FIFTH SESSION OF TRACK 2

An intelligent arbitrator associate for electronic commerce

Daniel W Manchala
Xerox Corporation
701 S. Aviation Blvd; ESAE-231
El Segundo, CA 90245, USA
e-mail: manchala@cp10.es.xerox.com

ABSTRACT

Growing businesses and the large number of transactions involved in conducting a business tend to give rise to conflicts among the parties involved in a transaction. Human society has evolved in a way to cope with these disputes by creating law and order bodies. An Intelligent Arbitrator Associate (IAA) that works with and helps the law enforcement and law adjudication authorities to resolve disputes that arise due to commerce conducted over the Internet is presented in this paper. The infrastructure over which the IAA operates, the architecture, and the protocols involved are described. Some of the architectural pieces include monitoring systems for copyright infringement and currency fraud, information extraction systems to predict and map crime, and access revocation systems to punish principals involved in illegitimate transactions. The IAA sends out intelligent agents with warrants to gather information from the various entities involved in the transaction. The social and legal issues and difficulties involved in deploying such systems into the real world are described in the paper.

Nomenclature

C, V, B, EN	Customer, Vendor, Bank, Electronic Notary
m	Electronic Goods
$\wp$	Payment
TID	Transaction Identification
T_{exp}	Expiration Time of Contract or Response
TS	Timestamp
VID	Vendor Identification
MD	Message Digest (MD5 or SHA), contents
k	Public Key
k^{-1}	Private Key
k_s	Session Key
( )	Message Digest performed on contents
{ }	Assymetric Cryptography performed on contents
[ ]	Symmetric Cryptography performed on contents

1. Background

1.1. *The Commerce Model*

In everyday commerce there are at least three important entities that are always involved in a transaction - the vendor who sells items, the customer who buys items and an intermediary that sits between the customer and the vendor. Intermediaries are economic agents that stand between the parties of contract or transaction (namely buyers and sellers), and perform functions necessary to the fulfillment of a contract. This simple commerce model can be extended to include commerce done electronically; for example, commerce done over the Internet has given rise to new types of intermediaries called electronic brokerages. Examples of electronic brokerages include information and payment brokerages, product brokerages, and retail brokerages [Kal95].

1.2. *Authentication, Authorization, and Electronic Payments*

One of the prime mechanisms for concluding a transaction is for payment of services or goods. In the world of electronic commerce, payments should be done securely, i.e. payments should be made so that none of the parties involved in the transactions are victims of commerce crime. Transactions are usually preceded by authenticating the parties, and by providing authorization proof (that a customer has sufficient credit in his account, or is authorized to conduct a certain transaction) to the respective parties in contract. Transactions conclude by an electronic payment for the services or goods delivered by the vendor to the customer.

1.3. *Law and Order Bodies*

Growing businesses and the large number of transactions involved for conducting businesses tend to give rise to conflicts among the parties involved in the transaction. Human society has evolved in a way so as to cope with these disputes by creating law and order bodies. These bodies include the law-making bodies, law-enforcing bodies, and law-adjudicating bodies. Whereas the law-making bodies are responsible for creating laws, the law-enforcing bodies ensure that laws are not broken and hence parties involved in unlawful activities are punished, and law-adjudicating bodies resolve disputes. In order to resolve disputes arising in the world of electronic commerce, new laws have to be created, breaches in law should be identified, and the guilty should be punished. An electronic commerce model including these bodies is shown in Figure 1.

2. Electronic Commerce Protocols and Disputes

Most electronic commerce protocols usually involve a customer, a vendor, and a bank. Protocols that involve trust and justification for disputes include a trusted third party and/or an electronic notary who keeps a signed document of the proceedings of transactions. In case of a dispute, an Intelligent Arbitrator Associate (IAA) works closely with the law adjudication authority to gather information, and would serve as a provider of legal knowledge.

