Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 6, June 2016, pg.224 – 232

E-Commerce- Study of Privacy, Trust and Security from Consumer's Perspective

Ms. Palak Gupta[1], Dr. Akshat Dubey[2]

[1]Jagannath International Management School, New Delhi, India
[2]Jagannath International Management School, New Delhi, India
[1] palak.gupta@jagannath.org; [2] akshat.dubey@jagannath.org

Abstract— Consumer disposition to the information quality of the website, trust, privacy concerns, reputation, security concerns, and the company's reputation have strong effects on Internet consumers' trust in the website. Major two critical problems for both e-commerce consumers and sites are privacy and security. Privacy is the control over one's personal data whereas; security is the attempted access to data by unauthorized users. Information security, therefore, is an essential management and technical requirement for any efficient and effective payment transaction activities over the internet. E-commerce security is the protection of e-commerce assets from unauthorized access, destruction, alteration, or use so its dimensions to be studied are- Integrity, Privacy, Non-repudiation, Authenticity, Confidentiality, and Availability. This paper would throw light on E-commerce privacy, security, its purpose, different security issues and how consumer's trust and purchasing behavior is affected by it.

Keywords— Role of trust, Electronic commerce, Consumer trust, Perceived risk, Internet consumer behaviour, Privacy and security, E-Commerce Security Issues

I. INTRODUCTION

Today, privacy, security and trust are major concerns for electronic technologies. E-commerce security is specifically applied to the components that affect e-commerce namely computer security, data security, integrity, availability and other wider realms of the Information Security framework. According to the Forrester report, Business to Consumer (B-to-C) Internet commerce enjoys a steady growth rate (about 19% per year), and it is a familiar mode of shopping for many consumers [2]. Many scholars have argued that trust is a prerequisite for successful commerce because consumers are hesitant to make purchases unless they trust the seller [9], [10], [11], [15] and [13]. Quite possibly, the key to success in Internet business is the establishment of trusted transaction processes where e-sellers create an environment in which a prospective consumer can be relaxed and confident about any prospective transactions [14]. Given the increasing prevalence of B-to-C Internet commerce,

there is an urgent need to analyze an online consumer's decision-making process from a holistic standpoint which can provide an understanding of the complex and dynamic phenomena of trust in online exchanges.

Web e-commerce applications that handle payments such as electronic transactions using credit cards or debit cards, online banking, PayPal or other tokens have more compliance issues and are at increased risk from being targeted than other websites as they suffer greater consequences if there is data loss or alteration. Mule, Trojan horse and worms if launched against client systems, pose the greatest threat to e-commerce privacy and security because they can subvert most of the authorization and authentication mechanisms used in an ecommerce transaction.

Trust has always been an important element in influencing consumer behavior toward merchants [35] and has been shown to be of high significance in uncertain environments such as Internet-based EC environments [36]. While a variety of factors such as branding and store reputation may influence trust, one missing factor is the face-to-face communication and lack of touch and feel which is present in physical interactions. Therefore, it has been argued that trust would be favorably influenced by increase in perceptions of security and privacy in EC transactions [37][38].

