ISBN 978-952-5726-07-7 (Print), 978-952-5726-08-4 (CD-ROM)
Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09)
Huangshan, P. R. China, 26-28,Dec. 2009, pp. 483-487

Study on Protection Measures of People's Information Privacy right in E-commerce

Xiaoming Meng
School of information, Guangdong University of Business Studies
Guangzhou, Guangdong, China
mxm_me@163.com

***Abstract*—Define the basic content of people's privacy information and information privacy right in E-commerce, analyze the creating reasons of the problem about people's information privacy right in E-commerce, point out some protection measures of people's information privacy right in E-commerce in four aspects, such as to improve people's safety awareness, to make good external environment of E-commerce, to improve the safety performance of E-commerce system, to prevent malicious attacks, and on the points of view such as the information security management, privacy information protection technology, law, management, humanities and social sciences and many other subjects.**

***Index terms*—E-commerce, privacy information, privacy right, information security**

Ⅰ. INTODUNTION

Now, the network and E-commerce is being applied widely and deeply, but at the same time, some illegal businesses or individuals driven by interests collect, theft, eavesdrop, intercept, destruct and spread the business privacy information of the people who take part in the E-commerce by adopting a variety of technical measures, and using the opening inherent weakness and technical loopholes of internet. All above invades the rights of people's information privacy, affects the people's trust for E-commerce, and constrains the rapid developing of E-commerce, and is not conducive to social stability and harmony. How does protect the people's information privacy right in E-commerce has become a focus problem that should be studied and discussed.

Ⅱ. CONTENT OF PEOPLE'S PRIVACY INFORMATION AND PRIVACY RIGHT IN E-COMMERCE

A. *People's Privacy Information in E-commerce*

The people's privacy information in E-commerce means that the information and data which is not known willingly in E-commerce activities, that is the people's privacy information. According to the characteristics, the people's privacy information can be divided into two categories: static privacy information and dynamic privacy information.

(1) The static privacy information means that the privacy information which is not on line, express and access in static type, such as the personal basic information, trait information, special information and trust information etc..

The personal basic information includes name, sex, age, hometown, political landscape, workplace, telephone number, address, E-mail which are used to describe the people's basic status, and job title, ID number which are used to describe the people's ID.

The trait information includes personality, voice, history, marriage and fertility status, family members, social relatives, height, weight, experience, property status, living preferences, measurements of women, etc.

The special information includes archival material, live or work or business activity logs, technical or commercial important documents, and the privacy information which is stored in a bank or certification center, computer cache, cookie, a temporary files etc.

The trust information includes loan records and the amount, business reputation, status to fulfill contractual responsibilities of law, status to implement the obligations etc. It is used to evaluate trust level.

(2) The dynamic privacy information means that the privacy information which is online, express and access in dynamic type. It includes online transacting information, secret information being transmitted online, and trace of network activities.

The online transacting information includes the account and password of credit card, consumer card and network card etc., and the information during payment and being transmitted and accessed online.

The secret information of all kinds of files being transmitted online includes e-mail, contract documents, business confidential documents, corporate strategic plan, decision programs, private documents, etc., which are transmitted online.

The trace of network activities includes IP address, online trait and privacy etc.

B. *People's Information Privacy Right in E-commerce*

People's information privacy right in E-commerce is a basic right in E-commerce era. It involves every part of the people's information collecting, transmitting, accessing and processing, such as:

(1) Right of privacy is not been peeped and intruded. It means that the privacy information shall not been peeped and intruded without being permitted.

(2) Right of privacy is not disturbed. It means that the network should be smooth and may not be intentionally interfered during online trading and online transfer

private information.

(3) Right of privacy is not been illegal collected, used and arbitrary spread. It means that the privacy information, such as personal basic data, special information, secret data, trust information, transaction information, trace of business activities online etc., is not been collected, used and spread without being permitted.

(4) Right of privacy is not been updated. It means that the privacy information, such as personal data, trust information and other important business information, should not be updated, tampered and distorted.

