ENHANCING TRUST BELIEFS IN E-COMMERCE THROUGH WHITELIST WEBSITE SECURITY PARADIGM

Dr. A.S. Khandelwal
Head of the Department, Computer Science, Hislop College,
RTM Nagpur University,Nagpur, Maharashtra

Abstract:
In the emerging global economy, E-commerce has increasingly become a strong catalyst for economic development. Based on the observation of the E-commerce management practices in India it is felt that there is a need to increase trust by providing additional layer of security in order to make E-commerce more acceptable. In this paper, new approach in website security mechanism with respect to E-commerce trust management is being discussed. Systems build using whitelist paradigm may create credible lock down secure websites. In conclusion, this may tremendously help in minimizing the customer fear and risk associated with sensitive and vital information such as banking details, credit card information, billing address etc., thereby enhancing the credibility of online marketplaces. It may promote confidence building in the consumer mindset apropos of online data security thus fueling E-commerce growth and potential user base.

Keywords: E-commerce; E-commerce trust management;website security mechanism.

1. Introduction:

E-commerce sales are sales of goods and services where an order is placed by the buyer, price and terms of sale are negotiated over an Internet, Extranet, Electronic Data Interchange (EDI) network, electronic mail, or other online system. To the consumer or the general public, probably the only visible part of E-commerce is in catalogue browsing and order placement via the Internet. Trust is a social and psychological phenomenon that is widely acknowledged as contributing to many forms of exchange, including e-commerce exchanges. Researchers have suggested that trust beliefs influence the online consumers' trust responses. This study may make a valuable contribution not only to information systems and diffusion research but also to online vendors in their attempts to engender consumer trust in their websites. However, there are a lot of other E-commerce activities that take place behind the scenes throughout the e-transactions. [1] The potential benefits of E-commerce are obvious. Still it is widely acknowledged through national surveys, which show that even today use of E-commerce is far below expectation. This can be attributed to many factors. Foremost among them is customer trust deficit in the whole E-Commerce process cycle.

The importance of the trust construct and its influence on human behavior is widely acknowledged by academics from across a wide spectrum of intellectual disciplines. Sociologists Gambetta et al [2], psychologists Deutsch et al [3], organisational behavior scientists Kraut, R. Rice.., Kramer & Tyler, Mishra , Mayer Davis & Schoorman, 1995; Sitkin & Roth [4-8], as well as economists Williamson, Zucker [9-10] , anthropologists Ekeh [11] and political scientists Barber [12] have contributed widely in the work that exists on this topic in their respective context. In the Information Systems (IS) field, researchers have shown an increasing awareness of how trust contributes towards the success of many types of virtual environments Cyr et al ; Briggs et al; Gefen et al ; Cortitore et al.; Huang et al.;Belanger et al Koufaris and Hampton Sosab et al; Gefen, 2003; Lee et al., 2001). [13-19]. In this paper, virtual environment with a new approach in website security mechanism with respect to E-commerce trust management is being discussed. Systems build using whitelist paradigm may result in a strong increase in adoption of online shopping.

India's Share of Online Commerce in International Market

India's share of online commerce is projected to grow from 1.3 percent of Asia-Pacific in 2006 to 3.3 percent by 2011. The projected value of the market over the years and projected for the upcoming years are:

2006 : $800 million
2007 : $1.2 billion
2008 : $1.9 billion
2009 : $2.8 billion

2010 : $4.1 billion
2011 : $5.6 billion

"On a country-by-country basis, India was expected to show the highest CAGR of 83.7 per cent in E-commerce revenue from 2003 to 2008, thus marginally exceeding the CAGR of 81 per cent expected in China," according

to IDC's forecast on Asia Pacific Internet market. India is the second most populous country and the largest democracy in the world. Now India has improved its position to the 43rd rank in the World of E-commerce activities. [20]

Global Scenario: E-commerce sales all over

B2C E-Commerce Sales* in Select Countries in the Asia-Pacific Region, 2006-2011 (bilions)