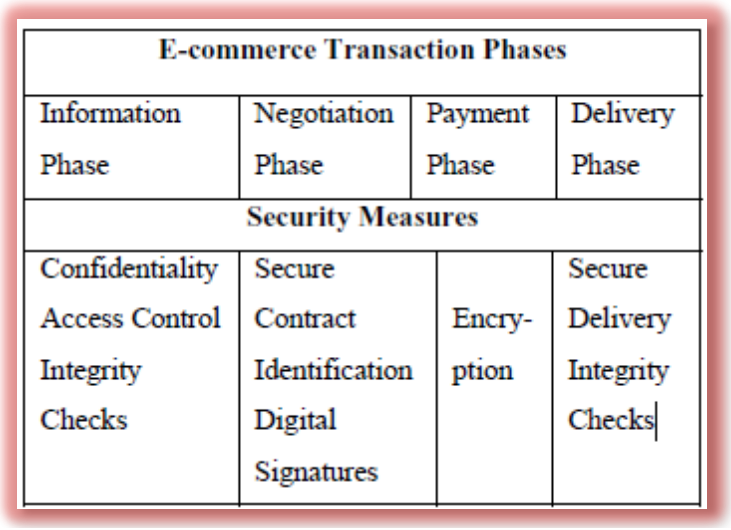
II.LITERATURE REVIEW

Generally interpersonal trust is focused if we talk about traditional commerce such as a customer's trust in a salesperson. Plank et al. [41] recognized that consumer trust could have multiple referents like product, salesperson and company and accordingly defined trust as a global belief on the part of the buyer that the salesperson, product, and company will fulfill their obligations as understood by the buyer. Similarly, in the e-commerce context [3], [5], [6] and [8] like researchers have tended to define and describe trust as the willingness of an individual to be vulnerable, a person's expectation, a subjective belief, reliance on parties other than oneself or a subjective probability.

There are **four categories of antecedents that influence consumer trust and consumers' perceived risk towards electronic commerce entities** [4] which are:

1. *Experience-based*: e.g., e-commerce experience, familiarity, Internet experience, etc.
2. *Cognition (observation)-based*: e.g., system reliability, privacy protection, quality of information, security protection, brand image, etc [7].
3. *Personality-oriented*: e.g., disposition to shopping habbits, trust, etc.
4. *Affect-based*: e.g., presence of third-party seals, reputation referral, recommendation, buyers' word-of-mouth, feedback, review comments, etc [12].

Ecommerce web site owners on one side are thinking of how to attract more customers and how to make the visitors feel secured when working on the site, while on the other side how the end users should rate a ecommerce website and what they should do to protect themselves as one among the online community [17]. Each phase of E-commerce transaction has security measures.



E-commerce Transaction Phases			
Information Phase	Negotiation Phase	Payment Phase	Delivery Phase
Security Measures			
Confidentiality Access Control Integrity Checks	Secure Contract Identification Digital Signatures	Encry-ption	Secure Delivery Integrity Checks

Fig 1 Security measures in different phases of Ecommerce Transaction [18]

Viruses are a nuisance threat in the e-commerce world. They only disrupt e-commerce operations and should be classified as a Denial of Service (DoS) tool. Password protection, encrypted client-server communication, public private key encryption schemes are all negated by the simple fact that the Trojan horse program allows the hacker to see all clear-text before it gets encrypted [19]. Due to the increase in warnings by the media from security and privacy breaches like identity theft and financial fraud, and the elevated awareness of online customers about the threats of performing transactions online, e-commerce has not been able to achieve its full potential. Many customers refuse to perform online transactions and relate that to the lack of trust or fear for their personal information [20]. Clearly, the online transaction requires consumers to disclose a large amount of sensitive personal information to the vendor, placing themselves at significant risk. Understanding (indeed, even precisely defining) consumer trust is essential for the continuing development of e-commerce [21].

III.E-COMMERCE IN INDIA

India has an internet user base of about 354 million as of June of 2015. Despite being the second largest user base in world, only behind China (650 million, 48% of population), the penetration of e-commerce is low compared to markets like the United States (266 M, 84%), or France (54 M, 81%), but is growing at an unprecedented rate, adding around 6 million new entrants every month. The industry consensus is that growth is at an inflection point. In India, cash on delivery is the most preferred payment method, accumulating 75% of the e-retail activities. Demand for international consumer products (including long-tail items) is growing much faster than in-country supply from authorized distributors and e-commerce offerings.

Largest e-commerce companies in India are Flipkart, Snapdeal, Amazon India, Paytm. India's e-commerce market was worth about $3.9 billion in 2009, it went up to $12.6 billion in 2013. In 2013, the e-retail segment was worth US$2.3 billion. About 70% of India's e-commerce market is travel related. According to Google India, there were 35 million online shoppers in India in 2014 Q1 and is expected to cross 100 million mark by end of year 2016.CAGR vis-à-vis a global growth rate of 8–10%. Electronics and Apparel are the biggest categories in terms of sales. By 2020, India is expected to generate $100 billion online retail revenue out of which $35 billion will be through fashion e-commerce. Online apparel sales are set to grow four times in coming years.

