Security Enhanced Direct Store Delivery System

Nitin Devikar and Yuliang Zheng
Department of Computer Science
University of Wollongong
Wollongong, NSW 2522, AUSTRALIA

September 2, 1999

Abstract

Currently there is limited security provided in carrying out business using Electronic Data Interchange (EDI). The aim of this paper is to enhance the security of Direct Store Delivery System which is a special form of EDI. The whole communication process is carried out using a trusted third party service provider with a view to maximize the performance of the system. The model describes authenticity using X.500 recommendations, confidentiality and integrity using public key cryptography and provides a low cost solution to the existing system. The transactions are carried out in the UN/EDIFACT format using the X.435 standards.

1 Introduction

The primary purpose of EDI is to provide communication standards that promote the interchange of common business information to facilitate the electronic linkages without human intervention. In recent years, both public and private sectors use EDI for trading purposes. The increasing use of EDI in financial transactions has made it necessary to consider network security in greater detail and enhance the security in these systems. The following issues need to be raised in view of security of the existing EDI systems [13].

- There is limited security in most of the present day EDI systems. They rely on password to access the system thus making it vulnerable to password guessing attacks.
- As more and more business information is transmitted between computer systems, we need to protect these transactions from unauthorized viewing and/or alteration. Unauthorized viewing can provide competitive information which we may not want to disclose. With the introduction of third parties and increased risk of unauthorized access to confidential information, we need to restructure the existing security features.
- Generally, EDI systems work on a point to point basis or have limited number of trading partners. The security and control features incorporated in the system is as strong as the weakest link in the EDI chain. A cross-vulnerability resulting from technical limitation can compromise the integrity of the dependent EDI systems.
- Different security standards may create problems when trading partners are adhering to different standards.
- The security features needs to be upgraded as the complexity grows.

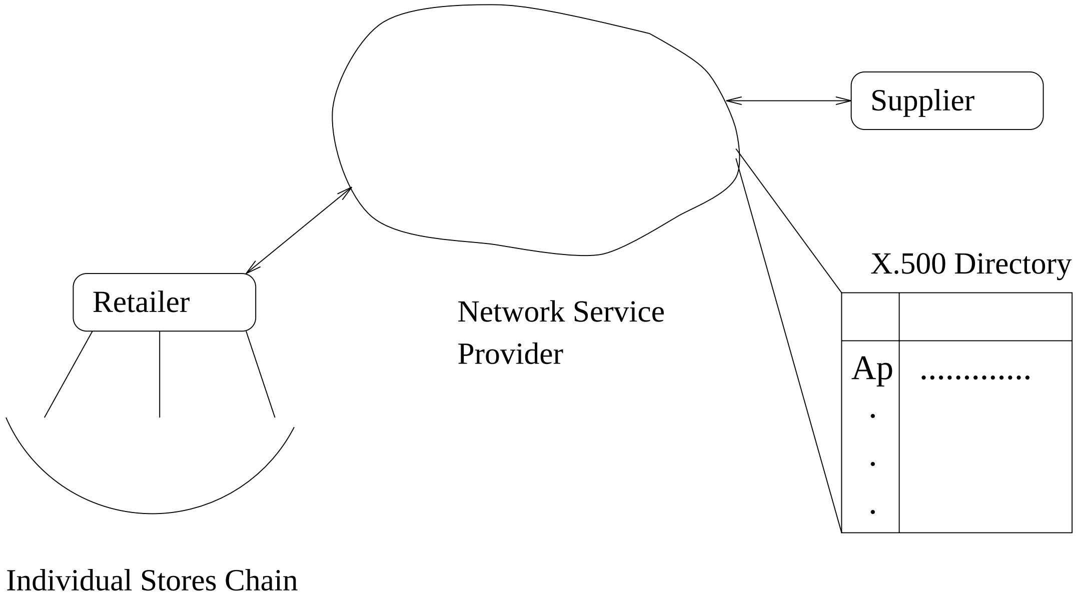

Figure 1: Direct Store Delivery System

is paper describes security enhancement of **Direct Store Delivery System** which uses a Trusted Third Party Service Provider or Value Added Network (VAN) over a network as shown in the figure 1 with a view to maximize the performance of the system. It provides a low cost security solution to the existing EDI applications. We use X.500 standards based on the Directory Services for resolving the address issues and mutual authentication based on the principal global identity [15]. The whole transaction in the model is carried out using the UN/EDIFACT format of transactions.

