.

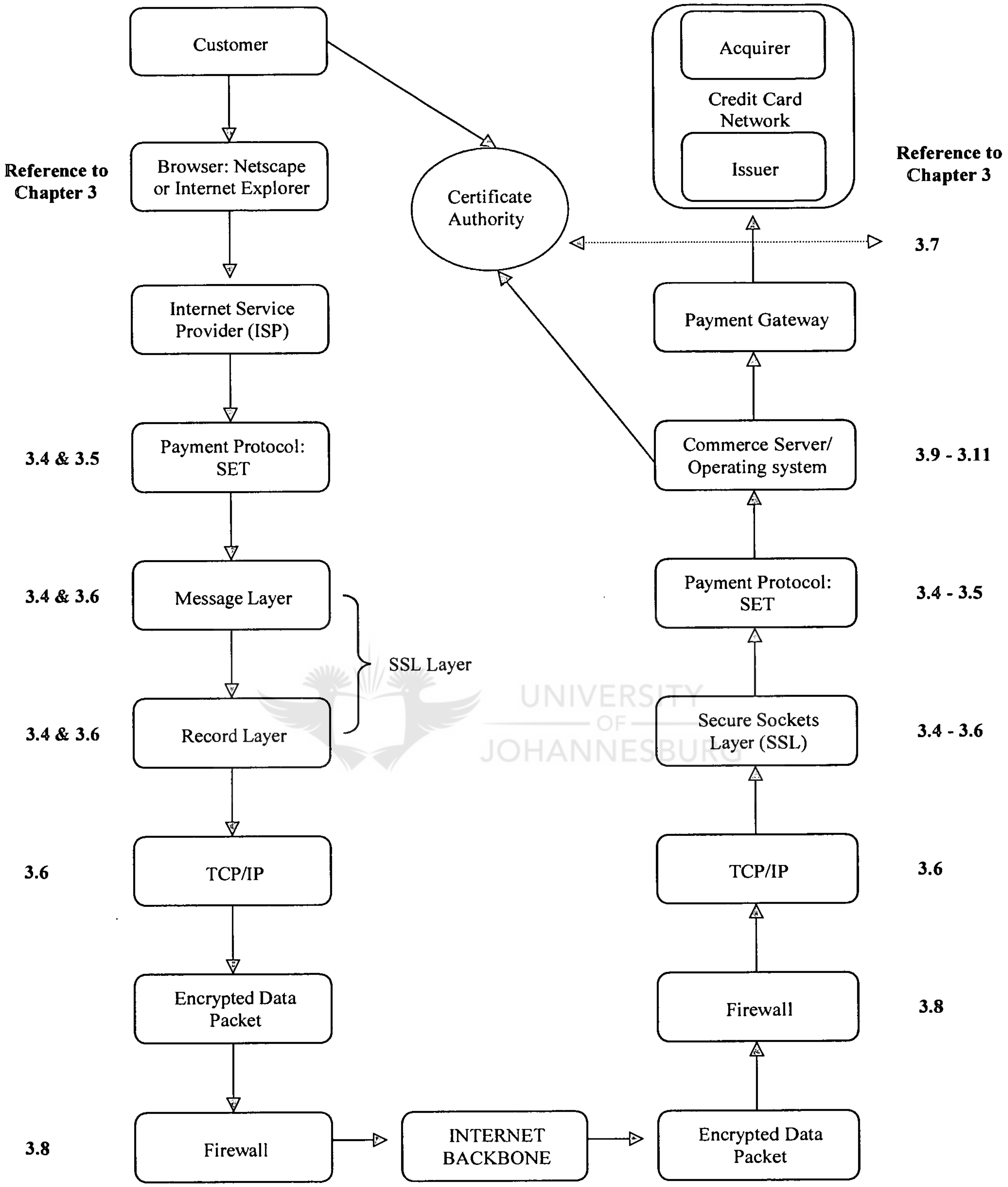


Figure 1.1 Access path of an e-commerce transaction adapted from (Loshin, 1997:21-24) (Bierer, 1994:55)(Garfinkel, 1997: 418)(Drew, 1998:26) (Ghosh, 1997:104)

CHAPTER 2

AUDIT RISK AND VALIDITY

CONTENTS PAGE

2.1 OBJECTIVE

This short dissertation deals with reducing audit risk in an e-commerce environment with specific reference to validity. The objective of this chapter is therefore to expand on audit risk and how it relates to validity.

As stated earlier, the purpose of validity is to ensure that actions taken by the computer are valid actions. In order to determine whether these actions are valid, the auditor needs to evaluate internal controls. Internal controls are concerned with achieving objectives, such as:

- Ensuring that transactions are executed in accordance with management's general and specific authorisation (Validity); and

- Ensuring access to records is permitted only in accordance with management's authorisation (Validity).

The auditor's evaluation of internal controls will influence audit risk (SAICA, 1998).

2.2 NATURE OF LITERATURE SURVEY

To ensure the credibility and acceptance of the findings of this short dissertation, it is essential that the literature survey be based on authoritative sources. References were restricted to those published by auditors, audit firms, professional auditing bodies, authoritative technical books by computer experts and authoritative electronic publications.

References to electronic publications were kept to a minimum due to the fact that electronic resources, such as web pages, newsgroups and mailing lists are updated on a daily basis. Electronic publications in this short dissertation are therefore referred to on the understanding that they can be neither complete nor completely up to date.

2.3 SCOPE, LIMITATIONS AND EXCLUSIONS

This chapter focuses on validity and audit risk.

Chapter three explains the technology used in securing an e-commerce transaction subject to the provisos that the e-commerce system are making use of the SET protocol, SSL protocol, Firewall technology and digital certificates.

2.3.1 Validity

None of the other control objectives i.e. completeness, accuracy and integrity, are addressed in this short dissertation. For the purposes of this chapter, it will be assumed that the research works published by Boshoff (1985,1990) on validity as a control objective are correct.

2.3.2 Audit Risk

Audit risk consists of

- Inherent Risk;
- Control Risk; and
- Detection Risk (SAICA, 1996: par 3).

There is an inverse relationship between detection risk and the combined level of inherent and control risk. Furthermore, detection risk has an effect on the nature, timing and extent of substantive tests. The nature, timing and extent of these substantive tests also depend on the auditor's assessment of control and inherent risk.

Detection risk can be reduced by increasing substantive tests. In a computer environment, this can easily be done by making use of computer-assisted audit techniques (CAATs) (SAICA, 1998:par 6) (SAICA, 1996:par38)(Jenkins, Cooke & Quest, 1992:353).

Inherent risks are inherent to the business or the computer system. An auditor cannot create or control inherent risk. Inherent risk depends on factors such as integrity of management, experience and proficiency of management, nature of the business or the computer system. (Robertson, 1993:452)(SAICA, 1996:par 9).

This chapter will therefore focus on control risk, ignoring detection and inherent risk. The reason for this is that inherent risk is not controllable and detection risk depends on the auditor's perception of inherent and control risk. This is not to say that inherent and detection risk is of less importance or uncontrollable.

2.4 DEFINITIONS

2.4.1 Inherent risk

"Inherent risk is the susceptibility of an account balance or class of transactions to material misstatement that could be material, individually or when aggregated with misstatements in other balances or classes, assuming that there were no related internal controls" (SAICA, 1996:par3).

2.4.2 Control risk

"Control risk is the risk that a misstatement that could occur in an account balance or class of transactions and that could be material, individually or when aggregated with misstatements in other balances or classes, will not be prevented or detected and corrected on a timely basis by the accounting and internal control systems" (SAICA, 1996:par3).

2.4.3 Detection risk

"Detection risk is the risk that an auditor's substantive procedures will not detect a misstatement that exists in an account balance or class of transactions that could be material, individually or when aggregated with misstatements in other balances or classes" (SAICA, 1996:par3).