III. CAUSING REASONS ANALYSIS ON PEOPLE'S INFORMATION PRIVACY RIGHT IN E-COMMERCE

There four main reasons causing the problem of people's information privacy right in E-commerce. First is that the sense of security safeguard is weak. Second is that the E-commerce external environment is not perfect. Third is that the security measures of E-commerce system is not strong. Forth is that the malicious attacks come from various aspects [1].

A. The Sense on Security Safeguard in E-commerce is Weak.

In e-commerce, people is as the main part of business, but due to most of them have weak security awareness and the lack of the necessary security technical knowledge, and can not comply with or ignore safety operation, leading to private information disclosure and privacy be violated.

(1) Sense of security safeguard is weak. For examples, it lacks of the sense of security protection, adopts unsafe operations in E-commerce.

(2) There is no good security operation habit in E-commerce activity.

B. The External Environment of E-commerce is not Healthy.

The external environment of E-commerce includes laws and regulations, third-party services (such as bank, authentication center, credit management and credit service, logistic and distribution, etc.), human ethics, computer support technology and so on.

(1) On the aspect of laws and regulations related. Although the "Digital Signature Law" promulgated and implemented and the "Personal Information Protection Law" will published very soon in China, and there are many items in most of our laws and regulations. However, there are many shortages existed in the existing relevant laws and regulations, such as the laws and regulations is still not completely and does not form system, law enforcement strength and punishment intensity are not enough, lack of incentives, lag behind the development of E-commerce.

(2) On the aspect of third-party services. Due to the constraint of laws and regulations is not very strong and the standards and norms are imperfect, these will lead to make various phenomenon of invading people's privacy right, such as to obtain the account and password of the bank cards and credit cards of users by cheating, stealing, testing and many other means, and will lead to false identity authentication; credit information management and credit services are imperfect, and will lead to credit information has been tampered, credit level distortion.

(3) On the aspect of human ethics. Now, the social credit system is imperfect, the honest and trustworthy social climate is forming. So the fraud, theft, distortion, and wanton dissemination of people's privacy information occur sometimes.

(4) On the aspect of public network security. Some network corporations and Websites can not obey their promise to protect the customer's privacy while they provide network services, father more, they deliberately distribute, sell people's privacy information, and the result is that the people's information privacy right is harmed.

(5) On the aspect of privacy protection technology. Because the information on internet is transmitted by the router, so some illegal persons or organizations steal user privacy information by scanning the key nodes and tracking the transmitting activities. In addition, while data warehouse, data mining technology is rising and using quickly, some illegal persons or organizations process and utilize the personal information indiscriminately, and these make the people's privacy information revealed.

C. The E-commerce System has not adopted Effective Safeguard Measures.

Now, most of E-commerce systems have no any effective safeguard measure in program design, network and system architecture, data security connection and management, identification and authentication, firewall configuration, intrusion detection and prevention etc. This leads the people's privacy information disclosure, and the right of people's privacy has been infringed.

(1) There are many shortcomings on developing trading software and bad behaviors of application development. For examples, ASP, JSP, J+ +, J2EE, WebService, etc., all of them exit some shortcomings. This often leaves a lot of "backdoor" and provides the interface for illegal users to load the application module (such as Trojan horses, etc.).

(2) It has not taken physical isolation measures between intranet and extranet, network and storage media. This leads to an intruder invades the internal network through external network to get the privacy information stored in the internal computers. As well as, neglecting the hierarchical management of the security and the logical isolation of the internal network information system will lead the people's privacy information disclosed.

(3) It does not use the ODBC method to connect with databases, but use direct accessing will lead the database information disclosed.

(4) The accounts and passwords are too simple in user identification and authentication, the password, this is easy to be cracked or guessed.

(5) There is no firewall or the firewall setups very simple and unreasonable, this leads the illegal invaders to steal secrets easily bypass the firewall.

(6) The lack of proactive intrusion detection, identification, forensics and other security measures leads the variety of network intrusion rampant fraud invading the network and leads the privacy information disclosed.

D. The Malicious Attacks come from Various Aspects.

Now, the malicious attacks include worms, backdoors, Rootkits, DoS, and Sniffer, etc. In recent years, malicious attacks in E-commerce are becoming more intelligent, the attack tactics are escalating renovation, and harmful level is increasing. According to analyzing, the main malicious attacks on privacy information in E-commerce shows bellow [2].