2.1. *A Simple Electronic Commerce Protocol*

Almost all protocols make use of cryptographic primitives to express the kind of security involved in the transactions. Consider the simple electronic commerce protocol shown in Table 1. A transaction begins with the customer querying the vendor for the price of an item (for example a piece of software program) shown in step 1. The vendor replies with the price, a transaction ID, current time of the transaction TID, time until when the price remains effective T_{exp}, and a message digest of the item **MD**(m), all signed using the vendor's private key as shown in step 2. Steps 1 and 2 may iterate for a certain number of rounds as part of price and item negotiation before going to step 3. The vendor needs to sign all this information so that when a dispute arises, the vendor can prove that at the time when the purchase negotiation started (TS), for the item (TID), the price was indicated by *price*, and that the item was what was claimed it was (**MD**(m)), and that the price was valid for a certain period of time only (T_{exp}). This vendor-signed information is sent to the electronic notary for record keeping, along with a plain-text version of the transaction identification TID, vendor identification VID, and the vendor's public key as obtained as part of the negotiation in steps 1 & 2. This is shown in step 3. The customer pays the vendor in step 4 indicating the transaction for which he/she is paying (TID). The payment is of course encrypted using a symmetric key so that the vendor can decrypt it after delivering the goods in step 5, and receiving the symmetric key in step 6.

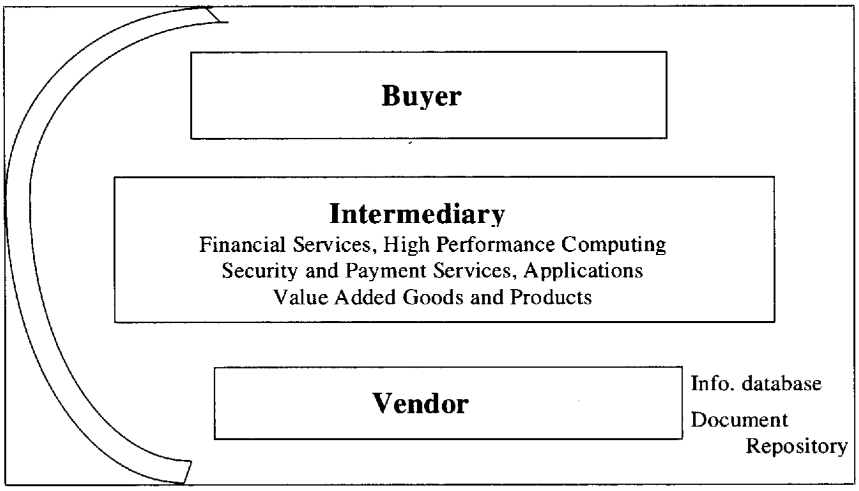
Buyer
Intermediary
Financial Services, High Performance Computing
Security and Payment Services, Applications
Value Added Goods and Products
Vendor
Info. database
Document
Repository

Figure 1. The Electronic Commerce Model

1.	C → V:	price-query, item of purchase
2.	V → C:	[*price*, TID, TS, T_{exp}, **MD**(m)] $v\text{-}k^{-1}$
3.	C → EN:	[*price*, TID, TS, T_{exp}, **MD**(m)] $v\text{-}k^{-1}$, TID, VID, $v\text{-}k$
4.	C → V:	$\{\wp\}c\text{-}k_s$, TID
5.	V → C:	m
6.	C → V:	$c\text{-}k_s$, TID

Table 1. A Simple Electronic Commerce Protocol Involving Customer, Vendor and Electronic Notary.

2.2. *The IAA in Electronic Commerce*

Figure 2 represents a typical electronic commerce model involving a customer, a vendor, an intermediary (an electronic notary), and the IAA. A dispute can arise when the customer is not satisfied with the transaction. For example, the purchased software item did not perform functions as it was claimed in the advertisement, but a later version had all the functions, etc. The customer complains to a judge about the injustice. The judge works with the arbitrator which sends an agent to the electronic notary, and queries it to obtain information relevant to the transaction. Agents may also be sent to the vendor, customer or electronic notaries and customers in other domains depending upon the information gathered from the electronic notary. The arbitrator reasons on the information and if it comes to a conclusion that a misdemeanor has been committed, it may advise the judge to impose sanctions against the vendor. The vendor may send other agents to restrict the suspect's ability to participate in electronic commerce or to revoke certain privileges. The power of the IAA to perform such things as revoking privileges should be granted by the government, or it could be a signed contract between the vendor, the customer and the arbitrator. This gives rise to legal concerns about the rights of an individual being constrained by the contract, since the geographical boundaries of the contract when spanning regions having different laws and digital evidence could easily be tampered with. Social concerns about the correctness of the arbitrator retrieving the correct evidence or the length of the contract that hinders people from reading and understanding the finer points may crop up as hindrances to the deployment of such systems.