2.5 BACKGROUND

The vast growth potential of Internet-based commerce is tempered by legitimate concerns over the security of such a system. Despite the potential rewards of conducting business on the Internet, major corporations have been slow to embrace this technology. The primary concern for both businesses and consumers in establishing and participating in e-commerce is the potential for loss of assets and privacy due to breaches in the security of transactions and corporate computer systems (Ghosh, 1998: 9).

Web security is a matter of degree. The more security measures you employ, the more you reduce your risk. Management's goal should, therefore be to reduce risk as much as is practical and affordable, and then to take additional measures so that if there is a security incident, they will be able to recover quickly (Garfinkel & Spafford, 1998:24).

According to Kamthan (1999), the risks associated with e-commerce can be classified broadly into the following categories:

2.5.1 Business Practices

E-commerce often involves transactions between strangers. With the anonymity of e-commerce, the unscrupulous can establish electronic identities with relative ease. This makes it crucial for people to know that the company, with which they are doing business, discloses and follows certain business practices. Without such information and the assurance that the company has a history of following such practices, consumers could face an increased risk of loss, fraud, inconvenience or unsatisfied expectations (Kamthan: 1999).

2.5.2 Information Protection

It is important for consumers to be confident that they have reached a properly identified WWW site, and that the merchant takes appropriate steps to protect private consumer information. Although it is relatively easy to establish a WWW site on the Internet, the underlying technology can entail a multitude of information protection and related security issues. As a result, the confidentiality of sensitive information transmitted over the Internet can be compromised. For example, without the use of basic encryption techniques, consumer credit card numbers can be intercepted and stolen during transmission. Without appropriate firewalls and other security practices, private consumer information residing on a company's e-commerce server can be intentionally or unintentionally provided to third parties not related to the company's business. Security breaches may also include unauthorised access to the consumer's computer through an Internet connection (Kamthan: 1999).

2.5.3 Transaction Integrity

Without proper controls, electronic transactions and documents can easily be changed, lost, duplicated and processed incorrectly. These attributes may cause the integrity of electronic transactions and documents to be questioned, causing disputes regarding the terms of a transaction and the related billing. Potential consumers involved in e-commerce may seek assurance that the company has effective transaction integrity controls and a history of processing transactions accurately, completely and promptly, and billing its consumers appropriately (Kamthan: 1999).

2.6 AUDIT RISK

As an auditor, one must always ensure that the level of audit risk is acceptable. The acceptable level of detection risk is determined by the auditor's assessment of inherent risk and by the effectiveness of controls. This affects the nature, extent and timing of substantive tests. As the risk of material misstatement decreases due to the lower inherent risk or more effective controls, so the amount of assurance required from substantive tests decreases (Jenkins, et al. 1992:17).

However, in an e-commerce environment, it is not that simple. It is the view of the author that in an e-commerce environment, inherent risk will always be high for three reasons:

- The nature of the technology used;
- The environment in which e-commerce is operated; and
- The accessibility of information in an e-commerce environment, whether it is authorised or unauthorised access.

2.7 VALIDITY

According to Robertson (1992:488), the objective of validity is to ensure that recorded transactions are the transactions that should have been recorded, thereby implying that in an e-commerce environment:

- The person initiating the transaction should be duly authorised to use the credit card;
- Only transactions initiated with a valid credit card should be processed; and
- The transaction information received by the merchant should correspond to the transaction information sent by the customer.

A computer can be programmed to test the precise validity of an item, thereby either accepting or rejecting the item. This usually happens if input can be matched with data on a master file, for example checking against the bank's computers whether a credit card number presented for payment has not been cancelled, stolen or expired (Jenkins, et al. 1992:176).

Ernst & Young's (1997:10) survey indicated that forty-five percent of companies that took part in their security survey had breaches in Internet security. As an auditor this means that you have a fifty-percent chance that validity has been undermined in some way.

The survey also indicated that companies are making use of the following measures to address information security:

Virus detection software	90 %
PC access control software	54 %

Dial back or secure modems	38 %
Firewalls	34 %
PC hardware security devices	26 %
One-time passwords	24 %
Terminal key locks or lock words	24 %
Data encryption	23 %
Single sign-on software	16 %
Telecommunications encryption	16 %
Signature verification	12 %
Public-key cryptography	5 %

It is significant to see that as security measures become more technologically advanced, fewer companies are making use of these measures. These measures are all helping to validate transactions and to reduce audit risk if implemented properly.

2.8 CONCLUSION

Unfortunately, the fact is that computer security is neither painless nor free. If managers avoid computer security and decide to take their chances, they live in a riskier environment.

The responsibility for implementation of adequate and effective controls lies with management. Therefore, when an auditor assesses the level of audit risk, he/she should also evaluate management's attitude towards security and the implementation of security measures.

CHAPTER 3

E-COMMERCE

CONTENTS PAGE

3.1 INTRODUCTION

This chapter explains the path of a typical e-commerce transaction as well as the technologies, protocols and solutions that are used and implemented to secure these electronic transactions.

As stated in chapter one, there are four key areas that need to be secured in an e-commerce environment, being the client-side, the data in transit (the e-commerce transaction itself), the commerce server and the operating system software. This chapter looks at the last three areas, focusing on the business-side rather than the client-side, it also expands on securing the data in transit, the commerce server and the operating system as well as the risks associated with the aforementioned.

3.2 DESCRIPTION OF AN E-COMMERCE TRANSACTION

In stages one to nine, a typical e-commerce transaction is explained as illustrated in figure 3.1.

Stage 1:

The client browses for items in a variety of ways:

- Using a browser such as Netscape or Internet Explorer to view an online catalogue on the merchant's World Wide Web page;
- Viewing a catalog supplied by the merchant on a CD-Rom; or
- Looking at a paper catalogue.

Stage 2:

The client selects the items to be purchased.

Stage 3:

The client is presented with an order form containing the list of items, their prices and a total price, including shipping, handling and taxes. This order form may be delivered electronically from the merchant's server or created on the client's computer through electronic shopping software.

Stage 4:

The client selects the means of payment. This specification focuses on the case when a payment card is selected.

Stage 5:

The client sends the merchant a completed order along with payment instructions. In this specification, the order and the payment instructions are signed digitally by the client who possesses a certificate.

Stage 6:

The merchant requests payment authorisation from the client's financial institution.

Stage 7:

The merchant sends confirmation of the order.

Stage 8:

The merchant ships the goods or performs the requested services from the order.

Stage 9:

The merchant requests payment from the client's financial institution (Garfinkel, et al. 1997:316) (Ghosh, 1998:133-135).

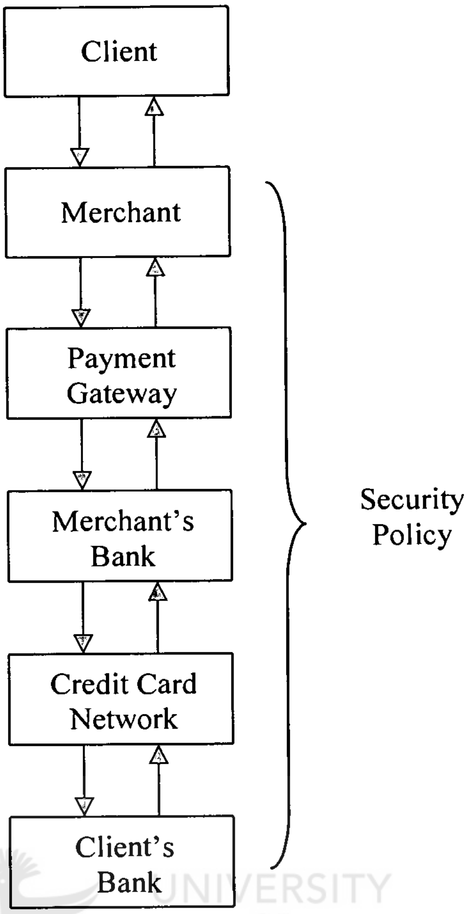


Figure 3.1 A typical e-commerce transaction (Garfinkel, et al. 1997:317, adapted)

3.3 SECURITY POLICY

The role of the security policy is to outline what is allowed, by whom and when. The security policy is only part of the security architecture that contributes towards securing the e-commerce transaction and therefore on its own it will not ensure compliance with the control objective of validity (Garfinkel, et al. 1997:256) (Ernst & Young, 1997:14).