(1) Monitor and password attacks. Because many of the agreements encryption or authentication technology have not adopted in every application-layer of E-commerce security system, and the user account and password information is transmitted in plain text format. This leads the attackers to make data monitor, to intercept confidential information transmitted by internet, public telephone network, line or installing receiving device in the range of electromagnetic radiation. Or, they infer useful information, such as bank account number, password and so on, by analyzing the volume of information flow, flowing direction, parameters of communication frequency.

(2) Network spoof attacks. By redirecting ARP cache communication data packets, rewrite the address mapping form the target machine's IP address to Mac, and leads the packet sent to the listener by the switch machine. This will lead privacy disclosed. The main methods of spoofing include Web spoofing attacks, TCP/IP spoofing, DNS spoofing, IP or name spoofing attacks.

(3) WWW attacks. This kind of attacks always use Java, ActiveX, JavaScript etc. to rewrite URL address and relative information to realize attacking.

(4) Trojan attacks. It is based on the network C/S principle, the attackers install C/S programs which communicate by ports on your computer, and the special programs will start when the computer operates in order to control the computer or steal important information.

(5) Buffer over flow attacks. Attackers can join attack codes, and enhance access right and control the computer when the buffer is overloaded if the buffer areas is overloaded and is not controlled.

(6) Rootkits attacks. Because the rookits is promised by attackers to access by backdoor, this will give a chance for attackers to start a Trojan to make attack or steal people's privacy information.

(7) Port attacks. The attackers can make attack by banding a Trojan to a legal port and get a legal ID, and enhance the right to get higher account and password.

(8) Sniffer backdoor attacks. The attackers can make attack by working under the hybrid / non-promiscuous mode.

(9) State manipulation attacks. The attackers can achieve the illegal visiting purpose by modifying the sensitive information, hidden form elements, and cookies in URL.

(10) SQL code embedded attacks. The attackers can make attack by inserting database query commands in the user input to realize database query, modify, and delete data and so on.

The harm of these malicious attacks is: attack the E-commerce system, to undermine the reliability of trading systems; disguise legal status, to undermine the authenticity of transaction identity; copy and theft of trade secrets, to undermine the confidentiality of information; tampers and delete information, to destruct the integrity of information; update and change information, to undermine the validity of information; invade the information system of certification department, to destruct non-repudiation of transactions.

Ⅳ. PROTECTION MEASURES OF PEOPLE'S INFORMATION PRIVACY RIGHT IN E-COMMERCE

How does prevent exposure the people's privacy information to protect their privacy right in E-commerce activities? Survey shows [3-4]: In the Internet users, there is 50% consider that increasing their own protection awareness is most important, 29.17% believe that installing a firewall and anti-virus software is important, 11.96% think that the important data is not online is a good idea, there are 6.88% consider that downloading the security patches regularly is very important. But the legal professions think that should speed up the construction of the relevant laws and regulations to protect the right of people's privacy in E-commerce. I believe that we should do the following four aspects well.

A. To Improve the Protection Awareness of People

(1) Should cultivate and improve the people's protection awareness

Because that the most privacy information disclosed events happen in "unconsciously", so it needs to strengthen the protection awareness and ability of privacy protection in E-commerce, such as education and training, to make peoples protect their own privacy right consciously.

(2) Should improve the people's security ability and make them have a good security operation habits.

The good security operation habits to protect privacy information in E-commerce includes: right use and setup Cookie, install privacy protection software and Cookie process software, protect password (it is not simple and general, do not access password), filter and mask threatening ActiveX, erase the traces of computer timely, hide or encrypt secret data, refuse the access come from threaten Website, install firewall, protect IP, use agent server, update the BUG of Windows generally, hide IP, plug the loopholes, erase "the documents saved" and "log files" and "attribute information of files" and "the history records in favorite".

B. Improve the External Environment of E-commerce

(1) Establish and improve the relevant laws and regulations to protect information privacy right of peoples

In China, the present laws setup on information privacy right is later than other country. The present laws are only relating to the Constitution, criminal law, civil commercial law and other, but there is no special law on protecting the right of people's information privacy. It should expect that the "Personal Information Protection Law" has entered the ranking of stage and will soon be promulgated and implemented.