	2006	2007	2008	2009	2010	2011
Australia	$9.5	$13.6	$20.4	$26.4	$28.7	$31.1
China**	$2.4	$3.8	$6.4	$11.1	$16.9	$24.1
India	$0.8	$1.2	$1.9	$2.8	$4.1	$5.6
Japan	$36.8	$43.7	$56.6	$69.9	$80.0	$90.0
South Korea	$9.6	$10.9	$12.4	$14.0	$15.9	$17.9
Asia-Pacific	**$59.1**	**$73.3**	**$97.7**	**$124.1**	**$145.5**	**$168.7**

*Note: converted at average annual exchange rates (projected for future years); total B2C e-commerce sales include all purchases made on a retail Web site, regardless of device used to complete the transaction; *includes online travel, event ticket and digital download sales; **excludes Hong Kong*
Source: eMarketer, January 2008

091218 www.eMarketer.com

The figure clearly shows India is showing growth in the E-commerce as we go from 2006 to 2011 but as compared to other countries, it is far behind. India is still in its initial stage of development.

E-commerce in India

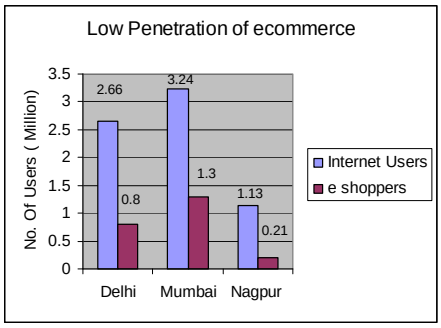
According to the Indian e-Commerce Report released by Internet and Mobile Association of India (IAMAI) and International Market Research Bureau) IMRB International, the total online transactions in India was Rs. 2300 crores in the year 2006-2007 (around 10 per cent of the organized Indian retail market) a 95 per cent rise over previous year's figures of Rs 1,180 crore and an over-300 per cent rise over the figures of 2004-05 (which was 570 crores). It grew by 30% to touch 5500 crores (approx by the year 2007-2008). According to a McKinsey-Nasscom report the E-commerce transactions in India are expected to reach 10000 crore by the end of 2009. [21]

IAMAI forecasted estimates e-commerce transactions are given in Table below.

Year	2002-03	2003-04	2004-05	2005-06	2006-07	2007-08	2008-09
B2C - Rs crore	130	255	570	1180	2300	5500	9259

Who is Responsible for Low Penetration of E-commerce?

According to Industry expert, Darpan Munjal, CTO (eCommerce) at IndiaTimes the largest factor for relatively slow adoption of E-commerce can be attributed to the security mechanism which failed to generate sufficient TRUST. The success is with those who are able to win customer's trust and offer a clear value proposition to the customer with a strong promise around quality execution. **Consumers and retailers both desire a totally safe, simple and complete online shopping.**



The figure of Internet users along with e-shoppers in Capital, Metro and non metro cities are shown in above chart. [22]

Threat to E-commerce

A recent survey by VeriSign, a provider of Internet security services, has revealed that at least 76% of Web users in India are exposed to online fraud and particularly phishing attacks as they are unable to identify the different forms of phishing currently happening online. [23]

2. Present Approaches in Security Mechanism to tackle Online Fraud and Phishing Attacks:

2.1 *Cryptographic techniques*

Cryptography has been playing an important role to ensure the security and reliability of modern computer systems. Since high speed and broad bandwidth have been becoming the keywords for modern computer systems, new cryptographic methods and tools must follow up in order to adapt to these new and emerging technologies. Theoretical and practical advances in the fields of cryptography and coding are a key factor in the growth of data communications, data networks and distributed computing. The mathematical theory and practice of cryptography and coding is popular in providing security mechanism. There is a need to focus on other aspects of information systems and network security, including applications in the scope of the knowledge society in general and information systems development in particular, especially in the context of e-business, internet and global enterprises. [24], [25].

