Öneri.C.6.S.23.
Ocak 2005.ss.129-136.

E-COMMERCE AND SECURITY

Levent ERTAUL[1], Ayse AKYOL[2]

[1]California State University, Department of Math and Computer Science, PhD.
[2]Trakya Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yardımcı Doçent Dr.

E-COMMERCE and SECURITY

Abstract: ***E-commerce became an important tool used by the companies in order to communicate customers directly and satisfy their personalized needs and requirements. Although e-commerce and its importance are increasing rapidly, it is well behind its potential. The main reason of its slow development is the security. The ultimate success of e-commerce will depend, to great extent, on the interest and confidence of consumers. The issue of security is not an easy problem and there are no definitive solutions to it. There will always be a fierce computation between people trying to protect their assets and people trying to defeat these protections. This will be a never ending story.***
In this paper, direct marketing, online marketing and e-commerce are defined; security issues are addressed; the existing security technologies in e-commerce are reviewed and finally the paper are concluded with general discussion about the achievability of security in e-commerce.

Keywords: ***Direct Marketing, Online Marketing, E-Commerce, Security***

E-TİCARET ve GÜVENLİK

Özet: ***Müşteriler doğrudan iletişim kurmak, onların kişisel istek ve ihtiyaçlarını karşılamak için e-ticaret, şirketler tarafından kullanılan önemli bir araç haline gelmiştir. E-ticaret ve önemi hızla artmasına rağmen, gerçek potansiyelinin oldukça gerisindedir. Bu yavaş gelişimin en önemli nedeni "güvenlik"tir. E-ticaretin başarısı büyük ölçüde müşterilerin ilgi ve güvenine bağlı olacaktır. Güvenlik kolay bir sorun değildir ve kesin çözümleri de yoktur. Her zaman, şirket varlıklarını korumaya çalışan insanlar ile bunları yenmeye çalışan insanlar arasında bir mücadele olacaktır ve bu bitmeyen bir hikaye olacaktır.***
Bu makalede doğrudan pazarlama, online pazarlama ve e-ticaret tanımlanmış; güvenlik konuları belirtilmiş; varolan güvenlik teknolojileri incelenmiş ve makale e-ticarette gerçekleştirilebilecek güvenlik hakkında genel bir değerlendirme ile tamamlanmıştır.

Anahtar Kelimeler: ***Doğrudan Pazarlama, Online Pazarlama, E-Ticaret, Güvenlik***

I. INTRODUCTION

While information is booming, communication structure is becoming multi-channel and more complex, costumer needs and requirements are changing and diversifying ever so endlessly, technological advances, globalization and economical developments are changing the market place dramatically.

For customers, having information and making comparisons became very easy with technological advances, and customers became more aware and selective in an environment with many companies and many product variations. In this aspect, companies needed to adapt and follow the change by using customized marketing implementations and direct marketing to satisfy customer's personalized requirements and needs rather than implementing mass marketing for every customer.

Sweeping changes in connecting technologies (i.e. computer, information, communication, transportation) are reshaping business models and marketing practices in most industries and causing marketers to redefine how they connect with the marketplace – with their customers, with marketing partners inside and outside the company, and with the world around them. Beyond competing in traditional "marketplaces", company's now have access to exiting new "marketspaces". Therefore, "conduct commerce in marketplaces" became "conduct e-commerce in marketspaces" [1]. Therefore, e-commerce operations are increasing day by day. E-commerce became an important tool used by the companies in order to communicate customers directly and satisfy their personalized needs and requirements. Although e-commerce and its importance are increasing rapidly, it is well behind its potential. The main reason of its slow development is the security. The ultimate success of e-commerce will depend, to great extent, on the interest and confidence of consumers.

In this paper, direct marketing, online marketing and e-commerce will be defined; security issues will be addressed; the existing security technologies in e-commerce will be reviewed and finally the paper will be concluded with general discussion about the achievability of security in e-commerce.