Section 2 provides the background on the concepts used in the model, section 3 describes the Direct Store Delivery System model and the security features provided and section 4 summarizes the paper with the gains in implementing the model and scope for further work.

2 Concepts and Mechanisms

The primary goal of any system is to carry out transactions in an open and secure fashion either on a point to point basis or on a public data network. However, in networked and distributed environments, what particular users are allowed to do depend upon the security policies in effect. Within a single domain where all processing nodes and network links are under the control of the same administration, security is not such a critical issue. However, when the transaction takes place between two separate domains and make use of public data networks, security issues must be considered in great detail. A trusted third party network provider provides some security functions like trusted key issuers, key-management facilities, user registration, notary services and security gateways.

2.1 Security Issues

Following are some of the network security issues which need to be considered for secure communication.

- Authentication

Authentication is a process used to:

- verify the identity of the sender of a message to the receiver to detect spoofing or impersonation.
- verify the integrity of the message by detecting changes (modifications) in a message introduced between the sending and receiving process.
- protect a unique message identifier used to detect attempts at insertion, deletion or replay of messages.

Most of the above threats can be countered by using strong authentication. In this, neither the entity which is authenticated nor any eavesdropper on the conversation can furnish the ability to impersonate the authenticating principal. There are some interception attacks which cannot be countered by strong authentication only. Hence, additional data encryption is needed to secure the channel. The well known cryptosystems are RSA [1] using public key techniques and DES, LOKI using symmetric key techniques. RSA is widely preferred algorithm for digital signatures as well as for authentication with secrecy.

- Key Distribution and Management

  Secure methods of key management are extremely important. In practice, most attacks on the public key systems are probably aimed at the key management levels, rather than at the cryptographic algorithm itself. Users must obtain a key pair securely and efficiently suited to their security needs. In compliance with the CCITT X.500 standards the directories contain certificates as well as the public keys. Certificates are unforgeable. Hence it is difficult to impersonate another user.

- Non-Repudiation of Origin and Receipt

  Non-repudiation of origin protects the recipient from the sender's denial of having ever sent the message, while non-repudiation of receipt protects the sender of the message from the receiver's denial of having received the message. Protection can be achieved by the sender including the digital signature with the message and the receiver sending the acknowledgment which contains the digital signature. In the protocol, the identity of the user is binded with the public key by digital signature by issuing certificates. The proof of delivery is done by the appropriate User Agent when it receives the message.

- Security Elements in EDI Messaging Structure

  The word envelope is used to represent different headers and trailers structured to form the EDI message as shown in figure 2. The UN/EDIFACT standard provides the following features:

  - the employment of established security mechanisms
  - security services to be implemented by trading partners themselves, end to end and transparent to the underlying communication protocols, which may themselves provide security services
  - independence of and transparent to the communication medium used
  - an open standard which supports all existing security mechanisms