2.2 *Paradigm of leaving and interacting*

Ambient assisted living concept is envisioned through a new paradigm of interaction inspired by constant provision to information and computational resources. This provision is enabled through invisible devices that offer distributed computing power and spontaneous connectivity. A nomad traversing residential, working, and advertising environments seamlessly and constantly is served by small mobile devices like portables, handheld, embedded or wearable computers. This paradigm of leaving and interacting introduces new security, trust and privacy risks thus support in confidence development. [26]

2.3 *Language-based techniques for security*

Few techniques have been implemented using programming language and program analysis techniques to improve the security of software systems. It explores and evaluates new, speculative ideas on the evaluations of new or known techniques in practical settings for solving emerging threats and important problems. It covers verification of security properties in software, automated introduction and/or verification of security enforcement mechanisms, Program analysis techniques for discovering security vulnerabilities. [27]

2.4 *Compiler-based security mechanisms*

This technique helps to detect host-based intrusion detection and in-line reference monitors
It also enforces security policies for information flow and access control. [28]

2.5 *Group-oriented cryptographic protocols*

Group-oriented cryptographic protocols are foundational for the security of various group applications, like digital conferencing, groupware, group communication systems, computer-supported collaborative work-flow systems, multi-user information distribution and sharing, data base and server replication systems, peer-to-peer and ad-hoc groups, group-based admission and access management, applications in federative or distributed environment, etc. A variety of cryptographic techniques and assumptions provides a solid basis for the design of provably secure group-oriented cryptographic protocols, which is an important and challenging task. Formal security models for group-oriented cryptographic protocols require consideration of a large number of potential

threats resulting from the attacks on the communication channel and from the misbehavior of some protocol participants. [29]

2.6 ***Security Architectures in Distributed Network Systems***

In recent years, there has been significant increase in Internet attacks, such as DDoS, viruses, worms, spyware, and malware, etc, causing huge economical and social damage. Security Architectures in Distributed Network Systems mechanism has provided ways to attack systems in a more easy-to-use, sophisticated, and powerful way. It has greatly helped in building more effective, intelligent, and active defense systems which are distributed and networked. It has provided ways to fully understand the attack mechanisms which enables to perform effective and comprehensive defense. [30]

2.7 ***Key Management for Sector and File based Storage Systems***

Stored information critical to individuals, corporations and governments must be protected, but the continually changing uses of storage and the exposure of storage media to adverse conditions make meeting that challenge increasingly difficult. Example uses include employment of large shared storage systems for cost reduction and, for convenience, wide use of transiently-connected storage devices offering significant capacities and manifested in many forms, often embedded in mobile devices. Protecting intellectual property, personal records, health records, and military secrets when media or devices are lost, stolen, or captured is critical to information owners. To remain or become viable, activities that rely on storage technology require a comprehensive systems approach to storage security. Key Management for Sector and File based Storage Systems techniques such as Cryptographic Algorithms for Storage, Cryptanalysis of Systems and Protocols, Unintended Data Recovery provides solutions in this scenario. [31]

2.8 ***Privacy and Data Sanitization***

Privacy and Data Sanitization method falls within the scope of collaborative security. Any useful collaboration takes place at some point in sharing data. Unfortunately, data sharing is one of the greatest hurdles getting in the way of otherwise beneficial collaborations. Data regarding one's security stance is particularly sensitive, often indicating one's own security weaknesses. This data could include computer or network logs of security incidents, architecture documents, or sensitive organizational information. Even when the data may not compromise the data owner's security stance, sharing may violate a customer's privacy. Data sanitization techniques such as anonymization and other mechanisms such as privacy-preserving data mining and statistical data mining try to address this tension between the need to share information and protect sensitive information and user privacy. [32]

3. Methodology:

All approaches in security mechanism to tackle online fraud and phishing attacks were examined. The measurement instrument was applied to samples with set of respondents who had strong technical backgrounds. For this study, the samples were obtained from the Engineering and IT students. It consisted of 250 individuals who completed and or are in process of obtaining an MCA degree / BE Computer technology. Care was taken that the respondents have adequate disposable income and technical competency to engage in online shopping. However, it is reasoned that an individual could be considerably outdated (which would reduce their knowledge and experience of online shopping). To overcome this potential limitation, an age limit of 28 years of age was imposed on the participants selected.