In many cases where the reasoning of the IAA is questionable, the IAA would go through the reasoning process to justify its conclusion to the law adjudication authority. There may also be instances where certain disputes need further help from an expert. In such cases, where the knowledge base is incomplete, the IAA captures the expert's knowledge while the expert (a judge) proceeds with the judgment, or while the expert (legal consultant) advises on legal matters to the IAA. The process of adding knowledge could be done by question-answering (knowledge acquisition), by manually adding judgment proceedings from a certain case (so that it could be helpful in a similar case), or by closely monitored deduction and induction (machine learning).

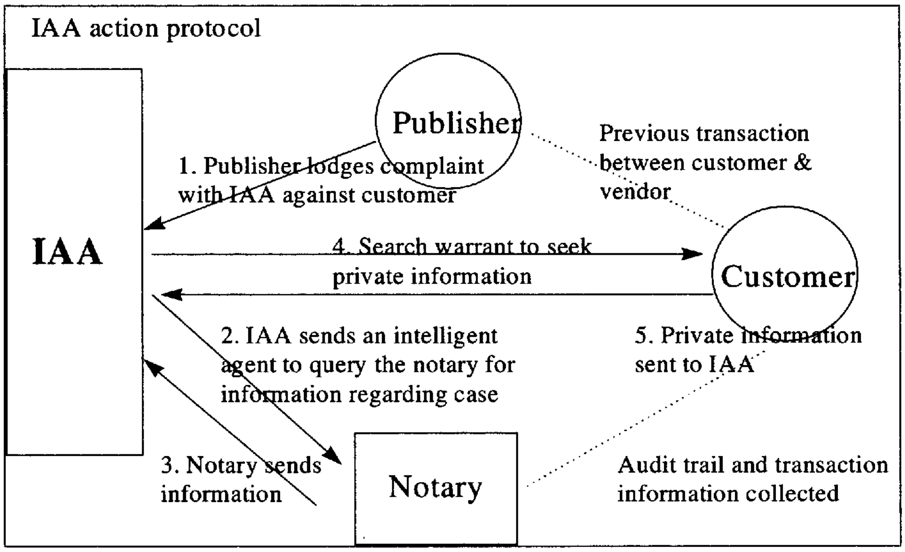
IAA action protocol
IAA
Publisher
1. Publisher lodges complaint with IAA against customer
Previous transaction between customer & vendor
4. Search warrant to seek private information
Customer
2. IAA sends an intelligent agent to query the notary for information regarding case
5. Private information sent to IAA
3. Notary sends information
Notary
Audit trail and transaction information collected

Figure 2. The Electronic Commerce Model with an Arbitrator Detailing Information Flow

3. Intelligent Agents and Search Warrants

In order for the IAA to conduct on-line searches, or merely get relevant information from electronic notaries, software agents that have the capability to route through the network, capture necessary information, and return this information to the IAA are introduced. Examples of such intelligent software agents that route themselves through the network, based on a certain node giving information on where else to gather information from, are manifested in the form of mobile agents [Lin95], [Sto96], or intelligent e-mail [Ric89]. These mobile agents also guarantee security. A software agent consists of a knowledge base, procedures and an encapsulating layer that contains routing and security information. Legal knowledge in the knowledge base can be represented using a variety of structures including rules and facts, atomically normalized form (ANF) [Deb86], object-oriented [Jac90], etc. Raghupathi [Rag92] discusses an expert system in the domain of 'product liability' using a blackboard architecture. Brouwer [Bro94] discuses various ways of representing legal knowledge by identifying certain characteristics of the legal domain. Bainbridge [Bai93] discusses broad methodologies for the construction of systems that will be of practical use and commercial viability, based on experience gained from building expert systems in the legal domain. To obtain confidential or private information, a *search warrant* is a carried by a software agent to conduct the authorized search. This software agent may also be called a *search agent.*

3.1. *Security and the Search Warrant*

In order that a proper, legal and reliable search be conducted, public key cryptographic techniques are used in the search process. This is important not only to prove to the principal under search that a legal search is being conducted, but also to avoid errors such agents may cause while interacting with other intelligent agents that perform real-time control functions. While it is possible to reduce the number of occurrences of such errors, it may be impossible to eliminate all of them, due to the non-deterministic network of interactions such agents make, while the need to authenticate or check for authorizations would sometimes be overlooked or not provided. A method of treating liabilities arising out of such interactions that would cause unpredictable decision-making errors can be covered using an insurance system [Kar96]. The search agent has the following in its security layer:

- A certificate from a certification authority to establish a means of authentication.
- A description of the search.
- Authorization information to gather information.