3.4 PROTOCOLS

To secure an e-commerce transaction as set out in figure 3.1, it is important to know which security attributes are and are not provided by a given protocol. This includes information such as which protocols encrypt data, which protocols authenticate consumers as well as servers, which protocols handle payments and which ones offer non-repudiation?

In table 3.1, the available security protocols are listed, along with their attributes.

System or protocol	What is it?	Algorithms used for encryption	Provided
PGP (Pretty Good Privacy)	Application for encrypting e-mail	RSA, Message Digest(MD)	Confidentiality Authentication Integrity Non-repudiation
SSL	Protocol for encrypting TCP/IP transmissions	RSA, RC4 Message Digest (MD)	Confidentiality Authentication Integrity Non-repudiation
SET	Protocol for sending secure payment instructions over the Internet	RSA, RC2 Message digest	Confidentiality of credit card numbers

S-HTTP	Protocol for encrypting HTTP requests	RSA, DES others	Cofidentiality Authentication Non-repudiation Integrity
S/MIME	Format for encrypting Electronic mail	User-specified	Confidentiality Authentication Integrity Non-repudiation
Kerberos	Network security service for securing high-level applications	DES	Cofidentiality Authentication
Ipsec and Ipv6	Low-level protocol for encrypting IP packets	DES	Confidentiality Authentication
PCT	Protocol for encrypting TCP/IP packets	RSA, RCZ, RC4, MD5	Confidentiality Authentication Integrity Non-repudiation

Table 3.1 Encryption systems available (Garfinkel, et al. 1997:218)

3.5 SECURE ELECTRONIC TRANSACTIONS (SET)

SET is a protocol designed to ensure that merchants and card-holders can conduct safe business over insecure networks such as the Internet. SET uses cryptography to:

- Provide confidentiality and security;
- Ensure payment integrity; and
- Authenticate both the merchant and the client (Garfinkel, et al. 1997:330).

The SET system prevents unauthorised people from accessing sensitive credit card information by substituting an X.509 v3 certificate for the credit card number (PriceWaterhouse, 1998:574).

3.5.1 SET COMPLIANCE TESTING

For a merchant to make use of X.509 v3 certificates he must comply with SET's compliance testing procedures. SETCo was jointly formed by VISA and Mastercard to serve as the governing body overseeing the adoption and standardisation of the SET protocol. To continue using the SETMark, a vendor must re-test with the newest SET tests every six months.

The SET compliance testing has two basic parts:

- Running a set of software tests; and
- Completing a SET check-list.

Once completed, the SET tests and the check-list are sent to the Software Compliance Authority (SCA). The SCA will examine the results and report to SETCo. (Drew, 1998:183-185).

3.5.2 Security assurances specified by SET

Ghosh (1998:132-133) explains the four security assurances specified by SET as follows:

3.5.2.1 Confidentiality of transmissions

In no way does SET attempt to secure the order information in a credit card transaction. SET's only concern is securing the payment information, which is the credit card number. RSA Data Security's public key cryptography algorithms are specified by SET to encrypt the credit card numbers so that only the credit card transaction-processing centre can interpret the encrypted numbers.

Conclusion

SET's use of message encryption ensures confidentiality of information.

3.5.2.2 Integrity of data.

A risk of any electronic communication is the corruption of the data being sent from one party to another. In e-commerce applications, the corruption of information can have disastrous financial consequences. As explained later in 3.6.4, digital envelopes and mathematical algorithms that employ message digests and digital signatures can be used to ensure the integrity of data in transit against corruption.

Conclusion

SET provides for digital signatures, which ensure the integrity of payment information.

3.5.2.3 Authentication of the credit card-holder involved

As in any credit card transaction, the merchant must be able to confirm that the client is indeed the legitimate card-holder for the specific credit card presented. Digital certificates can be used to verify that a consumer is authorised to use the credit card in an electronic transaction. The client obtains a digital certificate from the financial institution that issues the credit card. The certificate is digitally signed by the financial institution as an endorsement that the client is authorised to make a purchase. The digital certificate is offered by the client to the merchant for the purposes of identity verification. If the signature on the digital certificate is matched by the public key of the financial institution, the merchant will have the assurance that the card-holder is legitimate.

Conclusion

SET uses digital signatures and card-holder certificates to ensure the authenticity of the card-holder.

3.5.2.4 Authentication of the identity of the merchant to the card-holder

Generally, consumers also require assurances that the merchant is a legitimate participating merchant in the credit card association and that the merchant's identity is known to the consumer. The use of digital certificates can be used to verify the identity of the merchant.

Conclusion

SET provides for the use of digital signatures and merchant certificates to ensure authentication of the merchant.

3.6 SECURE SOCKETS LAYER (SSL)

The Secure Sockets Layer is a general-purpose cryptographic protocol for securing bi-directional communication channels and therefore a suitable protocol for use with e-commerce, offering:

- Authentication and non-repudiation of the server and the client by way of digital signatures;
- Confidentiality of data through the use of encryption; and
- Integrity of data through the use of message authentication codes (Garfinkel, et al. 1997:234).

Every Secure Sockets Layer server must have an SSL server certificate. When Netscape / Internet Explorer connects to a Web server using the SSL protocol, the server sends the browser its public key in an X.509 v3 certificate. The certificate is used to authenticate the identity of the server and to distribute the server's public key, which is used to encrypt the information that is sent from the client to the server, thus ensuring confidentiality (Ghosh, 1998:176).

Where the SSL protocol is chosen, it provides a secure channel between Web client and Web server. In order to make use of the SSL protocol, it must be selectively employed by the Web client and server, as opposed to the standard Internet protocols, such as TCP/IP used by default (Ghosh, 1998:103).

The Internet was not developed with security in mind and is therefore by nature an insecure channel for sending messages. When messages are sent from one Internet site to another, these messages are routed through a number of intermediate sites before reaching their destination. SSL secures the channel by providing end-to-end encryption of the data that is sent between a Web client and a Web server. Adding SSL to the protocol stack will secure messages from unauthorised viewing that may occur anywhere along the route from the client to the server. Unfortunately SSL secures only the communication channel and not the data residing on client and server machines (Ghosh, 1998:104).

The SSL v3.0 protocol consists of two layers, the message layer and the record layer, fitting in between the application layer and the transport layer as indicated in figure 3.2 (Garfinkel, et al. 1997:233).

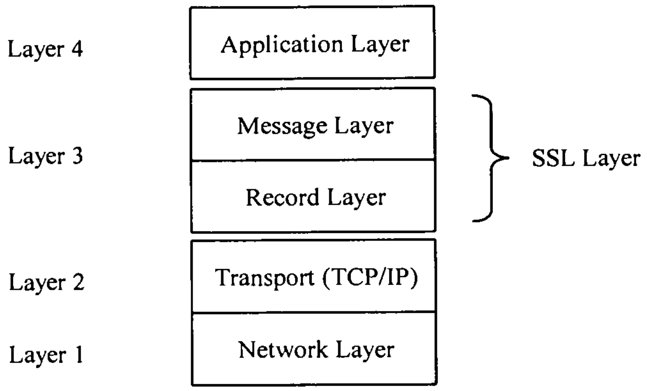


Figure 3.2 The TCP/IP 4-layer model for computer communications (Feghhi, et al. 1998:21, as adapted)

Ghosh (1998:103-104) explains that SSL rides on top of the TCP/IP stack in providing a secure channel. The TCP protocol provides reliable transmission of packets, but in order to obtain a secure communication channel, one needs to look further at SSL. SSL provides:

- Secure communication;
- Authentication; and
- Integrity of the data packet.