II. DIRECT MARKETING

In old fashion way of marketing, "mass

marketing" practices were applied by targeting the whole market with standardized products, prices, promotions, and distributing them through intermediaries. However, in modern marketing, firms targeted customers by seeking profitable ones through carefull analysis and adopted "direct marketing" practices. Nowadays, companies are trying to communicate these carefully targeted customers more efficiently to build long term and stronger direct relationships with them.

The main direct marketing tools are:

- face to face selling,
- telemarketing,
- direct mail marketing,
- catalog marketing,
- direct response television marketing,
- kiosk marketing
- online marketing (and e-commerce)

The rise in accessibility of computer technology and the advancements in software technology allow the generation of personalised letters and messages has eased the task of direct marketing [2]. Online marketing is conducted through interactive online computer systems, which link consumers with sellers electronically. Altough still in their infancy, internet usage and online marketing are growing explosively [1].

III. ONLINE MARKETING and E-COMMERCE

Online marketing offers great promise for the future. Its most ardent apostles envision a time when the Internet and e-commerce will replace magazines, newspapers and even stores as sources of information and shopping. Yet despite all the hype and promise, online marketing may be years away from realizing its full potential [1]. New technologies create opportunities to segment and effectively target customers and it is expected that a large number of customers will shop online through wireless web, mobilephones, laptops, personal digital assistants (PDAs).

E-commerce is revolutionizing business transactions. In fact, e-commerce is changing the way businesses of all sizes operate in terms of their interaction with customers and suppliers. In addition, it is contended that the rapid adoption of e-commerce by many firms is also providing the catalyst for societal change [3].

The Department of Trade and Industry proposed the following e-commerce definition to the Organisation for Economic Cooperation and Development (OECD): "Using an electronic network to simplify and speed up all stages of the business process, from designing and making to buying, selling and delivery' e-commerce is the exchange of information across electronic networks, at any stage in the supply chain, whether within an organisation, between businesses, between businesses and consumers, or between the public and private sectors, whether paid or unpaid" [3]. The definition as agreed in the UN - CEFACT (United Nations Centre for Trade Facilitation and Electronic Business) ad hoc group for Electronic Commerce: "Electronic Commerce is doing business electronically. This includes the sharing of standardised unstructured or structured business information by any electronic means (such as electronic mail or messaging, World Wide Web technology, electronic bulletin boards, smart cards, electronic funds transfers, electronic data interchange, and automatic data capture technology) among suppliers, customers, governmental bodies and other partners in order to conduct and execute transactions in business, administrative and consumer activities".

The growth of the internet and the possibilities for consumers, suppliers and banks to create a new type of shopping has resulted in the evolution of the e-commerce and e–commerce applications. An e-commerce application may address one or several phases of typical business transactions such as in phase 1 merchant makes an offer for a specific goods or services. According to this offer, the customer may place an order in phase 2. In phases 3 and 4, the customer makes a payment and the merchant delivers the goods or services to the customer. The handling of payment may require third parties such as banks or acquirer gateways. In either case, disputes may occur and these disputes must be addresses in phase 5 [4-6].

In spite of the well-publicized successful e-commerce stories many businesses and customers are still cautious about participating in e-commerce and security concerns are often addressed as being the single most important barrier. Consumers still worry that snoopers will eavesdrop on their online transactions or intercept their credit card numbers and make unauthorized purchases. In turn, firms doing business online fear that others will use the Internet to invade their computer systems for the purposes of commercial espionage or even sabotage. Online marketers are developing solutions to such security problems. However, there appears to be an ongoing competition between the technology of internet security systems and the sophistication of those who are seeking to break them [1].

IV. SECURITY ISSUES IN E-COMMERCE

Security continues to be and probably will always be a problem. If you over look that, you are in trouble. It once used to be about insurance and now it has become a lifestyle.

