A Study on Various Security Issues of E-Commerce Business Transaction

Varsha Jotwani[1], Dr.Amit Dutta[2]
[1]CS, AISECT University, Bhopal (M.P.) India.
[2]CS, BU Bhopal (M.P.) India.

ABSTRACT
While the usage of ecommerce application, information and communication technology enhances in private and professional existence, personal data is extensively stored. While service providers require relying on recognizing their consumers, aware characteristics administration and privacy increases into a new assessment for the service user, particularly in the electronic service circumstance. In E-commerce business transactions, buying and selling of products are done over electronic system or by the internet. At this time there are various technologies available to maintain the privacy at the same time.

Keywords:- E-commerce business, Security System, operating System Safety

I INTRODUCTION

Authenticating humans to computers remain a notable weak point in computer security despite decades of effort. Although the security research community has explored dozens of proposals for replacing or strengthening passwords, they appear likely to remain entrenched as the standard mechanism of human-computer authentication on the Internet for years to come. Even in the optimistic scenario of eliminating passwords from most of today's authentication protocols using trusted hardware devices or trusted servers to perform federated authentication, passwords will persist as a means of "last-mile" authentication between humans and these trusted single sign-on deputies. As a consequence, the vast amount of personal information thus available on the web has led to growing concerns about privacy of its users. Today global networked infrastructure requires the ability for parties to communicate in a secure environment while at the same time preserving their privacy. Support for digital identities and definition of privacy- enhanced protocols and techniques for their management and exchange become then fundamental requirements. A number of useful Privacy Enhancing Technologies (PETs) have been developed for dealing with privacy issues and previous works on privacy protection have focused on a wide variety of topics. Among them, for helping users in maintaining control over their personal information, access control solutions have been enriched with the ability of supporting privacy requirements, by regulating access to and release of users personal information. If privacy considerations are taken into account in the design of computer systems, they constrain the possible design space for such systems. Solutions that violate privacy constraints cannot be considered any more. Privacy constraints for computer systems stem primarily from two sources, namely from privacy laws and regulations and from personal privacy expectations of the computer users. Figure 1 shows the hierarchy of these constraints with a focus on privacy laws and regulations [1].