Each layer uses the services provided by the layer beneath it. From figure 3.2, it is clear that SSL is situated underneath the application layer. Thus, any application that makes use of SSL will have the following:

- Routing of packets provided by IP;
- Reliable delivery of packets provided by TCP; and

- Secure connection provided by SSL (Ghosh,1998:103).

3.6.1 Record Layer

The SSL Record layer is used for encapsulation of various higher level protocols, such as the SSL Handshake Protocol, which allows the server and the client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol begins transmitting or receiving. SSL v3.0 defines three protocols:

- **Alert protocol**

The record layer transmits specific types of messages, known as "alerts". Two levels of alerts exist: level one, which is a warning with respect to a problem that is not fatal, and level two, which is a fatal alert. The level two alert will result in the termination of the SSL session (Garfinkel, et al. 1997:417- 422).

SSL has thirteen alert messages. The relevant messages with respect to validity are listed in table 3.2.

- **ChangeCipherSpec protocol** (CCS)

This is when there are changes from one encryption algorithm to another, which usually occur at the end of a handshake, known as "strategies" (Garfinkel, et al. 1997:421).

Alert Number	Alert Name	Meaning
10	Unexpected message	An inappropriate message was received, indicating an error in one of the SSL implementations.
40	Handshake failure	The sender was unable to negotiate an acceptable set of security parameters.
41	No certificate	No appropriate certificate is available.
42	Bad certificate	Certification request failed. Reason: Corrupted certificate Signature did not verify.
43	Unsupported certificate	Sender does not support the type of certificate.
44	Certificate revoked	The sender received a certificate that had already been revoked.
45	Certificate expired	The sender received a certificate that has expired.
46	Certificate unknown	An error occurred during the processing of the certificate.
47	Illegal parameter	The sender found a value in the handshake that is out of range or inconsistent.

Table 3.2 Alert descriptions (Garfinkel, et al. 1997: 420-421)

- **Handshake protocol**

The handshake begins when the server and the client connect. The handshake is used to authenticate the client and the server, and to select the cryptographic algorithms for encryption as well as the other protocols that will be used during the communication session (Garfinkel, et al. 1997:421).

In addition to securing the channel via encryption, SSL provides authentication of the merchant's server. This means that if the channel has been secured successfully, the Web client is also assured that the server has been endorsed by a certification authority (CA). The CA will endorse only the identity of the Web server and not the quality of the Web content.

3.6.2 Encryption

SSL has two main functions, firstly to authenticate the Web server and secondly to encrypt the communication channel. To accomplish these two functions, SSL uses two different encryption technologies. The one is public key encryption, also known as asymmetric key encryption and the other is private key encryption, also known as symmetric key encryption (Ghosh,1998:114).

3.6.3 Public Key Encryption

Public key cryptography is known as asymmetric encryption due to the fact that it makes use of two different keys: one key to encrypt a message and a totally different key to decrypt that message. The one key is known as the public key and, as the name suggests, this key is shared with everyone. The public key is used to encrypt a message. The other key is known as the private key, known to only one person. The private key is used to unlock the code of the message encrypted with the public key (Ghosh, 1998:115-116).

In figure 3.3, the merchant and the client keep their private keys secret from each other, but they know each other's public keys. For the client to send a secure message to the merchant, the client encrypts the message with the merchant's public key. The merchant is the only one with the private key, so only the merchant can decrypt the message that was encrypted by the client with his (the merchant's) public key (Ghosh , 1998:114 - 115).

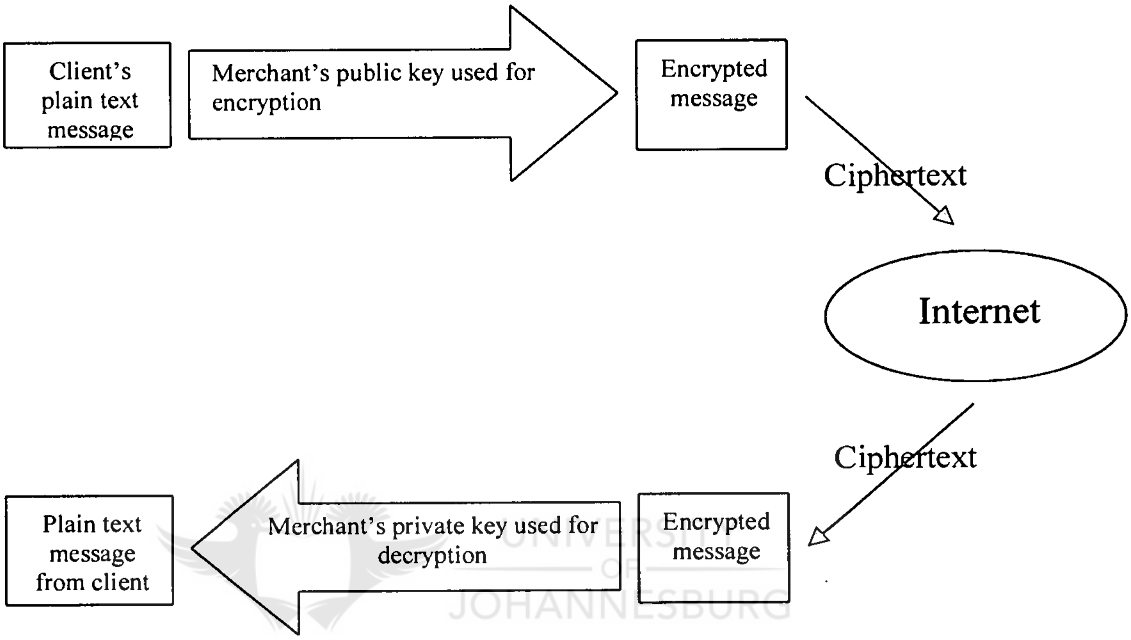

Client's plain text message
Merchant's public key used for encryption
Encrypted message
Ciphertext
Internet
Ciphertext
Encrypted message
Merchant's private key used for decryption
Plain text message from client

Figure 3.3 Public key encryption (Ghosh, 1998:116, adapted)

3.6.4 Digital Envelope

Public key cryptography has its value in authenticating the server and/or client and in providing unforgeable digital signatures. These methods can be combined to form a secure digital envelope. This secure digital envelope:

- Ensures that messages are confidential;
- Authenticates the identity of the sender; and

- Provides proof that the message has not been tampered with in transit (Ghosh. 1998:116).