The respondent's samples revealed the fact that the technique being used for providing security and reliability in ecommerce usage, there is an Ernest need to take extra measures. Majority of them strongly felt that reliability plays vital role in encouraging e-customers. However respondents appreciated few security mechanism but to increase e-commerce adoption they found lacuna of totally safe, simple and complete security mechanism.

S.No.	Currently used Techniques selected for study	Satisfied respondents in %
1	Cryptographic	68%
2	Paradigm of leaving and interacting	45%
3	Language-based techniques for security	07%
4	Compiler-based security mechanisms	02%
5	Group-oriented cryptographic protocols	68%
6	Security Architectures in Distributed Network Systems	52%
7	Key Management for Sector and File based Storage Systems	31%
8	Privacy and Data Sanitization	45%

4. Result and Discussion:
It was observed that the respondents need for good security mechanism in E-commerce is becoming more acute every day. Typical activities - including selecting, purchasing, and consuming services and products, conducting business increasingly depend on secured E-commerce website.

The studied approaches lacks in ensuring the security in totality and identity management by end-users. There is a need to reconcile (or strike the right balance between) two goals that are generally thought to be contradictory: the usability of the systems on one hand and their security and privacy on the other. The aim of is to provide recommendations for a modified approach which is implementable and provides deployable improvements for security and identity management. In this paper whitelist Website Security Paradigm are being discussed to ensure additional security to E-commerce systems. This approach may overcome the limitations of the current technologies and explore alternatives.

Domain Keys Identified Mail (DKIM) is a specification for cryptographically signing email messages, permitting a signing domain to claim responsibility for a message in the mail stream. Message recipients (or agents acting in their behalf) can verify the signature by querying the signer's domain directly to retrieve the appropriate public key, and thereby confirm that the message was attested to by a party in possession of the private key for the signing domain. DKIM signatures are applied and verified at the domain level so that individual users do not need to implement DKIM other than possibly to act on the results of message authentication performed by their domains. DKIM is intended to be complementary to (and can be used with) existing message security technologies such as PGP and S/MIME. [33-36]

White List paradigm for Secured E-commerce
Similar approaches can be made for white listing E-commerce transactions to confirm Guinness which may help to a very great extend to gain trust between parties.

- An explicit goal of Domain key identified transactions is to be minimally disruptive to existing E-commerce users. Unexpected changes to message appearance or functionality would likely result in confusion among less-sophisticated users and reluctance to deploy on the part of signing domains. This kind of methodology will carefully consider compromises between robustness and the brittleness of cryptographic signatures in environments. Common, innocuous modifications such as changing the end-of-line wrapping can be accommodated through the use of a canonicalization algorithm that removes such spacing features from the input to the signature calculation.

- Another approach to robustness in this methodology for the modifier of a message is to re-sign the message following the modification. This would typically be the case for mailing lists and commercial services that add advertising, mailing list instructions, or other material to messages. These "third-party" signatures will lead to advantage of trust that certain known third parties will sign only messages that have been legitimately introduced into the system creating white listing environment.

  To guard against downgrade attacks provisions may be made for a number of key management systems. The location of a key record may be specified by a "selector", an arbitrary name for the key and associated information. The initial key management defined through the use of TXT records stored in the signer's Domain Name System (DNS) hierarchy. In addition to the public key itself, the key record contains information such as the algorithms that are used to calculate the signature.

- External parties such as Sending domain may be authorized for E-commerce transactions on their behalf. This is frequently likable to be done by enterprises that outsource some of their services, such as technical support, benefits, and company newsletters. This methodology may provide several different ways of delegating signing authority to such parties. In this approach the external party may be provided a public key that the domain registers by creating a selector for it. If desired, the validity of the key can be restricted to particular addresses within the domain through the use of a tag in the key record. Signing authority for a given domain can also be granted by using NS records to delegate the entire domain key sub domain. This might be done to permit keys to be managed directly by an external entity, such as an E-commerce service provider, or an internal one, like a separate IT messaging organization.