Security on the internet works something like this old joke: Once there were two hunters in the deep forest. They had gone down to a nearby lake for some water, leaving their guns back at the campfire. A grizzly bear approached them rapidly, and after a frightening chase, fortunately the bear went on its way. Back at the camp, the first hunter asked the second hunter, "Why did you run? You know you can't outrun a grizzly". His friend replied, "I didn't need to outrun the grizzly, I just needed to outrun you". The analogy to internet security is that if someone wants to break into your system badly enough, he probably can. The key is to make it difficult enough that he chooses to go after someone else's system [7].

When today's e-commerce market is reviewed, an enormous variety of applications written in several languages running on top of different systems can be seen. Most of the applications work quite well, but it is hard to trust them since they lack strong security. There are different types of shortcomings in existing applications, among which:

- On the internet people cannot be sure of the other party's identity. Masquerading techniques pose a real problem since customers are not willing to spend money in stores they cannot trust (Authentication).
- The costumer does not want to reveal secret information to the rest of the world. Confidentiality must be necessary.
- Guaranteeing the integrity is necessary.
- There is no simple way of allowing or deniying access to certain resources in a system.
- Generation of proof of certain events is not possible.
- Storing sensitive information in a secure manner is not easy and adequate support is not always available [8].

In e-commerce and e-commerce applications there are four different issues as far as security is concern. These are:

- Client-side security issues
- Server-side security issues
- Transaction-side security issues
- Organizational and legal security issues

As it can be seen from the above issues that security requirements of e-commerce applications generally go beyond the more traditional requirements of network security [5,9-13].

IV.1. Client-side Security Issues

From the user's point of view, client-side security is the major concern. In general, client-side requires the use of traditional computer security technologies [4,6,9,11,14], such as:

- ***User authentication***: The authentication service is concerned with assuring that a communication is authentic. The function of authentication is to assure the recipient that the message is from the user that it claims to be. In other words these techniques allow server to verify that user is a legitimate user.
- ***User authorization***: The authorization service provides permission to access a resource.
- ***Access control***: The Access control service is a mechanism for limiting use of some resource to authorized users. It is the prevention of unauthorized use of a resource. These service controls, who can have access to a resource, under what condition access can occur, and what those accessing the resource are allowed to do.
- ***Anti-virus protection***: It provides protection against malicious codes (viruses, worms, Trojan horses etc).

With regard to communication services client may additionally require [4,6,9,11,14]

- ***Server authentication***: Client may require authentication of the server by using same techniques that are used in user authentication.
- ***Non-repudiation of receipt***: When a message is received, the sender can prove that the alleged receiver in fact received the message.
- ***Anonymity*** (anonymous browsing on the Web): It allows a principal to interact with others (in this case its Web browsing) without reveling ones true identity. The use of anonymity entails a responsibility to use wisely.

IV.2. Server-Side Security Issues

Server-side security is typically the major concern from the service provider's point of view. In general, server-side requires various security services [4,6,9,11,14,15] such as

- ***Client authentication***: These techniques allow server to verify that user is a legitimate user.
- ***Client authorization***: Authorization service

provides permission to access a resource for a legitimate user.

• ***Non-repudiation of origin***: It is a proof that the message was sent by the specified party. It actually provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

• ***Sender anonymity*** (anonymous publishing on the Web): Anonymity provides a shield to protect people from having to associate their identity with some data (in this case posting on the Web).

• ***Audit trial***: Auditing is the process of analyzing systems to determine what action took place and who performed them.

• ***Accountability***: It usually entails maintaining a log of security-relevant events that have occurred, listing each event and the person.

• ***Reliability***: It provides means that payment transactions occur either completely successful or not at all, but they never hang in an unknown or inconsistent state.

• ***Availability:*** Apart from needing to be secure, a server, in e-commerce, must be available and reliable. It must be available all the time, seven days a week, and 24 hours a day. It must also have some protection against denial-of-service (DoS) attacks, or at least be able to detect them early and start recovery procedures.