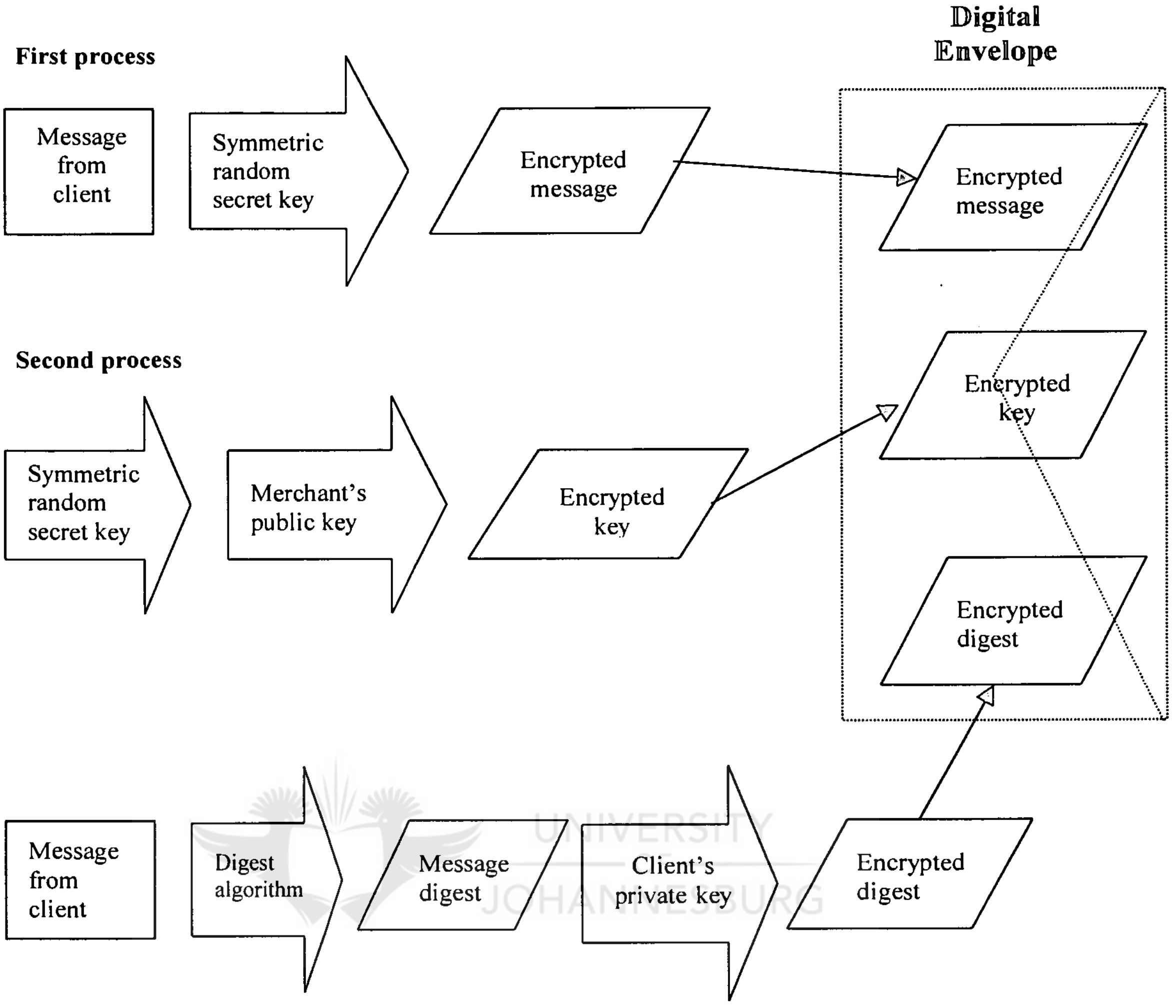


Figure 3.4 Creating a secure digital envelope (Ghosh, 1997:123)

Ghosh (1998:122-124) explains the process of a digital envelope as follows: in figure 3.4, the client generates a secret key randomly and uses it to encrypt the message via symmetric cryptography. The client will use the merchant's public key to encrypt this random key. Only the merchant can decrypt this random key with his private key.

In the first process, the client encrypts the letter using a secret key. In the second process the secret key that was used to encrypt the letter is encrypted with the merchant's public key.

In order to obtain authentication and data integrity, the client computes a message digest of the message, which generates a unique signature of the message. The client will then encrypt the message digest using his private key.

The encrypted message, the encrypted key and the encrypted message digest makes up the digital envelope and are sent to the merchant. The merchant:

- First decrypts the encrypted key with his own private key;
- Then he uses that key to decrypt the message from the client; and
- Then he decrypts the message digest using the client's public key.

The merchant will then re-compute the message digest of the letter and compare it with the message digest that the client included to ensure that the message has not been altered.

From an e-commerce point of view, private key encryption is not viable because the number of private keys necessary grows with the square of the size of the community (Baldwin & Chang, 1997:40).

3.7 DIGITAL CERTIFICATES

A digital certificate is a binding between an entity's public key and one or more attributes that relate to the identity of that entity. The digital certificate provides assurance that the public key belongs to the identified entity and that the entity possesses the corresponding private key. Trusted third-party certification authorities (CAs), such as Verisign, issue digital certificates. Before Verisign issue a digital certificate, they first confirm the identity of the subscriber (Feghhi, et al. 1998:63).

To prevent digital certificates from being forged, a certification authority incorporates its signature into the certificate by signing the certificate digitally, after authenticating the identity of the subscriber (Feghhi, et al. 1998:63).

The X.509 is an ISO certificate format with elements as shown in figure 3.5.

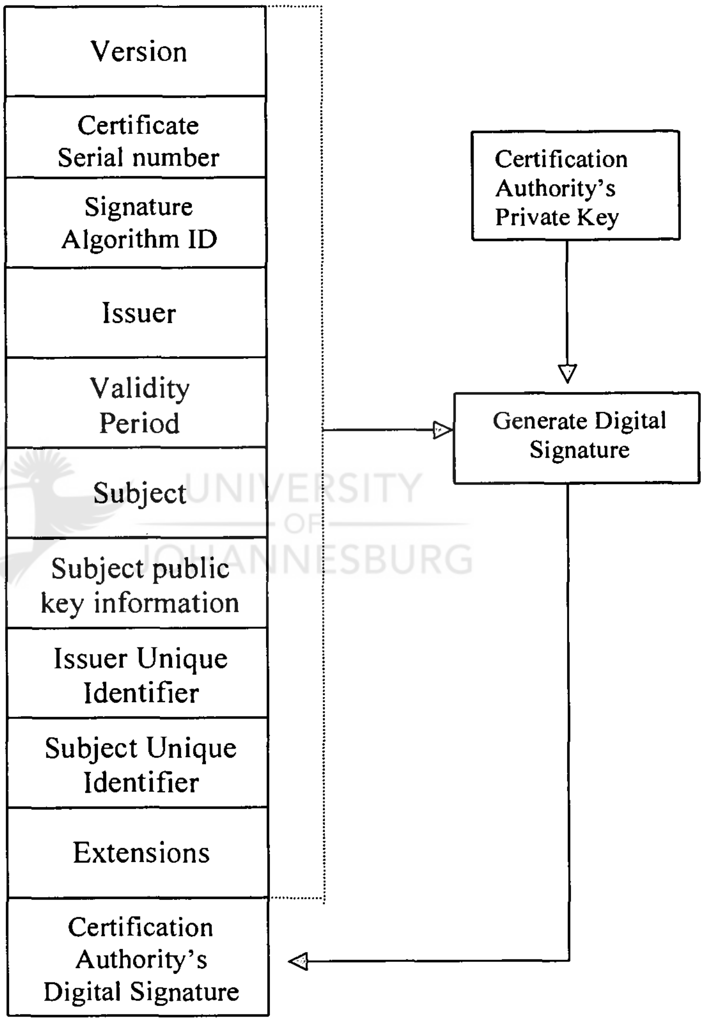

Version
Certificate Serial number
Signature Algorithm ID
Issuer
Validity Period
Subject
Subject public key information
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Certification Authority's Digital Signature
Certification Authority's Private Key
Generate Digital Signature

Figure 3.5 X.509 v3 Certificate format (Feghhi, et al: 1999:67)

From an audit point of view, the following fields in figure 3.5 are of importance:

- Version – Legal values are 1, 2 and 3;
- Certificate Serial number – A Certificate Authority assigns a unique serial number to every certificate issued;
- Issuer – Identifies the certification authority who has signed and issued the certificate;
- Validity period – Consists of the dates on which the certificate becomes valid as well as the date on which the certificate expires;
- Subject name – Identifies the entity whose public key is certified in the subject public key information field (Feghhi, et al. 1999:66 – 68).