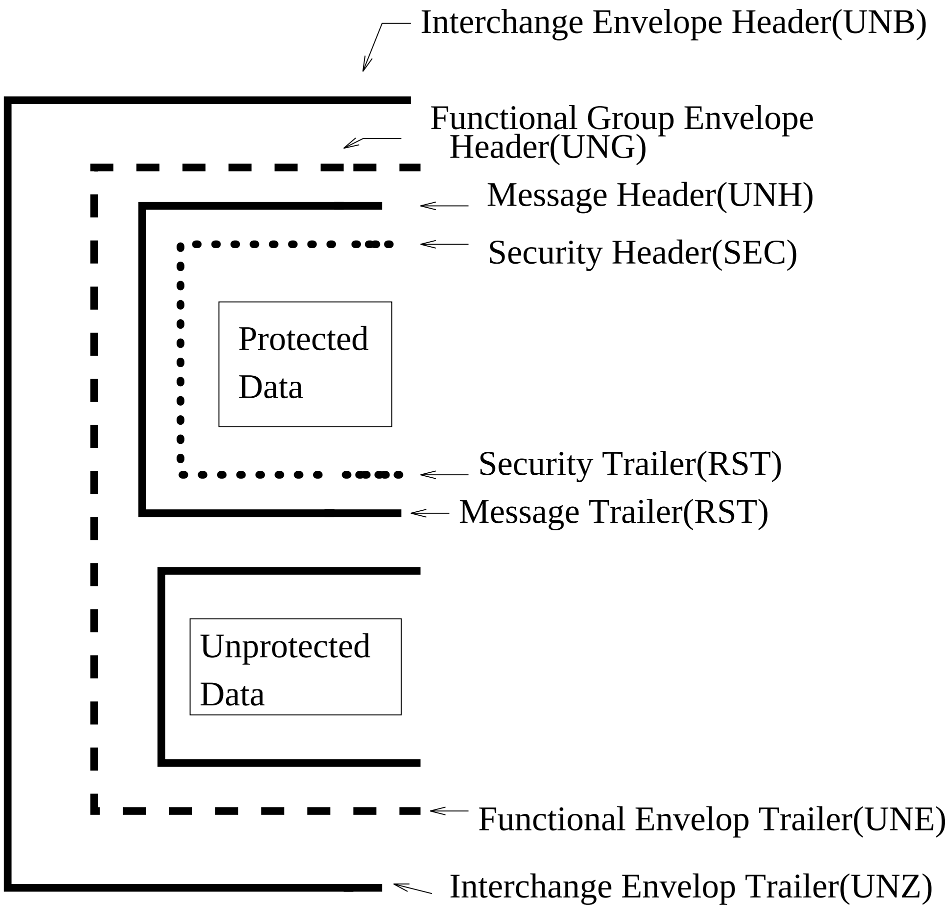
Interchange Envelope Header(UNB)
Functional Group Envelope Header(UNG)
Message Header(UNH)
Security Header(SEC)
Protected Data
Security Trailer(RST)
Message Trailer(RST)
Unprotected Data
Functional Envelop Trailer(UNE)
Interchange Envelop Trailer(UNZ)

Figure 2: UN/EDIFACT message format

  - not involving changes to individual messages. A global approach is adopted which can be applied to any message irrespective of the business application.

  All security functions except the non-repudiation of receipt are provided by the inclusion of generic security header and trailer segments after the message header (UNH) and before the message trailer(UNT). If required a financial transactions can use more than one security envelopes.

- Responsibility

  Another important feature that is incorporated is the responsibility for messages at each stage of the message path through the Message Handling System environment [16]. Since a Trusted Third Party is used, the transfer of responsibility is to be clearly identified and assured of further protection not only to the end users but also to the service provider. In the X.435 standard, the Responsibility Forwarded field is used to indicate whether Responsibility was forwarded or not. When responsibility is accepted, the security elements are checked.

- User Authorization and Access Control

  Authorization is an identity based access control for authorizing a particular user to carry out transactions. A simple way of doing this is to send the distinguished name and the password and the Directory confirms whether the credentials are valid. The user is then notified accordingly. The proper functioning of the logical access control assists in preventing and detecting (by reporting security violations and attempts to access) unauthorized access to data.

2.2 The Directory

The Directory Services is required to support the security services within the message handling system and provide a name server. Typically, the MHS may access the Directory to determine the credentials of a user for the authentication process, identify the intended receiver and to resolve the address issues. The two basic entities of the Directory Service are the Directory User Agent and the Directory Service Agent.

Each user's public key is stored in the Directory and a user wishing to have a secure exchange of messages with another user obtain the other user's public key using the Directory Services. He then uses this key within the required security service. The directory should be secured against tampering. Users are allowed to view and query the database and only the Certification Authority is allowed to modify an entry in the directory.

The security services can be provided by different layers and different protocols depending on the application requirements. The approach is based on the following functions:

- identification of the vulnerabilities of the system
- definition of security services
- placement of the security services in the particular protocol.