IV.3. Transaction Security Issues

Transaction security has kept many customers from purchasing on the internet. Much resistance has come from privacy issues and there are continual reminders of how unsafe these practices can be, even though "secure" software programs have been developed and continue to become more protective [16]. A prerequisite for the evolution of the electronic commerce is the existence of effective security mechanisms to protect commercial transactions. Consumers and providers of products and services are not expected to use widely e-commerce applications unless they are confident that electronic communications and transactions will be confidential, the origin of messages can be verified and the personal privacy can be protected. Personal privacy refers to all personal information including behaviour, communication and other personal data. One of the most important aspects of e-commerce is therefore the underlying secure payment scheme. Transaction security requires various security services [5,6,12,14,17] such as:

• strong data and user authentication, preferably based on X.509 certificates, digital signatures and personal smart cards

• privacy (confidentiality) of transactions using encryption

• transaction integrity using message digest algorithms

• non-repudiation to handle disputes about the transaction

• transaction anonymity guarantees

IV.4. Organizational and Legal Security Issues

The legal system has adapted quite well to computer technology by reusing some old forms of legal protection (copyrights and patents) and creating laws where no adequate one existed (malicious access). Law and computer security, in e-commerce, related in several ways. First international, federal, state and city laws can affect privacy and secrecy. These statues often apply to the rights of individuals to keep personal matters private. Second laws regulate the use, development, and owner ship of data and applications. Patents, copyrights, and trade secrets are legal devices to protect the rights of developers, and the owners of applications and data. Similarly, access control to data is supported by these mechanisms of law. Third, laws affect actions that can be taken to protect the secrecy, integrity and availability of computer information and services. However law does not always provide an adequate control. When e-commerce is concerned, the law is slowly evolving because e-commerce is a new thing, compared to houses, land or money. As a consequence, the place of e-commerce systems in law is not yet firmly established [14,17-19].

V. CURRENT E-COMMERCE SECURITY TECHNOLOGIES

E-Commerce is threatened by a wide variety of people, including criminal hackers, disgruntled employees or exemployees, competitors, terrorists, foreign agents, etc. The tools available to these parties have increased dramatically while the technological knowledge needed to use them has fallen. Moreover, the system is becoming more complex and interdependent, and therefore potentially more vulnerable. Because of their technical complexity, some of these dependencies may be unrecognized until a major failure occurs [20]. Existing security technologies for e-commerce will be addressed under the headings of Electronic Payment Security, Communication Security and Web security.

V.1. Electronic Payment Security

A secure payment scheme for electronic commerce must support strong authentication of each party, based on X.509 digital certificates, digital signatures and personal smart cards and also must provide confidentiality (privacy) of transactions by using strong encryptions. Along with the authentication and confidentiality, any payment system must provide transaction integrity. In addition to these, to avoid any conflicts among parties, non-repudiation (both source and destination) of transactions must be supported [5].

Substantial technical progress has been made in this area recent years. In Table 1 some existing electronic payment systems, which provide aforementioned services, are listed. Some of these schemes are more and some are less effective and popular but all of them are Internet based payment systems. The VISA\Master card SET system is having broad acceptance since it is very strong, comprehensive and effective system [6].

Table.1. Internet Based Electronic Payment Systems

Cybercash	IBM Electronic Commerce	Netscape	GC Tech
Checkfree	iPK Protocol	Netbank	Net Market
Digicash	Intuit	Mondex	Security First Networkbank FSB
Electronic Funds Clearing House	Netcheque	Sandia's Ecash system	VISA/MC SET

Source: Mavridis, I., Pangalos, G., Koukouvinos, T., & Muftic, S., A secure payment system for Electronic Commerce. www.infolab.gen.auth.gr/Phd/mavridis/DEXA99.pdf [5]

V.2. Communication Security

Communication security is provided by cryptographic security protocols in Networks. These protocols work on different layers of the network. Below crypto based security protocols which work at different network layers and used by e-commerce applications are given [6,14,17,18,21].