3.7.1 CERTIFICATE RENEWAL

When a certificate expires, a new certificate needs to be issued in order to continue to offer X.509 v3-based services. The authority that issues the certificate determines when it will expire. Currently certification authorities are issuing certificates that expire one year after the date on which they are signed. This one-year period is needed for the following reasons:

- The longer a certificate is used, the greater the chances are that the private key will be compromised; and
- Due to the rapid improvements in technology, a secure certificate signed today might be unsecure in two years (Garfinkel, et al. 1997:140-141).

3.7.2 CERTIFICATE REVOCATION LISTS (CRLs)

According to Feghhi (1999:74-75), certificate revocation lists are published by certificate authorities, and they distribute information about revoked certificates to certificate-using applications. A certificate revocation list contains the date and time of publication of the list, the name of the issuing certificate authority and the serial numbers of all the revoked certificates that have not yet expired.

As indicated in figure 3.4, every certificate has a validity period, during which time any certificate-using application that uses that certificate may rely on that certificate to be valid. During this validity period, the issuing certification authority maintains information about the status of the certificate. This information is provided to the certificate-using application (Feghhi, et al. 1999:74).

The revocation status of a certificate is the single most important field of data that a certification authority maintains about the status of a certificate. The revocation status of a certificate indicates that the scheduled validity period as indicated in the "Validity period" field has been terminated prematurely (Feghhi, et al.1999:75).

A certificate can be revoked by a certificate authority for a variety of reasons, such as a compromise of either the issuing certificate authorities or the subscriber's private key. (Feghhi, et al.1999:75).

3.8 FIREWALLS

A firewall is a computer that runs a specially written or modified operating system. This computer isolates the internal network from the Internet at large. The firewall serves as a choke point, and all the access from and to the network must be routed through the firewall, allowing only specific connections to pass through while blocking others (Garfinkel, et al.1997:20).

The implementation of firewalls has grown dramatically during the past two years, from thirty-two percent in 1996 to eight-two percent in 1998. At the forefront of firewall implementation are the e-commerce leaders (Mayo, 1999:105).

Firewall proxies can control access to both the Internet and the internal network by evaluating a set of rules, also known as packet filtering rules, for each connection attempt to a network. These rules must specify which types of network traffic are permitted on either side of the firewall i.e. from where connections are allowed, and to which machines connections are permitted. If a connection request is dropped when it does not meet the defined rules, malicious attacks can be stopped before they reach the commerce server (Ghosh, et al. 1998:212).

A firewall serves multiple purposes:

- It restricts connections to enter at a carefully controlled point;
- It prevents attackers from getting close to your other defences; and
- It restricts connections to leave at a carefully-controlled point (Young, 1997:24).

No research was done on the configuring of firewalls and on setting packet filtering rules, as research in this area has already been done by Young and are assumed to be correct (Young, 1997).

3.9 SECURING THE COMMERCE SERVER

The following question may come to mind: "Why bother with securing the web server if you have secure transaction protocols?" This question is answered by Ghosh (1998:23). "The security of the system is only as strong as its weakest link".

Ghosh (1998:157-160) goes on to explain that critical information is stored on the commerce server. This can include company-critical data that can lead to a loss of consumer confidence if compromised. Another concern is denial-of-service (DNS) attacks. This is when an attacker succeeds in bringing down a server so that the server is not able to respond to requests.

The commerce server is a particular set of extensions to a basic HTTP server designed to meet the specific needs of electronic commerce. It consists of a network server and software to conduct secure commerce and communications on the Internet. As indicated in figure 3.6, the software includes a Web server, a mail server, an FTP server, a news server, a remote login server and the necessary supporting software.

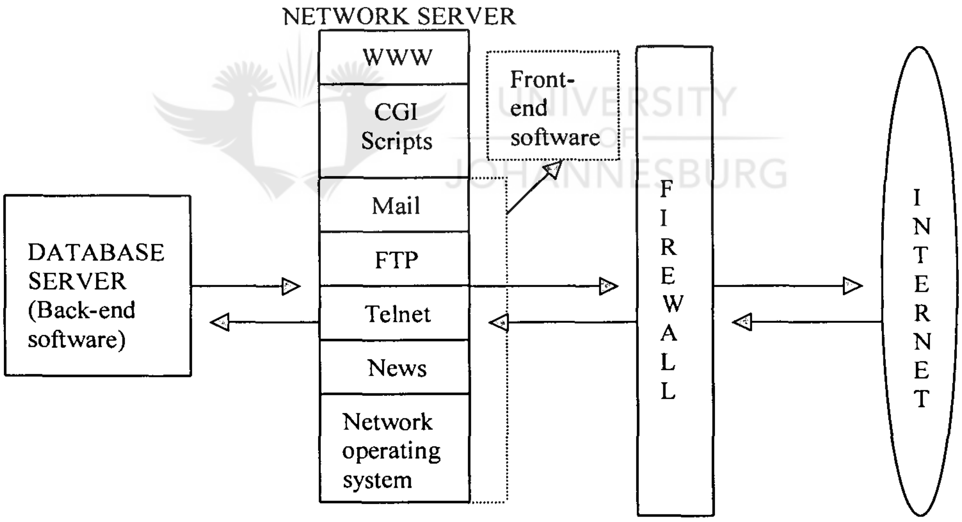


Figure 3.6 Components of a commerce server (Ghosh, et al. 1998: 159)

The back-end software normally consists of a database(s) where:

- Transactions are recorded;
- Accounts are kept up to date;

- Credit card numbers are stored; and
- An inventory of products is kept.

It is important for the commerce server to be the only one that can access these databases and that no one, who is accessing the commerce site, can initiate any queries of their own.

3.10 RISKS WITH RESPECT TO THE COMMERCE SERVER

Interpreters, shells, scripting engines and other extensible programs should never appear in a *cgi-bin* directory or, for that matter, anywhere else on a computer where they might be invoked when the commerce server receives a request. The *bin* directory usually contains programs considered necessary to keep the system functional, and in this case these would be cgi scripts in the *cgi-bin* directory. Unfortunately, many commerce servers are by default configured with scripting engines and other extensible programs in the *cgi-bin* directory (Garfinkel, et al. 1998:294) (Ball & Smoogen, 1998:314).

3.10.1 Common Gateway Interface (CGI) Scripts

CGI scripts are programs that are being run on the commerce server in response to a request that the commerce server received. CGI scripts are used for retrieving information, performing online Web site searches and for updating back-end databases. Scripting languages, such as Perl, makes it quick and easy to write CGI scripts. The disadvantage is that it is just as easy to program potentially dangerous system commands that can be executed in response to Web input (Garfinkel, et al. 1997:294).

3.10.2 Application Programmer Interfaces (APIs)

APIs are a new way of extending Web servers. With APIs the web server processes itself, and runs an application code within its own address space. Therefore it does not require that a new process be started for every new web request or interaction (Garfinkel, et al. 1997:293).

3.10.3 Services to be minimized

The Web server and other network servers such as mail, a file transfer protocol, news and remote login services form part of the front-end server software as indicated in table 3.3. Every Web server does not necessarily require mail, a file transfer protocol and news services, but the server provides these services because they are started by default. Providing network services on every available port can open up major security holes in a system, therefore increasing risk (Garfinkel, et al.1997: 268).

3.10.4 Access control to the commerce server

3.10.4.1 Hidden URLs

According to Garfinkel (1997:276), an easy way of restricting access to information and services is to make use of hidden and unpublished uniform resource locators (URLs) to store CGI scripts and HTML files although this is not very secure.

The reason for this is quite obvious: the URL is hidden only to the users who do not know about the hidden URLs. By making use of web "spiders", it is easy to expose these hidden URLs.