Certification authorities (CA) that provide certificates to conduct searches are appointed by the government. A certificate is usually represented in X.509 format [Cci93], and contains among other things information on the identity of the holder of the certificate, holder's public key and period of validity. Mutual authentication is then conducted between the search agent and the suspect's system. The search agent queries the system, and obtains information from it. This information is carried back to the IAA. The information is usually in encrypted form using a session key derived out of the authentication process.

A description of the search to be conducted is also contained in the security layer. This includes which database tables to search, the interval limits of the search, etc. The X.509 certificate also provides the authorization information. It is used as a capability [Sta95] that the information base at the suspect's end checks for authorization privileges.

4. Architecture of the IAA

The process of arbitration starts with the creation of intelligent agents when a complaint is received, and ends through the destruction of these agents after prosecution is delivered. In order to help in the process of arbitration, the arbitrator might need certain information about the crime and establishing the identity of the suspects. This information is usually obtained by inferring from previously gathered data from general network monitoring, and identifying certain patterns of suspicious movements in the way electronic commerce is conducted. The Information Extraction System (IES) monitors crime by reasoning on statistical data. This information is used to help predict locations and magnitude of crime that could occur in future, and could be used to prevent similar crimes from recurring. Punishing System or Rights Revocation System (RRS) come into play once it has been determined or established that a principal is suspected or has engaged in unlawful transactions.

4.1. *Information Gathering and Utilization*

Information Extraction System (IES): This system performs the following functions:

- *Identify Magnitude of Crime:* The severity of the crime and the urgency of the corrective action required triggers a level of alertness. This includes higher order transactions, and related transactions which when summed together would be a serious misdemeanor. For example, transferring funds greater than $10,000 out of the US should be reported on a tax form. People could transfer small amounts of money under different accounts owned by different persons, but who are connected as an illicit ring. A cognitive graph is constructed to create a network of related transaction movements by observing patterns of transaction flows. Such a graph identifies the illicit ring when cash flows involving huge amounts are sent to a common destination.
- *Measure Crime Hit Rate & Change*: Crime hit rate is the number of crimes committed by or against a host during a certain period of time. It is used to determine if the host needs to be shut down, protocols need to be changed, or any other preventive measures need to be taken. Crime in chunks of time intervals, each time interval covering a crime hit rate is used to create a crime hit spectrum. This is used to figure out if a suspect should be further prosecuted. For example, if the crime hit spectrum does not show signs of change despite checking (monitoring and controlling) the suspect, then the suspect may not have been involved in the crime and should be let out, or that the suspect is using different techniques to commit electronic commerce crimes.
- *Map the Nature of Crime:* The type and kind of crime also gives certain directions to apprehending and punishing the suspect. Different types of crimes include stealing digital currency, capturing credit card numbers, impersonation, intruding into a database to alter information, willfully giving wrong identification information to delay payment, etc. Mapping the nature and magnitude of crime could help isolate certain regions. This is very helpful when someone has let loose a virus, worm or a trojan horse. The effects of the attack are seen over time, and help in warning principals/hosts in a region to be cautious against these types of attack.

Monitoring System (MS) This system performs the following functions:

- *Currency Fraud Monitoring:* The IAA keeps track of double spending of electronic cash and usage of electronic booster checks[1].
- *Intrusion Detection*: Security-related network events, by which intrusion attempts can be detected and tracked could be performed using monitoring tools or intrusion detection

[1] A credit card holder (with the help of an agent) issues checks (called "booster checks" because the value of the check when deposited by the credit card agency usually increases the credit card limit severalfold) to temporarily increase the credit limit, and goes on a spending spree before the (hot) check is cleared by the bank. The card holder makes all his purchases and later seeks bankruptcy. By law, all credit card companies and agencies should post the amount as soon as a check is received from the card holder, and before it clears the bank.

systems (IDS). Examples of IDS include MIDAS [Seb88], IDES [Lun90a], NIDES [And94], NADIR [Hoc93] and DIDS [Sna91].

- *Copyright Infringement:* Whenever a piece of authorship work is extracted to be embedded in another work, without prior approval from the authors or publishers, the watermark (softmark) gets copied along with the extracted/copied work. Examples of such watermarking methods and tools include Xerox DataGlyphs and SysCop [Zhao 97]. These tools use spread spectrum techniques like direct sequence or frequency hopping. When this new work is submitted as an original piece, the copyright infringement monitoring system identifies parts of the work as non-original and without copyright approval. Works with embedded copyrighted material, but which has received copyright approval have necessary approval signatures on their watermarks.