A. ***Key drivers in Indian e-commerce are:***

- Rising standards of living.
- Increase in subscription to broadband Internet and escalating 3G & 4G internet users
- Increased usage of online classified sites like ebay.com, quikr.com, with more consumer buying and selling second-hand goods
- Enormous growth of Smartphone users, soon to be world's second largest smartphone user base.
- Availability of much wider product range compared to what is available at brick and mortar retailers.
- Evolution of multi facility startups like Jabong.com, Saavn, Makemytrip, Bookmyshow, Zomato Etc.
- Competitive prices compared to brick and mortar retail driven by reduced real estate and inventory costs and disintermediation.

India's *retail market* is estimated at $470 billion in 2011 and is expected to grow to $675 Bn by 2016 and $850 Bn by 2020, – estimated CAGR of 10%. According to Forrester [1], the e-commerce market in India is set to grow the fastest within the Asia-Pacific Region at a CAGR of over 57% between 2012 and 2016. As per "India Goes Digital", a report by Avendus Capital, a leading Indian Investment Bank specializing in digital media and technology sector, the Indian e-commerce market is estimated at Rs 28,500 Crore ($6.3 billion) for the year 2011 of which online travel constitutes a sizable portion (87%) of this market today. Overall e-commerce market is expected to reach Rs 1, 07,800 crores (US$24 billion) by the year 2017 with both online travel and e-tailing contributing equally. Another big segment in e-commerce is mobile/DTH recharge with nearly 1 million transactions daily by operator websites.

New sector in e-commerce is online medicine. Company like Reckwing-India, Buyonkart, and Healthkart already selling complementary and alternative medicine where as NetMed has started selling prescription medicine online after raising fund from GIC and Steadview capital citing· There are no dedicated online pharmacy laws in India and it is permissible to sell prescription medicine online with a legitimate license.

IV. E-COMMERCE PRIVACY

Privacy is a serious issue in electronic commerce, no matter what source one examines. Culnan [23] argued that privacy concerns were a critical reason why people do not go online and provide false information online. Indeed, relatively few consumers believe that they have very much control over how personal information, revealed online, is used or sold by businesses [24]. The combination of current business practices, consumer fears, and media pressure has combined to make privacy a potent problem for electronic commerce. Some people consider privacy to be a fundamental right; others consider it to be a tradable commodity. Besides "privacy", a number of terms such as, digital persona, notice, identification, choice, authentication, pseudonymity, anonymity, and trust are also major concerns in e-commerce to be addressed.

E-commerce sites could potentially collect an immense amount of data about personal preferences, shopping patterns, patterns of information search and use, and the like about consumers, especially if aggregated across sites. Not only it is easier than ever to collect the data, but also much easier to search these data [25]. New computational techniques allow data

mining to explore consumer's buying patterns and other personal trends in almost real time mode. Consumers have two kinds of privacy concerns. First, they are concerned about the risk of secondary use i.e., the reuse of their personal data for unrelated purposes without their consent such as sharing with third parties who were not part of the transaction in which the consumer related his or her personal data. Second, consumers are concerned over unauthorized access to personal data because of security breaches or the lack of internal controls [24].

A. *Technologies used for E-Commerce Privacy*

Majorly there are four broad categories of privacy technologies-

1. technologies used for surveillance
2. technologies for forming contracts or agreements about the release of private data
3. technologies for labeling and trust, and
4. privacy-enhancing technologies (PETs).

The technologies for surveillance and for data capture are used by companies for business purposes, but they have the side effect of generating biometrics, data trails, data warehousing and data mining thus affecting personal privacy. However, privacy enhancing technologies (PETs) attempt to balance the surveillance or tracking technologies through personal firewalls, cookie managers and digital cash (e.g., Ecash).