Services to be restricted	**Reason**
Domain name System (DNS)	Bugs in DNS implementation can be used to compromise a Web server.
Mail (SMTP)	Bugs in sendmail and other mailers can be used to break into a computer system.
Finger	Finger can be used to obtain information about a computer system that can be used to launch other attacks.
Netstat, systat	Netstat and systat can reveal a system's configuration and usage patterns.
Chargen, echo	These services can be used to launch data-driven attacks and denial-of-service attacks.
FTP	The standard FTP sends user-names and passwords without encryption, opening up to attack, accounts accessed by FTP.
Berkeley "r" commands	These commands use IP addresses for authentication and should be disabled.

Table 3.3 Services to be restricted on a server (Garfinkel, et al. 1997:268)

Web "spiders" are programs that scan all the pages on a Web server for keywords, compiling a database of these keywords. The hidden URLs are exposed when there is a link from the database indexed by the spider to the hidden URL.

3.10.4.2 Host-based restrictions

By specifying IP addresses or DNS host names, it is possible to restrict access to a commerce server, allowing only those IP addresses and DNS host names specified to access the commerce server (Garfinkel, et al. 1997:277).

3.10.4.3 Identity-based Access Controls

The most popular and common way of restricting access to a commerce server is by making use of user names and passwords. The problem with passwords and user names is that they are often shared among users, compromising security. An alternative to passwords nowadays is smart cards or public key certificates. Smart cards require that the user should be in possession of a card in order to gain access (Garfinkel, et al. 1997:279).

3.11 SECURING THE OPERATING SYSTEM

Vulnerabilities in the operating system form one of the biggest risks in securing the operating system. A firewall erected between the commerce server and the Internet is essential in preventing security break-ins through vulnerabilities in the operating system (Ghosh, 1998:210).

To eliminate these vulnerabilities, system administrators must regularly visit bug track-lists such as *Bugtraq.com.* By visiting bug track-lists, system administrators will be aware of flaws in the software and therefore be able to defend against attacks aimed at exploiting these flaws (Ghosh, 1998:248).

3.11.1 Logging

Log files record all system events from regular logins to attempts to break in. Log files will reveal how an attacker broke in, but only if the log file is not deleted or altered by the attacker. It is essential that a secure log server be set up. This log server should neither offer any services to the network nor allow any user accounts. These log files need to be monitored and audited on a regular basis to identify potential break-in attempts (Garfinkel, 1997:266).

3.12 CONCLUSION

The Internet today is a vast frontier of unknown elements, including new types of software, new discoveries of security flaws and unfriendly users. The most secure technical solution to preventing attacks launched from the Internet is to unplug the network from the computer. Besides the fact that this solution is not viable in today's business climate, it is not really a solution either. The components that comprise e-commerce systems should rather be adequately secured.

The path of an electronic transaction has been explained along with the technologies that are used to secure these transactions. Two protocols have been identified for securing data in transit, namely SSL and SET.

A secure communication protocol like SSL can be used to secure e-commerce transactions. Although this protocol can authenticate both users in a transaction and provide privacy, it does not provide protocols for payment. It is therefore crucial that the SSL protocol be used in conjunction with the SET protocol.

Firewalls are not directly responsible for securing e-commerce transactions, but they do play an indirect role in securing e-commerce transactions and are therefore an essential part of the e-commerce access path as set out in figure 1.1.

Based on this chapter, in which all the technologies involved with e-commerce have been explained, a check-list will be compiled as set out in chapter four.

CHAPTER 4

CHECK-LIST FOR VALIDITY IN E-COMMERCE

CONTENTS PAGE

4.1 INTRODUCTION

Now that the path of an e-commerce transaction and the technologies involved in e-commerce have been clearly defined and explained, a check-list will be compiled around these technologies to assist the auditor with the control objective of validity.

4.2 OBJECTIVE

The objective of this chapter is to compile a check-list subject to the provisos that the systems being audited are making use of:

- The SET protocol;
- The SSL protocol;
- Firewall technology; and
- Digital certificates

However, if the systems that are being audited are not making use of the SET protocol, the following should be kept in mind. Credit card numbers might be handled differently where the SET protocol is not used. Therefore, attention should be given to the following:

- Does the system store credit card numbers on the consumer's computer? If the answer is yes, the next question should be: are they stored in encrypted form? If not, then they should be encrypted.
- Does the system store credit card numbers on the commerce server? Unless recurring charges are expected, credit card numbers should not be stored on the server and those numbers that are stored on the server should be encrypted.
- Are stored credit card numbers purged from the system after the transactions have been completed? If a transaction is not recurring,

the numbers should be removed to avoid the risk of billing a customer for a second time accidentally or intentionally by an employee.

4.3 CHECKLIST FOR VALIDITY IN E-COMMERCE

This check-list will help the auditor in evaluating the validity of e-commerce transactions. Table 4.1 starts of by explaining what to check. The next three columns indicates whether this was checked or not. The last column refers back to chapter three where the technology was explained.

	YES	NO	N/A	Ref. to Chapter 3
4.3.1 SECURITY POLICY Obtain a copy of the latest security policy from management and check the following (the policy should specify at least the following): ○ Who is allowed access, what is the nature of the access and who authorises such access? ○ Who is responsible for security, upgrades and maintenance, and what is the regularity of upgrades and maintenance? ○ What types of material are allowed on served pages? ○ Which sites and external users are allowed to access the pages and data served? ○ What kind of testing and evaluation must be performed on new software and pages before they are installed? ○ How are complaints and requests about the server and web page content handled? ○ How does management react to security incidents? ○ When and how is the policy itself updated?				3.3

4.3.2 SECURE ELECTRONIC TRANSACTIONS (SET)

	YES	NO	N/A	Ref. to Chapter 3
By way of enquiries and observation, determine whether the criteria specified in the security policy are met. Report any non-compliance with the security policy to management.				3.5
4.3.2.1 SET COMPLIANCE TESTING				
○ Enquire directly from SETCo if the merchant is authorised to use the SETMark; and ○ Obtain the latest SET test software from SETCo and run these tests. Complete the SET check-list. Send the results to the SCA for evaluation and await the final evaluation from SETCo.				
4.3.3 SECURE SOCKETS LAYER				3.6
For a Web server to make use of SSL, a server certificate must be installed on the Web server. Check that a server certificate has been installed and verify the certificate information:				
Open Explorer/Netscape on the Web/Commerce server.				
4.3.3.1 Internet Explorer 5.x				
○ Click on **Tools**; ○ Click on **Internet Options**; ○ Click on the **Content** Tab; ○ Click on **Certificates;** ○ Click on **Personal** Tab ○ Select the certificate and double click;				

	YES	NO	N/A	Ref. to Chapter 3
○ Click on the **Details** Tab; and Check that the details in every field correspond to your knowledge of the merchant's Web site.				
4.3.3.2 Netscape 4.x ○ Double click on the lock at the bottom of the browser window; ○ Click on **Certificates**; ○ Click on **Yours**; ○ Select the certificate and **View**; and ○ Check that the information as per certificate corresponds to your knowledge of the merchant's Web site.				
4.3.3.3 Backup certificates ○ Confirm that the certificate has been backed up; ○ Import the backup certificate into a browser on a different computer; ○ Confirm that the certificate is password protected; ○ View the certificate and check that the certificate information corresponds to the information of the certificate on the Web server; and ○ Delete the certificate again after comparing it to the certificate on the Web server.				
4.3.3.4Alert Messages ○ Check log files for any of the alert messages and the regularity thereof. Enquire at management as to the steps taken in response to these alerts if any exist.					**3.6.1**

Ref. to Chapter 3

YES NO N/A

4.3.4 Ecryption 3.6.2

On the auditor's computer acting as a client

Open Internet Explorer/Netscape and make a connection to the merchant's Web site via an ISP and initiate a transaction with the Web site.

4.3.4.1 Internet Explorer 5.x

Double click on the yellow lock at the bottom of the browser window.

- Confirm that the information in the certificate corresponds to your knowledge of the Web site

4.3.4.2 Netscape 4.x

Check that the lock at the bottom of the browser window is closed.