In addition, the existing laws and regulations on privacy right protection are seriously lagging behind the rapid development of E-commerce. So we suggest that, while we setup laws, they should have a certain perspective, fully predict and estimate the development of E-commerce in future and the privacy violations that may occur; formulate relevant laws and regulations should take into account interests between information service provider and network application service provider, and peoples, and make be balance and coordination between them.

(2) Strengthen the integrity and moral setup, improve social credit system and credit management, to regulate credit information service

First is that it should strengthen education for peoples and make them respect for the privacy of others, and form a good social habit.

Second is that it should improve the social credit management system, solve the longstanding problems in the process of building a social credit system, and truly solve is credit information bottleneck.

Third is that it should improve credit information service management, evaluate the level and rate of credit service organizations, and make them have a high credit level first.

(3) Strengthen application study on network and information security technology applied in protecting privacy.

The technologies on protecting the people's information privacy right include digital certificate and encryption technology, P3P technology, firewall technology, invading checking technology, and information camouflage technology (such as digital watermarking, data hiding and data embedding) etc.

C. Improve Security Ability of E-commerce System

(1) E-commerce system developers should have good programming habits, take effective measures to seek to complete the procedure and software, eliminate the "back door" invasion of infringement behaviors (Trojan horses, etc.) to protect people's privacy information accessed without authorizing. In addition, they should update the system software and make "patchs" timely.

(2) Should adopt the physical isolating measures between internal network and external network, and between network and storages, to protect privacy information.

(3) Accessing databases should use ODBC dynamic link technology, but not use direct access method. This can reduce the choice of information in database disclosed.

(4) Should adopt long password in user's identity identification and authentication to increase the difficult of them cracked or guessed.

(5) Should install firewall software to prevent the illegal intruder to steal secrets.

(6) Should take a active intrusion detection, identification, forensics and other security defense measures to detect and screen a variety of network fraud intrusion.

D. Prevent Malicious Attacks

There are two steps to prevent malicious attacks. First is the malicious attacks detected. We can use detection technology to make real-time track, analyze and discover the malicious attacks in E-commerce. Second is adopting preventing measures to prevent malicious attacks.

(1) Detecting for the malicious attacks

The malicious attacks detection technologies include intrusion detection technology, trap technology and forensic technology [2].

Intrusion detection technology is based on Statistics and Fuzzy Logic to analyze. It is adapted to detect the malicious attacks that have anomalies. But it is difficult to detect network spoofs, Trojans and other hidden attacks.

Trap technology is based on making simulation network environment, setup loopholes to decoy attacks. It is adapted to the attacks which realize the gore by repeating test, such as sniffer backdoor. But it is difficult to detect embedding attacks and spoof attacks and denial service attacks.

Forensic technology is based on installing agents, creating diary log records to obtain proofs by analyzing. It is adapted to get proofs after attacked. But it is difficult to detect all kinds of present attacks.

(2) Prevent malicious attacks

We can adopt bellow technique measures to prevent the malicious attacks in E-commerce.

First is encryption technology. It is the main security preventing measure in E-commerce. It includes general encryption physic, data encryption standard (DES), symmetric encryption (private secret key cryptography system), asymmetric encryption (public key cryptography system), and symmetric secret key management.

Second is digital authentication and digital signature. We can use this technology to prevent data updated, confirm identification, prevent deny.

Third is identification center. It is used to provide identification identify and credit services.

Forth is to install firewall on the users' computers.

Fifth is SSL and SET security technology. These technologies are the key security technologies in payment system in E-commerce. We can use them to improve confidence, to guarantee information completion in trading, to improve security and reduce spoofs in E-commerce.

Sixth is security scan. It is an important technology in network security prevention. It is used in port scan, loophole scan to make intrusion detection.

Seventh is physical isolation. It is used to realize departing from internal and external, to avoid damaging from hacks and to protect privacy.

Eighth is to prevent monitoring and spoofing. We can use hard coding, IPSec, VPN and other encryption technologies to protect sensitive information.