The approaches discussed above may prove valuable tool in the fight against malicious E-transactions in E-commerce system. The message is an important tool enabling reputation, accreditation, and white list systems to aid in more accurate message evaluation.

In present scenario total secured system have become an essential aspect and cause of worry in E-commerce. Like any other technology, White Listing is surely going to play a major role in enhancing the efficiency/performance of an E-commerce system by adding an additional cover to the exiting approaches.

5. Conclusion:

The purpose of this paper is to discuss recent advances in improving security in E-commerce transactions and inspiring research on new methods and techniques to advance security engineering in industrial practices. The ever growing demand in e-security has made it a well recognized multi-disciplinary sub-area across software engineering, security engineering. Information assurance and security has become vital issues in networked and distributed information sharing environments. Security has thus become a fundamental problem in E-commerce hence it is need of the day to focus on developing secure software and understanding the security risks and managing these risks throughout the lifecycle of e-transactions. Finding effective ways to protect information systems, networks and sensitive data within the critical information infrastructure is challenging even with the most advanced technology and trained professionals. The new approach in website security mechanism with respect to E-commerce trust management can be achieved by building systems using white list paradigm which may create credible lock down secure websites.

There is a need to focus on understanding web security and privacy issues, and establishing new collaborations in these areas. Web is connecting people and amplifying the power of working together. Many of these new web technologies rely on the composition of content and services from multiple sources. The white list technology is the promise of inexpensive and easy way to compose secure services. The trust in E-commerce with respect to management of identities, reputation, privacy, anonymity, transient and long term relationships, and composition of function and content, both on the vendor side and consumer side can be enhanced exponentially. Thus, the trust Management in E-commerce through white list Website Security Paradigm may provide a solution as an active defense system to help in preventing huge economical loss to the nation.

References

[1] e-Commerce: Business,Technology, Society (4th Edition) by Kenneth C Laudon and Carol Guercio Traver
[2] Gambetta, D.G. (Ed.). 1988. Trust: Making and Breaking Cooperative Relations. Basil Blackwell., New York.
[3] Deutsch, M. 1962. 'Cooperation and Trust: Some Theoretical Notes.' In M. R. Jones (Ed.), Nebraska Symposium on Motivation, 275-319. Lincoln, Neb.: University of Nebraska Press.
[4] Kraut, R. Rice. R. Cool, C. Fish. R. 1998. 'Varieties of Social influence: The role of social norms in the success of a new communication medium', Organization Science, 9(4) July–August: 437-453.
[5] Kramer R. M. and T.R. Tyler (Eds.). 1996. Trust in Organizations: Frontiers of Theory and Research. Thousand Oaks, CA: Sage: 261-287.
[6] Mishra, A. 1996. 'Organizational Responses to Crisis: The Centrality of Trust'
[7] Mayer. R. C., Davis, J.D. and Schoorman, F.D. 1995. 'An Integrative Model of Organisational Trust', Academy of Management Review, 20(3):.709 – 734.
[8] Sitkin, S.B., and Roth, N.L. 1993. 'Explaining the Limited Effectiveness of Legalistic "Remedies" for Trust/Distrust', Organizational Science, 4: 367-392.
[9] Williamson. O.E. 1974. Markets and Hierarchies. New York: Free Press.
[10] Zucker, L.G. 1986. 'Production of Trust: Institutional Sources of Economic Structure, 1840 – 1920',
[11] Ekeh, P.P. 1974. Social Exchange Theory: The Two Traditions. Heinemann Educational, London
[12] Barber, B. (1983), The Logic and Limits of Trust. Rutgers University Press, New Brunswick, NJ Barney, J.B., and Hansen, M.H. 1994. 'Trustworthiness as a Source of Competitive Advantage', Strategic Management Journal, 15, 175-190.
[13] Cyr, D, Bonanni, C, Bowes, J. and Ilsever, J. 2005. 'Beyond Trust: Website Design Preferences Across Cultures' Journal of Global Information Management, 13(4): 24-52.
[14] Briggs, P., Simpson, B., and De Angeli, A. 2004. 'Trust and Personalisation: A Reciprocal Relationship?' In C
[15] Gefen, D. & Straub, D. 2003. 'Managing User Trust in B2C e-Services', e-Service Journal, 2(2): 7-24.
[16] Corritore, C.L., Kracher, B. and Wiedenbeck, S. 2003. 'On-line Trust: Concepts, Evolving Themes, A Model.' International Journal of Human-Computer Studies, 58: 737-758
[17] Huang, H., Keser, C., Leland, J., and Shachat, J. 2003. Trust, the internet, and the digital divide. IBM Systems Journal, 42(3): 507-518.
[18] Belanger, F., Hiller, J. S., Smith. 2002. W. J. Trustworthiness In Electronic Commerce: The Role Of Privacy, Security, And Site Attributes. Journal of Strategic Information Systems, 11, 245–270.
[19] Koufaris, M., and Hampton-Sosa, W. 2002. 'Customer Trust Online: Examining the Role of the Experience with the Web Site', CIS Working Paper Series, Zicklin School of Business, Baruch College, New York. Available at http://cisnet.baruch.cuny.edu/papers/
[20] www. Marketors.com, e Marketer, January 2008