V. TRUST IN E-COMMERCE

Trust is an important issue in e-commerce, because unlike real world transactions, the retailer is not present in person during the transaction and the consumer is not dealing with a real person. It is just dealing with an interface. It is much easier for an entity to set up a website and an electronic payment processing system than a real world storefront. It is cheaper, faster and more transparent. It is also much more difficult for customers to determine the authenticity of websites. This makes it very difficult to trust that the retailers are who they claim to be. Trust is a mental shortcut that consumers can use when trying to reduce the uncertainty and complexity of transactions and relationships in e-commerce markets. Online it is difficult to connect identities with actual individuals.

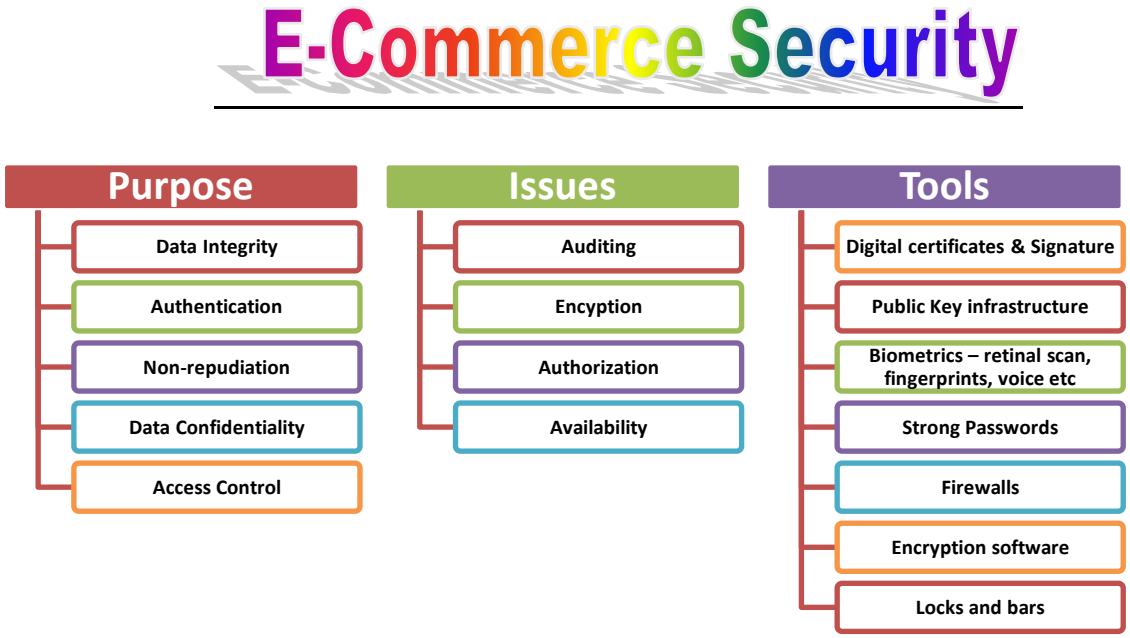
For consumers, security, privacy, functionality and user-friendliness issues are considered to be barriers to online shopping. Moreover, they want their personal data to be private and confidential so that they are not exposed to any fraud. They also want that the technology they are using should enable them to freely operate and take sensible control over it. But they are more flexible and willing towards taking risks with the people or organisations that they trust. The probable risk is higher in e-commerce mainly because of unawareness, proximity and negligible physical interactions. So, in order to see why consumer engage or do not engage in e-commerce, it is important to study their online trust in e-commerce as a marketplace.

Some factors which are the most important to the consumers for trusting a website are the security systems, privacy, reputation of the company, payment methods offered by it, customer service provided, the website design, control of technology, ease of usage, user friendliness of the website, and the price offered by the company. When we look at the age wise differentiation of factors, it is observed that the people in age group of above 35yrs are more reluctant to use internet as a market place than those who are 18-35yrs.

