Security Forensic on E-commerce

Rongsheng XU
IHEP Computing Center
Chinese Academy of Sciences

Abstract: E-commerce could not be further developed without sufficient security. To deal with daily rampant Hackers, Forensic technology on E-commerce should be considered with the prevention issues, so that safe E-commerce could be insured.

Key Words: E-commerce; security; forensic

While bringing people conveniences, Internet gives rise to the problem of security simultaneously. It’s the same that when traditional commercial mode applied on Internet, it brings about many problems of security. The security is of great importance in financial affairs, systems that need high speed verification and authentication, the E-commerce Website and the database etc.. As we know, E-commerce is often subjected to the attack and the cheat of hackers. With the development of E-commerce, hacker attacking becomes more and more serious so that it now turns out to be an important aspect that interferes the development of E-commerce. Nowadays Chinese government puts great emphasis on Internet security, and the newly established National Computer & Information Security Management Center is the infrastructure that prompts all levels of work to strengthen the security of network.

Although network security companies are striving to develop detecting & forewarning products against cheat and intrusion, there’s no absolutely effective method against hacker intrusion, whereas hacker could continually find the flaws of the open system, and intrude into the network system of E-commerce at anytime, which cause interference and damage to E-commerce. Therefore, security becomes a problem that should be concerned by the trade of E-commerce insurance as to how to utilize the forensic technology against the hacker intrusion and damage. In this essay, we will discuss the forensic technology in E-crime elementarily.

There are many methods hacker uses to attack and destroy network systems, which include the typical the intruding based on internet application (i.e. remote log-in, anonymous file access, WEB and mail service) and other non-authorized access, detection before attack, protocol decode, system proxy attack, etc. As to the inner hacker, particular attention should be paid to such deeds as obtaining super-user
authority, using source beyond authority, illegal operation, modifying information, and exposing information etc.. In addition, we should be wary of the illegal installation of such Trojan Horse software that could implement refuse-service attack. Furthermore, hacker could alter the login program to a postern one, which works as the normal login program, yet could capture the user password without being noticed. Thus we should use the firework technology for the safety defense of network, safety scanning tools for detection of flaws and vulnerability. Finally don’t forget to backup the system files so as to recover in time in case of being attacked.

It’s not neglectable and of great importance to prevent future trouble by seizing the invader with effective monitoring methods. Hitherto there’s no arbitrage or justice organization in charge of E-commerce issue, nor corresponding law on E-commerce to solve the it. Thus it’s a great difficulty in the field of E-commerce to judge the conflict. Therefore, we should use tools to actively monitor the status of host and the alteration of key files while defending against the hacker intrusion. To capture signals is to collect evidence in the part of spot being attacked.

In the society, there are many effective legal methods that could be used to collect enough evidence for such crime as theft, homicide shortly after the court receives the case, then it turns to analyze and solve the case. While in the virtual world of network, finding an obvious network intrusion or attack could not be cited as a direct proof in court, as the recode of digital itself is liable to be fabricated and juggled. For example, once a homepage was attacked by hacker, but you could not bring a suit against the attacker with the record in the hard disk of your server. This kind of digital proof could not be simply accepted by the law organization, as the third party and even more people or program could alternate or cover the original record, thus it’s impossible for us to obtain proof and clues for such digital crime so quickly as we could do in the realistic society by obtaining the fingerprint or using such tools as police watchdog.

It is a worldwide difficulty to obtain the proof of intrusion or being attacked by taking measure on a machine itself, but it is the digital forensic technology that is of help to solve it. However, hitherto there are not enough tools or products available to provide for the legal justification even though the domestic departments concerned have been paid close attention to the computing forensic research work. It is reported that once several lawyers couldn’t submit the exact computing documental proof in their hands to the court as current acknowledged legal proof after they received some enterprises’ knowledge property right cases. That is to say, if these electronic documentation is not obtained on the spot, or by the notary public directly, it cannot be cited as legal proof.

In order to solve the problem of an objective network and computing forensic of crime with the legal effect, some specialists are making a series of experiments that
investigate into the digital crimes. In the future, the record made by a computing forensic system is just like the black casket on the airplane, which can provide the accessory data to detect and obtain proof, with the characters of guard against destroy and juggle.

The technical difficulty for digital forensic is, first, how to bypass the recording devices, which is transparent for both user and hacker, so that it wouldn’t reduce the efficiency of E-commerce, but prevent the auditing devices from potential attack and ensure the security of the digital forensic system itself by using various self-protections. Second, the recording speed and space require enough hardware and software with certain analysis capability. Third, how to ensure the record obtained against being juggled, that is the probativity of the notarization. On the basic of these records, the court can analyze the time, location, actions and other proofs concerned.

China is developing the future Broadband network with fiber technology that is able support the latest IPv6 as well. So we should correspondingly develop the new detection and forensic technology against intrusion in Broadband network, the new network security system structure model and the new network security control platform, to meet the needs of the future E-commerce.

We begin to cooperate with the National Patent Bureau in this field, and we keep contact with some legal institutions. It is one of the most strategic work, so we look forward to achieving more approval and assistance from authority of E-commerce, and investment from enterprises. We can say that security technology cannot ensure network security absolutely, but as for the network society, enterprise and personnel can obtain the insurance from network forensic.

(The author is researcher of CAS, chief of the project of the Prevention System Against Hacker Intrusion, which is one of the Innovative Knowledge of Chinese Academy of Sciences)