• **PAP**: Password authentication Protocol provides password security

• **CHAP**: Challenge-Handshake Authentication Protocol offers password security stronger then PAP

• **EAP**: Extensible Authentication Protocol is a general protocol for PPP authentication that supports CHAP

• **PPP**: Point-to point protocols provide secure access to remote host.

• **ECP**: Encryption Control Protocol protects confidentiality of data carried with PPP

• **MAC address filtering (Firewalls)**: Decides for each packet whether it should be forwarded or dropped at machine level.

• **IP address filtering (Firewalls)**: Decides for each packet whether it should be forwarded or dropped based on IP address.

• **IPSec**: IP Security provides Authentication, Confidentiality, Integrity and protection against replaying and IP spoofing attacks. It is basic protocols of Virtual Private Networks (VPN).

• **SOCKS**: provides a flexible framework for developing secure communications by easily integrating other security technologies. It also provides authentication and establishes a second connection to the required server.

• **SSL/TLS**: Secure Socket Layer/ Transport Layer Security Protocols provide data integrity, confidentiality and authentication. They are implemented in many Web browsers (Internet Explorer, Netscape). Many internet based e-commerce applications are based on these protocols.

• **SASL**: Simple Authentication and Security Layer is a mechanism to add authentication and authorization support to connection-oriented protocols

• **Application Gateways and Content Filters (Firewalls)**: control passing traffic through to host based on the content of the messages (checks malicious codes such as viruses, worms or specific patterns).

• **SSH**: Secure Shell helps to establish a secure connection to the network services or secure remote execution of commands

• **Secure TELNET**: provides authenticated and secured remote access

• **RADIUS**: Remote Authentication Dial in User Service provides authentication and authorization for dial in users.

• **TACACS +**: The Terminal Access Controller Access Control System provides a way to centrally validate users attempting to gain access to a router or access server.

• **S/MIME**: Secure/Multipurpose Internet Mail Extension provides authentication, integrity with digital signature and confidentiality to e-mail applications.

• **S-HTTP**: The Secure HyperText Transfer Protocol provides authentication, integrity and confidentiality to messages in WWW environments.

• **KERBEROS**: provides secure access control to

network resources.

All of these protocols have specific advantages and disadvantages [6,14,17,18,21], and all of them generally enable us to develop secure commercial transactions for a wide range of applications.

V.3. WEB Security

Web-based e-commerce applications are changing the way consumer buy goods and access information. These applications commonly employ or use the combination of technologies such as HTML (Hypertext Markup Language), XML (eXtensible Markup Language), JavaScript, Java (JSP (JavaServer Pages Technology), Servlets), ASP, dynamic html and CGI (Common Gateway Interface) [6,14,17,18,21].

The current e-commerce solutions utilize the web and represent a composition of diverse technologies:

• **User interface**: through html, xml, Java, JavaScript

• **Server Functions:** through dynamic html, JSP, ASP, J2EE, CGI or servlets

The real challenge here is to formulate secure impenetrable applications in light of the combinations of a variety technologies and capabilities because most of the above technologies are having some security problems. When they are used, a special attention must be paid other wise developed applications might have real!!! security problems [6,11,14,17,18,21].

VI. CONCLUSIONS

Traditional marketing concept differs from modern marketing in following points:

• In traditional marketing, companies largely focus on sales and products, tend to implement mass marketing practices by standard products, and they try to increase market growth, by finding new customers, via use of mass media for promotion.

• In modern marketing however, companies largely focus on customer and markets, tend to use marketing implementations onto carefully targeted customers, try to

- o develop long term relationship with existing customers as well as finding new ones,
- o establish connection with customers directly,
- o develop customized products to satisfy customer's personalized requirements / needs,
- o work with other organizations through strategic alliances.