[21] Survey conducted by Internet and Mobile Association of India (IAMAI) and International Market Research Bureau) IMRB International, 2009
[22] www.internettime.com/blog
[23] www.jtaer.com/documentos/CFP_trust_and_trust_management.Pdf
[24] http://www.sitacs.uow.edu.au/jucs/, Security Journal of Universal Computer Science (JUCS), Special Issue on Cryptography in Computer System, February 2008.
[25] http://www.icsd.aegean.gr/SecPerU2007, SecPerU 2007 3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Held in conjunction with the EEE Istanbul, Turkey, July 20,2007
[26] http://esorics2007.inf.tu-dresden.de / , ESORICS 2008 12th European Symposium on Research in Computer Security, Dresden, Germany, September 24-26, 2008
[27] http://www.cs.umd.edu/~mwh/PLAS07/, PLAS 2007 ACM SIGPLAN Workshop on Programming Languages and Analysis for Security, San Diego, CA, USA, June 14, 2009.
[28] http://www.dfrws.org/ , DFRWS 2007 7th Annual Digital Forensic Research Workshop, Pittsburgh, PA, USA, August 13-15, 2007.
[29] http://www.hgi.rub.de/gocp09/ , GOCP 2007 1st International Workshop on Group-Oriented Cryptographic Protocols, Held in conjunction with the 34th International Colloquium on Automata, Languages and Programming (ICALP 2009), Wroclaw, Poland, July 9, 2009.
[30] http://nss2008.cqu.edu.au/ , NSS 2008 IFIP International Workshop on Network and System Security, Dalian, China, September 20, 2008.
[31] http://ieeeia.org/sisw/2005/, SISW 2005 2nd International IEEE Security in Storage Workshop, San Diego, California, USA, September 27, 2005.
[32] http://www.trustcomp.org/secoval/, SECOVAL 2007 3rd Annual Workshop on the Value of Security through Collaboration in cooperation, Held in conjunction with the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm 2007), Nice, France, September 17-21, 2007.
[33] Callas, J., Donnerhacke, L., Finney, H., and R. Thayer,"OpenPGP Message Format," RFC 2440, November 1998
[34] Ramsdell, B., "S/MIME Version 3 Message Specification," RFC 3851, June 1999.
[35] Fenton, J., "Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)," RFC 4686, September 2006
[36] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", Internet-Draft draft-ietf-dkim-base-10 (work in progress), February 2007.