3 The System Model

The Direct Store Delivery System [10] is a chain of stores where ordering and deliveries are carried out centrally and the chain handles the distribution to the individual stores. It uses

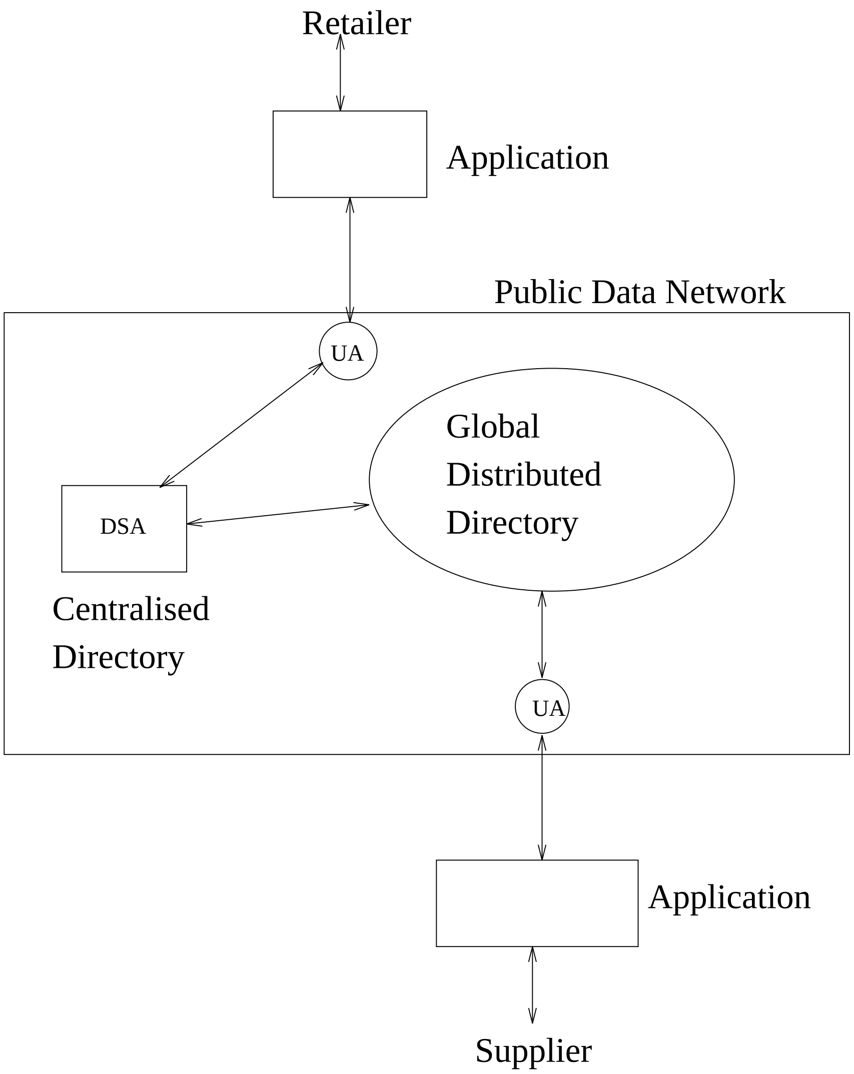

Figure 3: Functional Model of Direct Store Delivery System

EDI to place bulk order on the suppliers telling him how much to deliver and when. Thus the retailers continue to get the benefit of centralized ordering and like Just-In-Time stock management reduces inventory and saves on warehouses and material handling costs. The merchandise can be ordered faster and given item is never out of stock. At the same time there is increased vulnerability to illegal access with the use of public data network and trusted third party.

The system consists of User Agent and Message Store in the messaging environment modeled as a functional object as shown in figure 3. The whole transaction process can be divided into independent processes:

- Service Initiation → Initiation process starts with the retailer logging into the network through the access units User Agents.
- Verification of Public key of the trading partner → The user can verify the public key of the trading partner from the database query and get the appropriate certificate from the directory database.

- Generation of the Session key for transactions → Once the authentication of the trading partners has taken place then they can generate a session key to encrypt the subsequent traffic on the association.
- Trading : After completing all the above processes, the user can carry out transactions. The transaction generated is dumped into the mail box of the supplier who processes it and sends an appropriate response to the request. The auditing of the whole process is done by the third party and the user keeps a copy of the log of the transactions.

The security requirements are related to the user's perceived threats and his assessment of the cost of the security breach. Keeping this in view, the following generic security services are added to the direct store delivery system.

3.1 Basic Security Services

The message consists of two parts, namely an Envelope and a Content. The Envelope contains the necessary information for routing and delivering purposes and the Content contains the actual information which is to be transferred.