VI. E-COMMERCE SECURITY ISSUES

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Consumers fear the loss of their financial data, and e-commerce sites fear the financial losses associated with any resulting bad publicity and break-ins. There are a number of critical social and organizational issues with security. The first is the development of adequate organizational processes for risk management, development of security policies, separation of duties, security assurance and access control. The second is that the weak link in security is often employees or users, rather than the technology [34] and the third is software engineering management, or managing how security technology is deployed.

A persistent problem is users' differing and incorrect models of security and their seeming unwillingness or inability to adhere to critical security policies and guidelines. For example, users may store passwords in unencrypted files on vulnerable machines or employees may divulge their passwords to third parties.



A. ***Major types of E–Commerce Threats-***

1. **Unauthorized access-** It implies illegal access to data, systems or applications for some malicious purpose. In Passive unauthorized access the hacker listens to communication channels for finding secrets or content which may be used for damaging purposes. However, in Active unauthorized access the hacker modifies system or data with an intention to manipulate or change. Some current examples include ineffective encryption or lack of encryption for home wireless networks [27], a popular home-banking system that stores a user's account number in a Web "cookie" which hostile web-sites can crack [28] and mail-borne viruses that can steal the user's financial data from the local disk or even from the user's keystrokes [29]. Home computer, Point-of-Sale (POS) terminals in brick-and-mortar stores, as well as a variety of mobile and handheld devices can easily be targeted by hackers.

2. **Denial of Service-** It may occur by spamming and viruses. Spamming is basically unusual e-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it. DDOS (Distributed Denial Of service Attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target. However, viruses are self-replicating computer programs designed to perform unwanted events. Worms are special viruses that spread using direct Internet connections and Trojan Horses are disguised as legitimate software that trick users into running the program.

3. **Theft and Fraud**-Fraud occurs when the stolen data is used or modified. Theft of software implies illegal copying from company's servers or theft of hardware, specifically laptops. Hackers break into insecure merchant web servers to harvest archives of credit card numbers generally stored along with personal information when a consumer makes an online purchase. The merchant back-end and database is also susceptible for theft from third party fulfillment centers and other processing agents.

B. ***Technologies used for e-commerce Security***

1. Encryption algorithms like Public Key Infrastructure (PKI) systems which are based on asymmetric cryptography are highly secure as they are coupled with Secure Socket Layer (SSL) protocol and the interbank standard suite, ANSI X9. PKI often requires a centralized, highly available intermediary for key management, and especially for prompt notification about revoked key-pairs [30].

2. A digital signature, which can be used to sign contracts, to prove identity for access or to provide authenticity of an electronic distribution is the best example of PKI.

3. Smartcards [31] can be used to store data about the bearer of the card, including identification credentials, financial data, medical records etc. Smartcards can allow POS transactions to be more intricate, because the entire user's data is always available. This architecture can also avoid the centralized storage of personally sensitive data.

4. Digital cash and networked payments through which a consumer might buy electronic data or a digital service without revealing his purchases to a financial clearinghouse and identity to the merchant [32]. Micropayments such as per-article newspaper subscriptions and PayPal, a payment intermediary, have also been financially successful.

5. Digital watermarking technology [33] is another popular internet security mechanism where the technical goal is to find ways of cryptographically tagging electronic content (especially images and audio) in a way that is non removable, non-forgeable, and recognizable. The watermark tag is generally designed to be invisible or unobtrusive.

VII. FINDINGS

The study reveals that consumer's loyalty to a web site is closely linked to the levels of trust. Thus, the development of trust not only affects the intention to buy, as shown by previous researchers, but it also directly affects the effective purchasing behavior, in terms of cost, preference, and frequency of visits, therefore, the level of profitability provided by each consumer. In addition, the analyses show that trust in the internet is particularly influenced by the security perceived by consumers regarding the handling of their private data. Alleviation of monetary risk through limited liability clauses has only a small impact on consumer trust. Web browsers and Web sites should display visible security mechanisms such as statements about data protection and firewalls (protection), an unbroken lock/key (encryption), digital certificates (authentication) from trusted third parties and familiar and verifiable domain names (verification).