These above changes can be seen easily when some of hot topics of marketing literature, such as database marketing, one-to-one marketing, relationship marketing, supply chain management, are looked into. All of these topics directly related to development of new technologies. The main reason of rapidly increased usage of e-commerce is that companies try to use available new technologies to implement and achieve modern marketing strategies. For example, customers specifications and their usage patterns can be determined (database marketing) and direct relations with existing customers can be established (one-to-one marketing) by constituting powerfull databases. Besides, firms need to create relationships with customers, suppliers, distributors, agencies, retailers, wholesalers, employees etc. (relationship marketing) rather than achieving just one transaction. The other topic explains the process from supplier to the end user (supply chain management). Since the success will depend on how entire supply chain performs against competitor chains, firms try to strengthen their connections with partners in the supply chain. As a result, new technologies and e-commerce has created very attractive possibilities for understanding customers better, establishing more powerfull relations with customers and other stakeholders, and therefore more effective and efficient marketing strategy.

More companies in the future will use online marketing and e-commerce if obstacles such as security addressed otherwise e-commerce may be slow to grow. If more secure ways of business are developed, consumers and firms will not consider themselves vulnerable about their personal information and they will go with e-commerce. Without security, most business operators and their clients may decide to forgo use of internet and revert back to traditional methods of doing business. To counter this trend and get benefits of e-commerce, the issues of Client/Server Side security, Transaction-side security and Organizational and legal issues must be constantly reviewed and appropriate countermeasures must be developed. These security mechanisms must be implemented in away that they do not harm e-commerce.

Technological developments are very important to provide security in e-commerce. The future of e-commerce depends on these developments. Security in e-commerce is one of the main problems of such trade. Based on the research among internet users indicates that internet usage for e-commerce transactions largely depends on security and protection of privacy [22].

Unfortunately there is no silver bullet to solve the security problems of e-commerce with existing technologies since each of them have some sort of security advantages and disadvantages and they require constant security improvements depending on the changing circumstances (new attacks etc). Major weakness of these available techniques is a lack of maturity and standardization (at least for some of them e.g. SET).

Technology only offers a wide range of tools to

solve some specific and clearly stated problems. It seems that these available but complex technologies must be combined to have a desired level of security. Even with this approach we can only show that a specific system is resistant against a set of well known attacks. Since we don't know all possible attacks in advance, it's impossible to say whether system is secure. Security is a system property that is not fully provable anyway. Nevertheless we believe that it's possible to build more secure systems with the existing technologies if we use, integrate them correctly and implement them securely. In other words the best way to build security is to use best technologies with best combinations.

The place of e-commerce systems in law is not established yet but this law is a prerequisite for the successful deployment of e-commerce applications. It should be addressed as quickly as possible.

Finally, the issue of security is not an easy problem and there are no definitive solutions to it. There will always be a fierce computation between people trying to protect their assets and people trying to defeat these protections. This will be a never ending story.

REFERENCES

[1] Kotler, P., & Armstrong, G. (2001). *Principles of Marketing*. 9th Edition. New Jersey: Prentice Hall.

[2] Jobber, D. (1995). *Principles and Practice of Marketing*, Berkshire: McGrawhill Book Company.

[3] Brooksbank, D., Thomas, B., Packham, G., & Morse, L. (2002). E-Commerce and Small and Medium Sized Enterprises in South East Wales; A Clear Case for Intervention?". Working Paper, *ISBA National Small Firms Policy & Research Conference*, Brighton.

[4] Oppliger, R. (1999). Shaping the research agenda for security in E-commerce. *10th International Workshop on Database and Expert Systems Applications*, Italy.

[5] Mavridis, I., Pangalos, G., Koukouvinos, T., & Muftic, S. *A secure payment system for Electronic Commerce.* (infolab.gen.auth.gr/Phd/mavridis/DEXA99.pdf).

[6] Stallings, W. (2003). *Network Security Essentials: Applications and Standarts.* 2nd Ed. New Jersey: Prentice Hall.

[7] Hofacker, C.F. (2001). *Internet Marketing*, Third Edition, New Jersey: John Wiley & Sons.