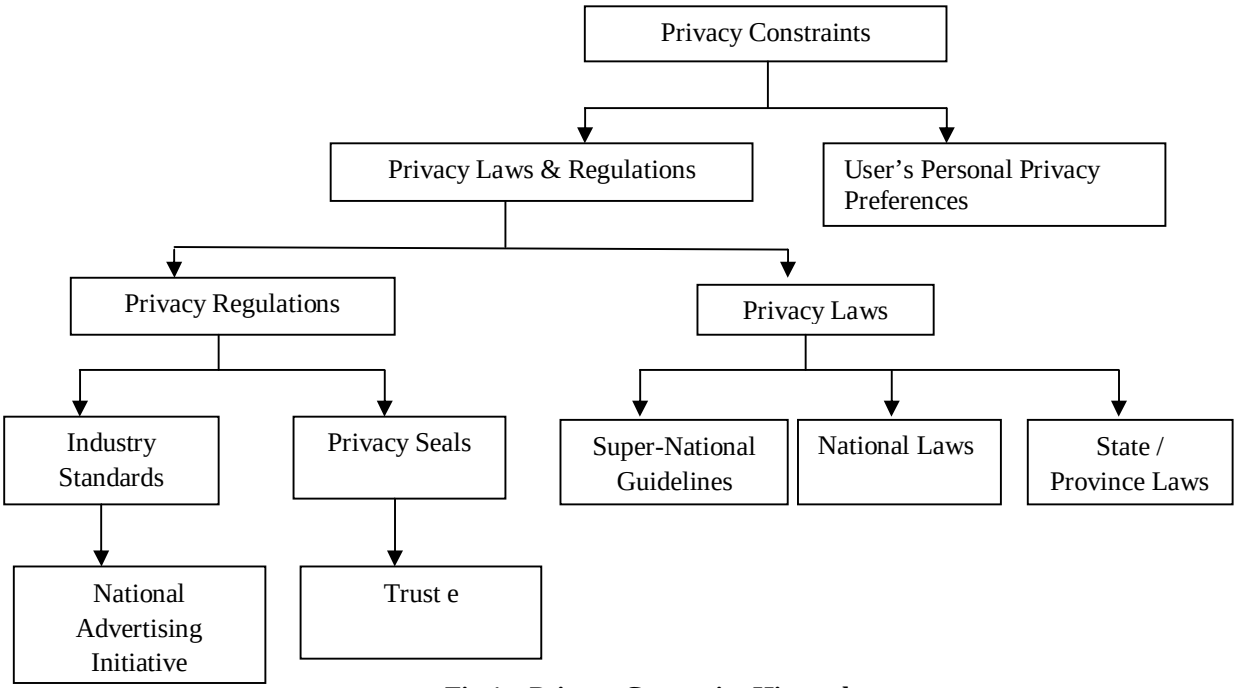

Fig 1 – Privacy Constraint Hierarchy

The need of user authentication is a fundamental security requirement in computer society. With wide-spread of distributed computer networks, remote user authentication has been introduced to identify a user remotely, and has been widely studied [2], [3], [4]. In general, authentication services may require three factors, i.e., password, smart card and biometric characteristics. The authentication based on a password is called password-based authentication i.e. Facebook login system. A system which authenticates users by using password and smart card is called two-factor authentication. In which, a client can pass authentication only if the client has correct password and the corresponding authentic smart card. The biometric-based authentication mainly employs the biometric characteristics, e.g. fingerprint, palm print, and iris. Three-factor authentication is introduced to incorporate the advantages of the authentication based on password, smart card, and biometrics. A well designed three-factor authentication protocol can greatly improve the information assurance in distributed systems. The earliest user authentication mechanism through the Internet is based on password.

II SECURITY CONSIDERATION AND ITS CONCEPT

The major security issues that may exist during the transmission of data are as follows:

(a) Confidentiality: It should be computationally infeasible for an adaptive attacker to gain any partial information on the contents of a text, without knowledge of the sender's or designated recipient's private key.

(b) Unforgeability: It should be computationally infeasible for an adaptive attacker to masquerade an honest sender in creating an authentic text that can be accepted by the other algorithm.

(c) Non-repudiation: The recipient should have the ability to prove to a third party (e.g. a judge) that the sender has sent the text. This ensures that the sender cannot deny his previously texts.

(d) Integrity: The recipient should be able to verify that the received message is the original one that was sent by the sender.

(e) Public verifiability: Any third party without any need for the private key of sender or recipient can verify that the text is the valid of its corresponding message.

(f) Forward secrecy of message confidentiality: If the long-term private key of the sender is compromised, no one should be able to extract the plaintext of previously texts.

III E-COMMERCE SAFETY STRATEGY

(a) The E-Commerce Network Devices Safety Security Strategy- The security strategy of E-commerce system level often consisted by system isolation, access control and authentication technique. System isolation is an effective isolation way in e-commerce operation process. Isolation means dividing the network into several non-communicating networks according to the difference of network security level, so that the networks or devices of different security levels have no access to each other and get the safety isolation goal. At the present stage, we often take VLAN network technique based on the original isolation way to segregate the service network or the office network, by this we can set effective and reasonable access strategy to executive access strategy of different network resource and prevent illegal users visit the protected resource. The main way and strategy is according to the access control list and security strategy to control the information flow, to check and filter network information and data, to screen out the effective and reasonable data and to intercept unsafe information and data. The interception means after the scanning, tracking and early warning to network system, distinguish it initiatively, timely and effectively, and then block it. This process will check and analyze the network device and the security holes, including network service, firewall, router, mail servers and web server etc. As to end-customers, we often use the authentication which is used on e-commerce customers, for example, electronic business links network account, account password, dynamic password, Ukey secret key, IC card, magnetic card, fingerprint technique etc. By all means ofauthentication, we prevent illegal users visit enciphered data, ensure the identity materials, property information and other data will not be revealed, tampered or destructed [5-6].

(b) The E-Commerce Operating System Safety Security strategy- Operating system is in charge of device management, data storing, information sending and the scheduling of all kinds of system resource, the security of operating system directly influences the safety of application system and information data. When we test the security of operating system as the server-side, we should scan and analyze different versions operating systems, divide operating systems according to their security risk level, make test report about the security hole of system based on the scanning result and repair the data hole leakage and system bug in time, so to protect applications and data from embezzling or

destructing from the server system level. As end-customer, when choosing the operating system which that suits us, we should try to avoid installing dubious software, protect and back-up the system. When some abnormalities occurred, we should recovery system and reduce the damage to e-commerce transaction course caused by operating system.