VIII. CONCLUSION

Not only must e-commerce sites and consumers judge security vulnerabilities and assess potential technical solutions, they must also assess, evaluate, and resolve the risks involved. A networked application cannot offer full measures of connectivity, security, and ease-of-use, all at the same time; there seems to be an intrinsic trade-off here, and some sacrifice is unavoidable. Accordingly, the first security concern from an e-commerce merchant's perspective should be to keep the web servers' archives of recent orders not on the front-end web servers but behind the firewall [26]. Furthermore, sensitive servers should be kept highly specialized, by turning off and removing all inessential services and applications (e.g., ftp, email). Until e-commerce vendors achieve the necessary delicate balance of privacy, trust and security, effective and quantitative ecommerce transactions will remain a problem. Thus the mechanisms of encryption, protection, verification and authentication indeed influence perceptions of security. The marketplace can be trustworthy only when consumers feel trust in transacting in that environment.

REFERENCES

[1] Forrester, US e-business Overview: 2003–2008, July 25, 2003.
[2] Online Advertising To Reach $33 Billion Worldwide By 2004. Forrester Research Press (1999) http://www.forrester.com/ER/Press/Release/0,1769,159,FF.html.
[3] S. Ba, A.B. Whinston, H. Zhang. Building trust in online auction markets through an economic incentive mechanism. Decision Support Systems, 35 (3) (2003), pp. 273–286.
[4] J.B. Barney, M.H. Hansen. Trustworthiness as a source of competitive advantage. Strategic Management Journal, 15 (1994), pp. 175–190.
[5] S.E. Beatty, M. Mayer, J.E. Coleman, K.E. Reynolds, J. Lee. Customer–sales associate retail relationships. Journal of Retailing, 72 (3) (1996), pp. 223–247.
[6] A. Bhattacherjee. Individual trust in online firms: scale development and initial test. Journal of Management Information Systems, 19 (1) (2002), pp. 211–242.
[7] C.C. Chen, X.-P. Chen, J.R. Meindl. How can cooperation be fostered? The cultural effects of individualism–collectivism. Academy of Management Review, 23 (2) (1998), pp. 285–304.
[8] E. Brynjolfsson, M. Smith. Frictionless commerce? A comparison of Internet and conventional retailers. Management Science, 46 (4) (2000), pp. 563–585.
[9] D. Gefen. Reflections on the dimensions of trust and trustworthiness among online consumers ACM SIGMIS Database, 33 (3) (2002), pp. 38–53.
[10] S.L. Jarvenpaa, N. Tractinsky, L. Saarinen, M. Vitale. Consumer trust in an Internet store: a cross-cultural validation. Journal of Computer Mediated Communication, 5 (2) (1999).
[11] D.J. Kim, Y.I. Song, S.B. Braynov, H.R. Rao. A multi-dimensional trust formation model in B-to-C ecommerce:a conceptual framework and content analyses of academia/practitioner perspective. Decision Support Systems, 40 (2) (2005), pp. 143–165.
[12] D .J. McAllister. Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. Academy of Management Journal, 38 (1) (1995), pp. 24–59