3.1.1 User Authorization

For using the services the user has first to identify his credentials to the server. Once the credentials are established, the user can use the services to either query the database or carry out other transactions. The user, after entering the name, is prompted for a password which consists of the user's name, a one-way hash of the password, a timestamp and a nonce which is returned to the user to be used. To prevent the hash of the password and the nonce from being intercepted over the network, they are encrypted using the public key of the CA. If the one way hash of the password from the database matches with that of the user, the CA returns the nonce encrypted with the public key of the originator.

3.1.2 Key Management

The RSA public key system is used to exchange the DES keys. The public key of the receiving User Agent is used to encrypt the DES key employed in the message encryption. The sending User Agent transfers this encrypted DES key to the receiving UA. The X.509 Directory Authentication framework is used for the authentication of the public keys of the users.

3.1.3 Authentication Protocol

As discussed earlier, the provision of the three services : Message Origin Authentication, Content Integrity and Non-Repudiation of Origin are grouped together.

The message-origin-authentication service is provided by the existence of message token which contains a signature which uniquely identifies the origin of the message. However, this does not guarantee that there has been no modification of the message. To achieve this, the *content integrity check* is included in the signed data part of the token.

The receiver obtains the trusted copy of the public key from the CA of the sender. If the CAs of the sender and the receiver are different, the receiver uses the certification path that has been supplied as part of the originator's certificate, to determine the copy of the receiver CA's public key. Using this, the receiver validates the signature on the originator certificate.

The Protocol

The protocol is slight modification of the existing X.509 Directory mutual authentication protocol [6].

step 1

The exchange between the two parties A and B with A sending message to the Authentication Server AS (in this application the Third Party) to find the public key of B [2]. This is done by looking up into the database of the Directory.

$$A \rightarrow AS : A.B$$

Step 2.

$$AS \rightarrow A : D_1.D_2$$

where $D_1 = D(k^s_{AS}, A.k^p_a.t_1.t_2)$
$D_2 = D(k^s_{AS}, B.k^p_b.t^{'}_1.t^{'}_2)$,
$t_1, t^{'}_1$ are timestamps, $t_2, t^{'}_2$ are the lifetime of the corresponding keys and . indicates concatenation. In order to sign data, the user applies a one-way hash function to the data followed by his digital signature (private transformation) D. The timestamps are needed to guard against the replay attack [3]. An intruder is not able to replace the messages in the previous steps since he does not have the secret key of the AS.

Step 3.

$A \rightarrow B : D_1.R_A.B.data^1_a.E(k^p_b, data^2_a).D(k^s_a,$
$h(R_A.B.data^1_a.E(k^p_b, data^2_a)))$

where R_A is nonce chosen by A, h is strong one way hash function, $data^1_a$ is the plaintext data which they sign to preserve the integrity and $data^2_a$ is the secret data to be exchanged between the two principals A and B.

step 4.

$B \rightarrow A : R_B.A.R_A.data^1_b.E(k^p_a, data^2_b).$
$D(k^s_b.h(R_B.A.R_A.data^1_b.E(k^p_a, data^2_b)))$

where R_B is nonce generated by B, $data^1_b$ is the plaintext data and $data^2_b$ is the secret data to be exchanged.

step 5.

$A \rightarrow B : R_B.D(k^s_a.h(R_B, B))$

Thus at the end of the protocol, both the users are convinced that they are communicating with the right person. The above authentication process safeguards the integrity as well as confidentiality of the message. The users can then generate a session key which is used to encrypt the subsequent traffic on the association.

3.1.4 Non-Repudiation of Delivery

The sender of the message requests this service from the receiver by including a proof-of-delivery-request flag as a part of the signed-data in the message token to the receiver. The proof-of-delivery is computed as a signature on the unencrypted message-content and the various other parameters. The receiver then returns the proof-of-delivery together with his certificate to the sender of the message.

3.1.5 Access Control Mechanisms

In this paper we will consider the access control between a User Agent and its corresponding Message Store. This is achieved by using another type of token called a *bind-token* which is exchanged between the UA and the MS at the time of connection initiation. The token includes information as signed data and time which is checked by the MS to determine if it is valid. The token signature is computed using the UA's secret RSA key. The MS then returns the token to the UA which makes further checks and if all these checks are satisfied, then the connection can be established. The token from the MS to the UA is signed which implies the MS to have its own RSA pair [9, 17].