- Double click on the lock;
- Click on **Security Info**;
- Click on **View certificate**; and
- Confirm that the information in the certificate corresponds to your knowledge of the merchant.

4.3.5 Certificate Revocation Lists 3.7.2

- Request a certificate revocation list directly from the certificate authority that issued the Web server's certificate. Check the revocation list and ensure the certificate does not appear on the list; and

	YES	NO	N/A	Ref. to Chapter 3
○ If the certificate appears on the list, enquire from management as to the reason for this.				
4.3.6 Digital Envelope				**3.6.4**
On the auditor's computer acting as a client				
○ Create a test message;				
○ By making use of RSA's symmetric key encryption, generate a secret key;				
○ Use this key to encrypt the message;				
○ Use the merchant's public key to encrypt this secret key;				
○ Make use of MD5 and compute a message digest for the message;				
○ Message digest command: MD5 <*filename1*> <*filename2*> <*filename1*> = Name of file for which to compute message digest <filename2> = Name of file where to save the message digest				
○ Encrypt this message digest with your own private key; and				
○ E-mail the encrypted message digest, the encrypted message and the encrypted secret key to the merchant.				
On the merchant's computer				
○ Using the backup certificate, decrypt the encrypted secret key;				
○ Use this key to decrypt the encrypted message;				
○ Decrypt the message digest using your own public key;				
○ Re-compute the message digest for the message and compare it to the message digest received;				

	YES	NO	N/A	Ref. to Chapter 3
○ Select an audit sample of messages received and re-compute the message digest for each message. If differences are computed by MD5 enquire about this from management; and				
○ If no differences are found, enquire from management whether any differences in comparing message digests were detected by them and the regularity of differences if they occurred and the procedures followed in response to these differences.				
4.3.7 Digital certificate				
○ Enquire directly from the Certificate Authority who issued the certificate that they are indeed the issuer of the certificate to the merchant.				
4.3.8 Securing the commerce server				**3.9 & 3.10**
○ Check the *cgi/bin* directory for any shells, scripting engines or extensible programs;				
○ Enquire from management as to the services provided by the Web server and if they are all required;				
○ Use a web spider to check for hidden URLs on the Web server;				
○ Check if IP addresses and DNS hostnames have been specified.				
○ If so try accessing the Web server from an unspecified IP address or DNS hostname; and				
○ Try accessing the Web server by using fictitious user names and passwords.				

	YES	NO	N/A	Ref. to Chapter 3
4.3.9 Securing the operating system ○ Inspect the log files for any attempted break-ins and the regularity thereof; ○ Check the log server and ensure it does not support any user accounts or any other services to the commerce server; and ○ Visit the operating system vendor's web site for information on new patches or service packs released to fix the security problems found. Check to see that the current version of the software running on the merchant's web server corresponds to the latest version available from the vendor's web site.				**3.11**

Table 4.1 Check-list for securing validity in e-commerce

With respect to 3.8 – Firewalls, refer to research done by Young (1997:73) chapter five – Audit Guidelines.

4.4 CONCLUSION

A check-list was compiled to serve as a framework in helping the auditor to assess the level of control risk. By making use of the above check-list, the auditor will be able to determine the overall validity of transactions. In the author's opinion, the objective of this chapter has been achieved.

CHAPTER FIVE

CONCLUSION

CONTENTS PAGE

5.1 INTRODUCTION

There is no "silver bullet" solution when it comes to securing e-commerce transactions. All software components involved in handling e-commerce transactions over the Internet/WWW must be equally secured.

As Ghosh states (1998:23): "The security of the system is only as strong as its weakest link". It is therefore imperative to focus on these weak links (risk areas) when evaluating an e-commerce system.

5.2 OBJECTIVES REACHED

The objectives of this short dissertation, as set out in chapter one, have been met, in that the risks and risk areas that arise from conducting business via the Internet and the World Wide Web have been identified, and that a check-list was compiled as set out in chapter four of this short dissertation.

5.3 NEW AREAS FOR RESEARCH

Further research may be undertaken in the area of e-commerce where the focus is placed on the e-commerce client as opposed to the e-commerce merchant as discussed in this short dissertation.

New research may be undertaken to address the issue of auditing an e-commerce merchant/client and the effect on the entire audit process, from the planning of an audit to the finalising of an audit.

5.4 CONCLUSION

To secure an e-commerce system, four areas must be addressed: Web client security, data in transit security, Web/Commerce server security and security of the operating system. Much of the attention that has been paid to Web security has involved the problem of protecting information from unauthorised interception as it travels the Internet. In this regard, two protocols were identified: the SET protocol and the SSL protocol. SET secures the payment information by making use of cryptography where as SSL provides a secure channel between the Web client and the Web server, preventing any eavesdropping and securing the order information.

Technologies used in e-commerce are developing at a phenomenal rate. As a result of these developments in technology, secure today might be insecure tomorrow. The auditor therefore needs to keep abreast of the newest technologies, as they become available and to adapt these new technologies into the check-list as set out in chapter four. In an e-commerce environment, the auditor must make use of technology to audit technology. This can be done only by keeping up with new developments in the IT industry.

BIBLIOGRAPHY

ANON. 1999: Security eases e-commerce fears: F&T Net, 3(4) July 1999: 28-30.

BALDWIN, RW & CHANG, CV 1997: Locking the e-safe: IEEE Spectrum, 14(2) February 1997: 40-47.

BALL, B & SMOOGEN, S 1998: Teach yourself linux in 24 hours; Indianapolis, Indiana: SAMS Publishing.

BIERER, D 1994: Inside NetWare 4.1; Indianapolis: New Riders Publishing.

BOSSHOFF, WH 1990: A Path context model for computer security phenomena in potentially non-secure environments; Johannesburg, D.Comm. thesis.

DREW, GN 1998: Using SET for secure electronic commerce; Upper Saddle River: Prentice Hall PTR.

ELLISON, C 1999: Heavy traffic of e-commerce; VARbusiness, 2(1), March 1999: 103.

ERNST & YOUNG 1997: 1997 1st Annual global information security Survey.

FEGHHI, J; FEGHHI, J & WILLIAMS, P 1999: Digital certificates applied internet security; Massachusetts: Addison Wesley Longman.

GARFINKEL, S & SPAFFORD, G 1997: Web commerce & security; United States of America: O'Reilly & Associates.

GHOSH, AK 1998: E-commerce security; New York: John Wiley &Sons.

JENKINS, B; COOKE, P & QUEST, P 1992: An audit approach to computers; Great Britain: Clays Limited.

KAMTAN,P 1999: E-commerce on the WWW – A matter of trust. http://www.irt.org/articles/commerce.htm

LOSHIN, P 1997: TCP/IP clearly explained; London: Academic Press Limited.

MAYO, D 1999: Internet security – involved with e-commerce?; VARbusiness, 2(1), March 1999: 105.

PRICE WATERHOUSE 1998: 1998 Technology forecast.

PRICEWATERHOUSECOOPERS 1999: 1999 Technology forecast.

ROBERTSON, JC 1993: Auditing, United States of America: Richard D. Irwin INC.

SAICA (South African Institute of Chartered Accountants).(1996): SAAS 400, Risk Assessments and Internal Control. July 1996. The South African Institute of Chartered Accountants.

SAICA (South African Institute of Chartered Accountants).(1998): SAAS 4012, Computer Assisited Audit Techniques. April 1998. The South African Institute of Chartered Accountants.

SET SECURE ELECTRONIC TRANSACTIONS LLC 1999: http://www.setco.org/downloads/set_bk1.zip

WATNE, D & TURNEY, PB 1984: Auditing EDP systems, New Jersey: Prentice-Hall.

YOUNG, BC 1997: Auditing validity on the Internet with specific reference to firewalls, Johannesburg: Rand Afrikaans University, M.Comm. dissertation.