[13] G.L. Urban, F. Sultan, W.J. Qualls. Placing trust at the center of your Internet strategy. Sloan Management Review, 42 (1) (2000), pp. 39–48.
[14] P. Grabosky. The nature of trust online. The Age (2001), pp. 1–12.
[15] KIM, Dan J.; FERRIN, Donald L.; and RAO, H. Raghav. A Trust-Based Consumer Decision Model in Electronic Commerce: The Role of Trust, Risk, and Their Antecedents. (2008). *Decision Support Systems*. , 44(2), 544. Research Collection Lee Kong Chian School Of Business. Available at: http://ink.library.smu.edu.sg/lkcsb_research/1147.
[16] Carlos Flavián, Miguel Guinalíu, (2006) "Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site", Industrial Management & Data Systems, Vol. 106 Iss: 5, pp.601 620.
[17] V.Srikanth "Ecommerce online security and trust marks". IJCET ISSN 0976 – 6375, Volume 3, Issue 2, July- September (2012).
[18] Shazia Yasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012.
[19] Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues"Proceedings of the 35th Hawaii International Conference on System Sciences – 2002.
[20] Rashad Yazdanifard, Noor Al-Huda Edres "Security and Privacy Issues as a Potential Risk for Further Ecommerce Development"International Conference on Information Communication and Management – IPCSIT vol.16 (2011).
[21] Pradnya B. Rane, Dr. B.B.Meshram. "Transaction Security for Ecommerce Application" IJECSE -ISSN-2277-1956. 2012.
[22] Culnan, Mary J. 2000. Protecting Privacy Online: Is Self-Regulation Working? Journal of Public Policy and Marketing, 19 (1) : 20-26.
[23] Culnan, Mary J., and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10 (1) : 104-115.
[24] Dhillon, Gurpreet S., and Trevort T. Moores. 2001. Internet Privacy: Interpreting Key Issues. *Information Resources Management Journal*, 14 (4) : 33-37..
[25] Winner, D. 2002. Making Your Network Safe for Databases. SANS Information Security Reading Room, July 21, 2002.
[26] Borisov, N., I. Goldberg, and D. Wagner. 2001. Intercepting Mobile Communications: The Insecurity of 802.1. Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking : 180-189.
[27] Graves, P., and M. Curtin. 2000. Bank One Online Puts Customer Account Information At Risk. http://www.interhack.net/pubs/bankone-online.
[28] Neyses, J. 2002. Higher Education Security Alert From the U.S. Secret Service: List of Keystroke Logging Programs. http://www.unh.edu/tcs/reports/sshesa.html.
[29] Adams, C., and S. Farrell. 1999. Internet X.509 Public Key Infrastructure certificate management protocols. Internet RFC 2510.
[30] Rankl, W., and W. Effing. 1997. *The Smartcard Handbook*. New York: John Wiley.
[31] Chaum, David. 1985. Security Without Identification: Transaction Systems To Make Big Brother Obsolete. Communications of the ACM, 28 : 1030-1044.
[32] Delaigle, J-F., C. De Vleeschouwer, and B. Macq. 1996. Digital Watermarking. Proceedings of the Conference 2659 - Optical Security and Counterfeit Deterrence Techniques : 99-110.
[33] Anderson, Ross. 1994. Why Cryptosystems Fail. *Communications of the ACM*, 37 (11) : 32-40.
[34] Schurr, P.H. and Ozanne, J.L. (1985), ``Influences on exchange processes: buyers' preconceptions of a seller's trustworthiness and bargaining toughness'', Journal of Consumer Research, Vol. 11 No. 4, pp. 939-53.
[35] Fung, R. and Lee, M. (1999), ``EC-trust (trust in e-commerce): exploring the antecedent factors'', Proceedings of the 5th Americas Conference on Information Systems.
[36] Chellappa, R.K. (2001), ``The role of perceived privacy and perceived security in the development of trust in electronic commerce transactions'', ebizlab working paper, Marshall School of Business, University of South California, Los Angeles, CA.
[37] Ramnath K. Chellappa and Paul A. Pavlou, "Perceived information security, financial liability and Consumer trust in electronic commerce transactions", Logistics Information Management, Volume 15 . Number 5/6 . 2002 . pp 358-368.
[38] A Study on the Factors That Influence the Consumers' Trust on E-commerce Adoption; http://arxiv.org/ftp/arxiv/papers/0909/0909.1145.pdf.
[39] R.E. Plank, D.A. Reid, E.B. Pullins. Perceived trust in business-to-business sales: a new measure. The Journal of Personal Selling & Sales Management, 19 (3) (1999), pp. 61–71