(c) Strategy of E-Commerce Data and Document Security- When e-commerce is running, the storage and transferring of most text documents, pictures and applications need to depend on the management and operation of computer files. So the security strategy of computer files storage and transfer process becomes the key focus of e-commerce operation process. As to the transfer of file information in e-commerce, we can use security disposal mechanism like encryption, electronic signature, integrity authentication etc. to make effective security disposal and let the transferred files can be only deciphered and read under the condition the receivers use related security identification mechanism. This kind of security precaution strategy took during the file transfer to some extent reduce the possibility of the files being intercepted, tampered or destructed. As to the storage security of e-commerce files, we can use the way of authentication and password protection taking effect simultaneously. The important files stored in local network or the network is in the state of double-encryption, even when the others get the file by illegal way, he also needs to crack two security protection precaution strategies if he wants see the content of the file. To take effective security precaution on storage and transfer of e-commerce files can prevent external illegal incursion and internal information revealing. The files and data in the operation of e-commerce enterprises depend on database to be stored. In database itself, the security level and system level security can meet the routine application of enterprises. By changing database password regularly, improving password strategy, managing database hierarchically, we can achieve the goal of overall process encryption and control for the visiting, access and transfer of database [7].

(d) Strategy for the safety of ecommerce Transaction- An e-commerce transaction involves the identity verification of all involved parties, the application of digital certificate and digital signature, and the encryption of transmitted commands and data under SSL protocol. Compared with traditional commerce, e-commerce is encountering some new problems, such as the information leakage, revision and falsification as well as attacks from computer viruses. Therefore, safe and reliable communication networks should be established to ensure the security of the data and information as well as the promptness, effectiveness, reliability, integrity and confidentiality of e-commerce transactions. In the e-commerce transactions, there are two major security standards, namely, SET (Secure Electronic Transaction) at the application layer and SSL (Security Socket Layer) at the session layer. SET protocol is a security standard raised by VISA and MasterCard for protecting e-wallet, e-mall and certificate authority. It is used to protect the confidentiality of information and the reliability of data and identify the accounts of both the buyers and the sellers [8].

IV CONCLUSION

In the globalization of economy, e-commerce brings great influences on economy, politics and law. There are many strategies for e-commerce security: developing the education and training of e-commerce in enterprises to improve their security consciousness; adopting multi-layered network and cryptography to guarantee information security; enhance risk analysis, prevention and control to reduce system risk; complete e-commerce legislation to guarantee the interests of all involved parties.The research on e-commerce security strategies will help to improve e-commerce security techniques, complete e-commerce management system, create conditions for the healthy development of e-commerce and inject new vitality into e-commerce.

REFERENCES

[1] GWang, Y. and kobsa A. (2009). Privacy-enhancing technologies. In Gupta , M. and Sharman, R., editors, Social and Organizational Liabilities in Information Security, pages 203–227.

[2] A. K. Jain, A. Ross, and S. Pankanti, “Biometrics: a tool for information security,” IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, 2006.

[3] J. Yu, G. Wang, and Y. Mu, “Provably secure single sign-on scheme in distributed systems and networks,” in TrustCom, 2012, pp. 271–278.

[4] G. Wang, J. Yu, and Q. Xie, “Security analysis of a single sign-on mechanism for distributed computer networks, ”IEEE Trans. Industrial Informatics, vol. 9, no. 1, pp. 294–302, 2013.

[5] D.Mao, “A study of Consumer Trust in Internet Shopping and the Moderating Effect of Risk Aversion in Mainland China”,Hong Kong Baptist University Hong Kong Hong Kong,(2010)

[6] D. J. Kim, D. L. Ferrin and H. R. Rao, “A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents”, Decision support systems, vol. 44, no. 2, **(2008)**, pp. 544-564.

[7] S. A. Majore, , H. Yoo and Taeshik Shon, “Next Generation Electronic Record Management System based on Digital Forensics v”, International Journal of Security and Its applications, vol.7, no.1, **(2013)**, pp. 189-194.

[8] P. A. Pavlou, “Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model”, International Journal of Electronic Commerce, vol. 7, no.3, **(2003)**. pp. 69-103.