[8] Win, B.D., Bergh, J.V.D., Matthijs, F., Decker B.D., & Joosen, W. (2000). *A Security Architecture for e-commerce applications.* (http://www.cs.kuleuven.ac.be/~bartd/PAPERS/bdw-sec2000.ps.gz).

[9] Marchany, R.C., & Tront, J.G. (2002). E-Commerce Security Issues. *Proc. of the 35th Hawaii International Conference on System Sciences,* p.193. (http://csdl.computer.org/comp/proceedings/hics/2002/143/5/07/14350193.pdf)

[10] Sahuguet, A. (1998). *Piracy: The dark side of Electronic Commerce.* CIS-700/2 University of Pennsylvania.

[11] Ghosh, A.K. *Securing Electronic Commerce: Exposing the Weak Links.* Reliable Software Technologies Corporation. (http://www.rstcorp.com/~anup/IBconf.ps).

[12] Kailer, R. (2003). Accountability in Electronic Commerce Protocols. *Proceedings of the IEEE Syposium on Security and Privacy*, pp.200-205.

[13] Ettredge, M., & Richardson, V.J. (2002). Assesing the Risk in E-Commerce. *Proc. of the 35th Hawaii International Conference on System Sciences, p.194.* (http://csdl.computer.org/comp/proceedings/hics/2002/143/5/07/14350194.pdf)

[14] Hassler, V. (2001). *Security Fundamentals for E-Commerce.* Norwood: Artech House Computer Security Series.

[15] Liew, C.C., Ng, W.K., Lim, E.P., Tan, B.S., & Ong, K.L. (1999). Non-repudiation in Agent-Based Electronic Commerce System. *IEEE 10th International Workshop on Database and Expert Systems Applications, pp.*864-869. (http://csdl.computer.org/comp/proceedings/dexa/1999/0281/00/02810864.pdf)

[16] Peeples, D.K. (2002). Instilling Consumer Confidence in E-Commerce. *S.A.M. Advanced Management Journal*, 67(4), pp.26-32.

[17] Bishop, M. (2003). *Computer Security: Art and Science*, Boston: Addison Wesley.

[18] Pfleeger, C.P., & Pfleeger, S.L. (2003). *Security in Computing.* 3rd Ed. New Jersey: Prentice Hall.

[19] Matsuura, J.H. (2002). *Security, Rights, and Liabilities in e-commerce.* Norwood: Artech House.

[20] McCrohan, Kevin F. (2003), Facing the Threats to Electronic Commerce. *The Journal of Business & Industrial Marketing.* 18(2/3), pp.133-146.

[21] Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network Security: Private Communication in a Public world.* 2nd Ed. New Jersey: Prentice Hall.

[22] ITO. (2002). *Dünyada ve Türkiye'de Elektronik Ticaret ve Vergilendirilmesi.* İstanbul: Istanbul Ticaret Odası Yayınları, 6.

Levent ERTAUL (lertaul@csuhayward.edu) is a member of faculty in the department of Math & Computer Science. He received B.S. degree in Electrical and Electronics Engineering from Anatolia University in 1984, an M.S. Degree in Electronics Engineering from Hacettepe University in 1987 and a Ph.D Degree in Engineering and Applied Sciences department from the University of Sussex (UK) in 1994. He has an extensive back ground in teaching and research. He was involved in industrial, international, and government funded research activities. He was a visiting professor in Information Security Labs of Oregon State University (OSU) in 2002. He has published articles in such areas as computer networks security, cryptology, security in wireless networks and mobile agents security, telecommunications security.

Ayşe AKYOL (ayseakyol@mail.trakya.edu.tr) is a member of faculty in the department of business. She received BA degree in business from Dokuz Eylül University in 1990, MA degree in human resources management from İstanbul University in 1996, Ph.D degree in marketing from University of Portsmouth (UK) in 2000, MSc degree in business research and consultancy from University of Portsmouth in 2002. Her research interests are international marketing, export, social and environmental orientation, marketing ethics.