Rights Revocation System (RRS)

- *Quarantine Observation*: Agents monitor network traffic for fraudulent currency disposition, or copyright infringement. A suspect is kept under quarantine observation until it has been established that the principal is innocent.
- *Change Access Rights*: Certain access rights are restricted or new electronic currency is not issued. Sometimes, an electronic legal notice (signed by the arbitrator) would be sent to the principal, and a copy to the communication service provider to disconnect the principal from the computer network.
- *Service Blockers*: Service blocking agents watch for certain transactions and block them from coming in to the principal or going out from the principal.

The extent to which an RRS system (through a system operator) can limit access of users to certain services (like the bulletin board service) is debated (with regards to the free speech act) in Bovenzi [Bov96]. A catch and punish model has been suggested in [Ket95] for use along with an electronic payment system.

5. Copyright Management

5.1. *The Copyrighted Work*

A softmark is embedded into the copyrighted work that contains the author's work. Copyright information includes author's name, publisher's name and address, information stating whether it is a derived or original work (in the former case, the original author's information is also included), copyright fees, author's or publisher's public keys. All this information is signed by the publisher's private key. Thus, the ability to modify this information (the softmark) is held only by the publisher. The entire copyrighted work is encrypted by the vendor's session key. The customer is furnished with session key for the current document as part of the authentication/authorization exchange. Figure 3 shows an electronic publishing model.

5.2. *Payment of copyrighted fees*

The steps involved in the process of payment of copyright fees is as follows:

1. Newly created work is sent from the author to the vendor/publisher.
2. Publishers add/modify the softmark by adding a stamp of approval (digital signature). Only publishers (or the original authors themselves) can modify the softmark since it is encrypted using the publisher's private key.

3. Principal A's work along with the new softmark is sent back to Principal A who could sell it.
4. This entire procedure can be recorded by an electronic notary (a copyright office or a patent office).

5.3. *Copyright infringement*

Consider the case when Principal A decides not to pay copyright fees, but wishes to sell the derivative work or a copy of the original as his original work (plagiarism). The copyright infringement monitoring system described above would identify infringement by decrypting the softmark, and comparing the information with that of the original authors and publishers.

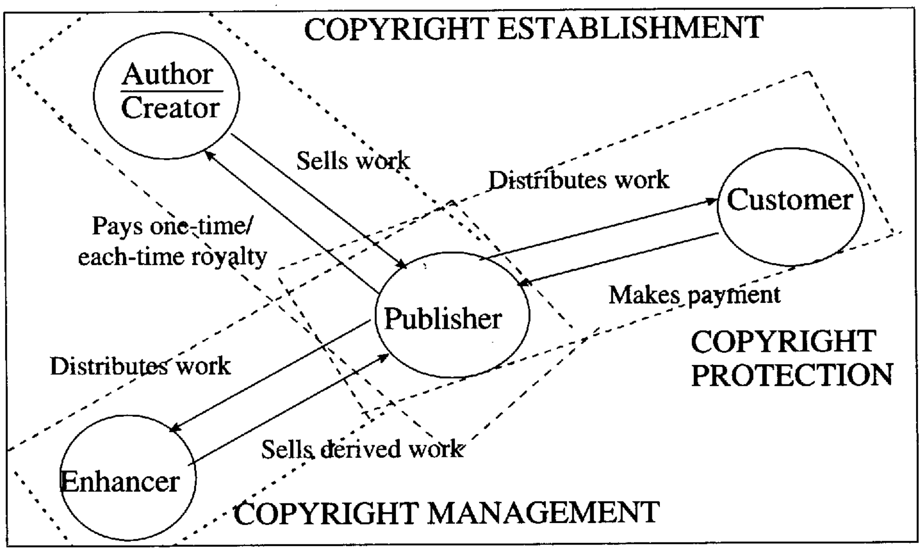

Figure 3. Electronic Publishing Model

6. Conclusion

This paper introduces an IAA that works with the law adjudication authority. The IAA is an expert system with a knowledge base consisting of rules elaborating the ethics for conducting commerce electronically, regulations that would improve the integrity of transactions, captured knowledge based on previous cases to help identify culprits, extrapolaters to help detect movement of crime, and rules to determine the amount of punishment necessary for a determined culprit, etc. The policing function of the IAA is performed by sending a software agent along with a search warrant to quiz the suspect (customer or vendor) on various legal issues like payment of dues, payment of copyright fees, compromising others authentication and authorization information, general information for increasing credit limits, etc. This audit information is carried back to the policing unit of the IAA. The IAA uses expert system techniques to determine if the capabilities of the suspect should be revoked. As the system is being put into use, we can see the knowledge base growing, with the ability to extract more complex information.