Ninth is to prevent Web service attacks. It is need to strengthen the professional training for application developers to void various loopholes remained while they are developing software.

Tenth is XML technology. We can use XML technology to establish effective mechanisms to ensure the information flow safe transmitted, and to realize the trade security in E-commerce.

Eleventh is P3P technology. Using P3P technology in E-commerce can realize the safe transmitting of dynamic information and security protection of static privacy information, and prevent various attacks to steal the transaction information.

Twelfth is digital watermark technology. Because watermark has robustness, transparency, anti-aggressive properties, and low complexity, etc. We can use it to realize identifying and information hiding to protect information transmitted in E-commerce safe.

Thirteenth is voice or fingerprint identification technology. We can use both of voice/fingerprint and encryption technologies to realize double identification to improve the security of E-commerce, and it is effective for anti-repeat attacks.

Fourteenth is smart card and middleware technologies. We can use them to realize “hard program” to overcome the shortages of traditional security technologies.

Fifteenth is information camouflage. The camouflage can be divided into basic camouflage, watermark, data hiding and embedding technology [8]. We can use the special characters, such as hiding, security, correction and so on, to realize information hiding, right of information identification, identity identification etc.

In a word, in practice application, we should comprehensively use many of them to build integration security environment to improve the level of protecting privacy information safe in E-commerce, and to prevent malicious attacks come from every aspect.

Ⅴ. CONCLUTIONS

It is a complex system engineering to protect the people’s information privacy right in E-commerce. It not only involves the security problems of E-commerce privacy that is transmitted dynamically, but also includes the security problems of E-commerce privacy that is been storage statically, it is not merely a technical security problem but also includes the non-technical problems such as laws and regulations, strategy measures, credit system, commercial idea and so on. In the process of E-commerce developing, we want to solve the preventing problem of people’s privacy information right in E-commerce, to promote the health and fast developing of E-commerce, to protect the privacy right of both sides in E-commerce transaction, to promote the harmonious development of society. The first thing we must do is that to establish and perfect the corresponding laws and regulations and the social credit system, to build the honest and honor, health and harmonious humanities social environment. The second thing we must do is that to make the rules of safe operation for E-commerce, to draw up effective managing, strategies and measures of protecting privacy. The third thing we must do is that to improve the security performance of E-commerce software, to foster good habit of developing application programs, to strengthen the security measures of protecting the databases of E-commerce, to promote the studying on the technology protecting E-commerce privacy. Therefore, this article overcomes the one-sidedness existed in formerly studying such as "the heavy theory but light practice, the heavy qualitative but light quota, the heavy management but light technology", it has certain theoretical and practical significance for protecting the privacy right in E-commerce and for promoting health and fast developing of E-commerce.

Ⅵ. ACKNOWLEDGMENT

This work is supported by Philosophy and Social Sciences Foundation (07O05) of Guangdong Province, China.

REFERENCES

[1] Xiaoming Meng. “Study on safeguard measures of network privacy”. *Modern Library and Information Technology, Peking, China*. 2005(4), pp.92-95, 91.

[2] Xiaoming meng. “Study on detection and prevention technology for malicious attacks in E-commerce”. *Electronic Commerce Study, Peking, China*, 2006(4), pp.43-48.

[3] Licahng Guo. “How to protect privacy right using laws”. *Guangming Daily, Peking, China*, 22th. August, 2008.

[4] Tianwen Xu. “Principles and thought on privacy right in China”. *Journal of Zhuhai Municipal Administration Institute, Zhuhai, China*, 2007(2), pp.57-60.

[5] Yan Ceng, Bin Cheng, Zhonglin Liu. “Discuss network privacy right on the view of legal, thechnology and ethics”. *China Information Review, Peking, China*, 2006(2), pp.32-35.

[6] Wenjuan Wei. “Discuss on the legal protection of network privacy right”. *Legal System and Society*. Yunnan, China, 2007(1), pp.286.

[7] Xiao Hong. “Discuss on construction of network privacy right protection”. *Library Theory and Practice, Peking, China*, 2006(5), pp.38-39.

[8] Yixian Yang. “Information camouflage and security”. *Computer Security, Peking, China*, 2002(11), pp.50-53.