3.1.6 Message Loss

Vulnerability to the message loss is considered critical to the EDI application. The types of message loss can be distinguished as :

- failure of the UA or MS
- loss of individual message due to security violations.

So the transfer of messages between responsibility domains requires protection for service providers in addition to that of end users.

4 Summary

This paper specifies a model for a secure direct store delivery system. It is straightforward model which provides a high degree of security in a cost effective manner and has many desirable features. Particularly, if the third party provides the directory services, then electronic transactions can be carried out with reasonable degree of security over the network. It relieves the user from burden of maintenance, upgradation of the system and expansion to other networks. Furthermore, once the user authentication is complete, all security features of the direct store delivery system will be transparent to the user.

The system makes no assumptions about the reliability of the underlying network. The data is transmitted in an encrypted form to ensure that even a third party cannot extract any information enroute. For this appropriate end-to-end encryption must be provided to counter traffic analysis.

Acknowledgments

We would like to thank the anonymous referees for ACSC'95 for their helpful comments. The second author was supported in part by ARC A49232172, ATERB N069/412 and a University of Wollongong Research Program grant.

References

[1] R. Rivest, A. Shamir and Adleman. A Method for obtaining digital signatures and public key crypto-systems, *Communications of the ACM*, Vol. 21, no. 2, pp 102-126, 1978.

[2] R. Needham and M. Schroeder. Using Encryption for authentication in large network of computers, *Communications of the ACM*, Vol. 21, no.12, pp 993-999, 1978.

[3] D. Denning and G. Sacco. Timestamps in Key Distributed Protocols, *Communication of the ACM*, vol 24, no 8, pp 533-535, 1981.

[4] J. Tardo and K. Alagappan. SPX: Global Authentication Using Public Key Certificates, *IEEE Symposium on Research in Security and Privacy*, pp 232-244, 1991.

[5] B. Jerman-Blazic. Security in Value Added Networks, Security Requirements for EDI, *SBT/IEE International Telecommunication Symposium*, pp 361-365, 1990.

[6] M. Toussiant. Analyzing Security of Cryptographic Protocols, *IEEE Journal on Selected Areas in Communications*, Vol. 11, No. 5, pp 702-714, 1993.

[7] G. Dickson and A. Lloyd. *OSI*, Prentice Hall of Australia Pty Limited, ISBN 0-13-640111-2, pp 279-283,303-307, 1992.

[8] C. Mitchell and A. Thomas. Standardizing Authentication Protocols Based on Public-Key Techniques, *Journal of Computer Security*, pp 23-36, 1993

[9] C. Mitchell, D. Rush and M. Walker. A Secure Messaging Architecture Implementing the X.400, 1988 Security Features, *The Computer Journal*, Vol 33, No. 4, pp 290-295, 1990.

[10] P. O'Grady. *Putting the Just-In-Time Philosophy into Practice*, Kogan Page Limited, London, ISBN 1 85091 121 5, 1988.

[11] S. Kent. Internet Privacy Enhanced mail, *Communication of the ACM*, vol 36, No. 8, pp 48-60, 1993.

[12] D. Gaon, K. Eller, W. Free and F. Ogden. Concept of Implementing A Globally Distributed X.500-Based DoD Directory, *MILCOM'92 Communication -Fusing Comand, Control and Intelligence Conference Record*, pp 1195-1199, 1992.

[13] A. Marcella and S. Chan. *EDI Security, Control and Audit*, Artech House, 1993.

[14] D. O'Mahony. Security Considerations in a Network Management Environment,*IEEE Network*, pp 12-17, 1994

[15] Information Processing Systems - Open Systems Interconnection - *The Directory Authentication Framework*. ISO/IEC 9594-8:1993, also CCITT 1988 Recommendation X.509.

[16] CCITT Recommendations Message Handling Systems : *Electronic Data Interchange Messaging System Recommendations X.435*, 1991.

[17] V. Varadharajan. Security in a Distributed Message Handling System , *IEE Colloquium on 'Message Handling - Past, Present and Future'*, pp 5/1-9, 1991.

[18] *C.C.I.T.T. Draft Recommendations X.400, Message Handling Systems - System and Services Overview*, Version 5.5, April 1988.

[19] M. Purser. *Secure Data Networking*, Artech House Inc. , MA, 1993.