References

[And94] Anderson D *et al*, Next Generation Intrusion Detection Expert System (NIDES), Software Design, Product Specification and Version Description Document, Project 3131, SRI Intl. July 11, 1994.

[Bai93] Bainbridge D I; Expert Systems in Law: Practice and Problems, *International Journal of Applied Expert Systems*; Vol 1, No. 1, 1993.

[Bov96] Bovenzi G, Liabilities of System Operators on the Internet; *Berkeley Technology Law Journal,* Vol. 11, No. 1, Spring 1996.

[Bro94] Brouwer P W; Legal Knowledge Representation in the Perspective of Legal Theory; in H Prakken, A J Muntjewerff & A Soeteman (eds). *Legal Knowledge Based Systems: Jurix '94: The relation with Legal Theory*, Lelystad: Kininklijke Vermande, pp. 9-18, 1994.

[Cci93] The Directory - Authentication Framework; CCITT Recommendation X.509, 1988; revised 1993.

[Deb86] Debessonet C G and Cross G R, An Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information; *High Technology Law Journal*, Vol. 1, No. 2, Fall 1986.

[Hoc93] Hochberg J et. Al., NADIR: An Automated System for Detecting Network Intrusion and Misuse, *Computers and Security*, vol. 12, No. 3pp. 235-248, May 1993.

[Jac90] Jackson P, *An Introduction to Expert Systems*, Addison Wiley, Wokingham, England, Second Edition, 1990.

[Kal95] Kalakota R; Organizing for Electronic Commerce; *Electronic Commerce Conference*, Austin, Tx; Oct 29 -31, 1995.

[Kar96] Karnow C. E, Liability for Distributed Artificial Intelligence; *Berkeley Technology Law Journal*, Vol. 11, No. 1, Spring 1996.

[Ket95] Ketchpel S; Transaction protection for information buyers and sellers; *Proceedings of the Dartmouth Institute for Advanced Graduate Studies '95: Electronic Publishing and the Information Superhighway*, 1995; Also available at http://robotics.stanford.edu/users/ketchpel/dags4.html

[Lin95] Lingnau A, Drobnik O, Doemel P; An HTTP-based Infrastructure for Mobile Agents, *Proc. of the 4th Intl. WWW Conf.*, O'Reilly & Assoc., Sebastopol, Calif., 1995, pp. 461-470.

[Lun90] Lunt T F et. Al, IDES: A Progress Report, *Proc. of the Sixth Annual Computer Security Conference*, Tucson, Az. Dec. 1990.

[Rag92] Raghupathi W and Schkade L; The SKADE LITorSET Expert System for Corporate 'Litigate or Settle' Decisions; *Intelligent Systems in Accounting, Finance and Management*; Vol. 1, pp. 247-249, 1992.

[Ric89] Richardson P W and Danielsen T, Intelligent Messages or When Messages Come Alive, in *Network Information Processing Systems*, Boyanov K and Angelinov R, eds., North Holland, New York, 1989.

[Seb88] Sebring M M, Shellhouse E, Hanna M E, and Whitehurst R A, Expert Systems in Intrusion Detection: A Case Study, *Proc. 11th National Computer Security Conference*, Baltimore, Oct. 1988, pp. 74-81.

[Sna91] Snapp S et. Al, DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype, Proc. 14th National Computer Security Conference, Washington D.C, Oct. 1991, pp. 167-176.

[Sta95] Stallings W, *Network and Internetwork Security - Principles and Practice*; Prentice Hall and IEEE Press, pp. 256, 1995.

[Sto96] Stone S et. al., Mobile Agents and Smart Networks for Distributed Simulations, *Proc. 14th Workshop on Standards Interoperability of Distributed Simulations*, Inst. for Simulation and Training, Orlando, Fla. 1996, pp. 909-917.

[Zha97] Zhao J; SysCoP *Digital Watermarking for Copyright Protection*; http://www.crcg.edu/syscop

Daniel Manchala is currently a member of the research and technology staff at Xerox Corporation, El Segundo, California, USA, where he has been working in the areas of Electronic Commerce and Digital Security. He obtained a PhD in Computer Science from Texas A&M University, USA, in 1995. His other interests include Vibration Control, Digital Watermarking and Distributed Computing. He is a member of IEEE and ACM.