[20] W. Ford. *Computer Communications Security : Principles, Standard Protocols and Techniques*, Prentice Hall Ltd, NJ ,1994.

[21] S. Muftic(et al.) *Security Architectures for Open Distributed Systems*, John Wiley and Sons., UK, 1993.

[22] *Electronic Data Interchange : Streamlining Business Communications*, Computer Technology Research Corporation, USA, 1993.

[23] P. Swatman. Integrating Electronic Data Interchange into Existing Organisational Structure and Internal Application Systems: the Australian Experience, Phd thesis , 1993.

[24] G. Simmons. *Contemporary Cryptology : The Science of Information Integrity*, IEEE Press New York, 1992.

[25] J. Barkley. Security in Open Systems, *NIST Special Publication 800-7*, Computer Systems Technology, US Department of Commerce, NIST, October 1994.

[26] C. Mitchell, D. Rush and M. Walker *CCITT/ISO Standards for Secure Message Handling*, IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, pp 517-524, 1989.

[27] C. Mitchell and C. I'Anson. Security Defects in CCITT Recommendations X.509 – The Directory Authentication Framework, *Computer Communication Review*, vol 20, no. 2, April 1990, pp 30-34.

[28] C. Pfleeger. *Security in Computing*, Prentice Hall International Inc.,NJ, 1989.

[29] J. Steiner, C. Neuman and J. Schiller. Kerberos : An Authentication Service for Open Network Systems, *Proceedings of USENIX Winter Conference*, pp 191-202, February 1988.

[30] M. Burrows, M. Abadi and R. Needham. A Logic of Authentication, *Research Report 39*, Digital Systems Research Center, Palo Alto, California, A condensed version of this report appeared in *ACM Transactions on Computer Systems*, Volume 8, No. 1, pp 18-36, February 1990., February 1990.

[31] J. Cobb *Security Implications in Electronic Data Interchange* IEE Colloquium on 'Standards and Practices in Electronic Data Interchange' (Digest No. 106), pp 7/1-4, 1991.

[32] Security Issues in the use of Electronic Data Interchanges, *CSL Bulletin* from the site http://www.csl.nist.gov, June 1991.

[33] B. Schneier. *Applied Cryptography : Protocols, Algorithms and Source Code in C*, John Wiley and Sons, New York, 1994.

[34] S. Bellovin and M. Merritt. Limitations of the Kerberos Authentication System, *Proceedings of USENIX Winter Conference*, pp 1-16, 1991.

[35] V. Voydock and S. Kent. Security Mechanisms in High-Level Network Protocols, *ACM Computer Surveys*, 15(2), pp 135-171, June 1983.

[36] J. Berge. *EDIFACT Standards*, NCC Blackwell Limited, 1991.

[37] B. Di Turi. Security in EDIFACT Messages, *Computers and Security*, vol 12, No. 5, pp 447-455, August 1993.

[38] T. Dosdale. Security in EDIFACT Systems, *Computer Communications Magazine*, vol 17, No. 7, pp 532-537, July 1994.

[39] Recommendations for UN/EDIFACT Message Level Security, UN/EDIFACT WP.4 Document, R.1026 Add 1, 1994.

[40] D. Zazula. EDI-PRO : An Integrated Environment for Electronic Data Interchange, *Computer Communications Magazine*, vol 17, No. 12, pp 876-885, December 1994.

[41] EDIFACT - Application Level Syntax Rules, ISO-9735, ISO, Geneva, Switzerland, 1988.

[42] W. Caelli, D. Longley and M. Shain *Information Security Handbook*, MacMillan Publishers Ltd., UK, 1991.

[43] D. Gerberick. Working Paper on Functional Specifications for an EDI Cryptoserver, *Security Audit and Control Review*, pp 11-19, Summer 1991.

[44] W. Pugsley. Electronic Data Interchange - An Overview, *Proceedings of the International HP Users Conference*, Brussels, paper BU/OA/09, 1989.

[45] D. Coppersmith. Analysis of ISO/CCITT Document X.509 Annex D, IBM Research Division, Yorktown Heights, June 1989.

[46] C. Schuba and E. Spafford. Addressing Weaknesses in the Domain Name System Protocol, MS Thesis, Purdue University, USA, August 1993.

[47] J. Zoreda. *Smart Cards*, Artech House, Boston, USA, 1994.