ISSN:0975-9646

Cyber Attack Detection Techniques – Solutions

P.Vishalini,
Lecturer in Computer Sceince

K.Swaroopa Rani,
Lecturer in Computer Sceince

Ch.Vimala,
Lecturer in Computer Sceince

Abstract: The intensification of Information and Communication Technologies usage in all facets of life exceedingly amplify the incidents of information security policy breaches, cyber crimes, fraud, commercial crimes, cyber laundering etc, hence require a well developed approach to tackle these incidents in order to realize legally defensible digital evidence. Since electronic evidence is fragile and can easily be modified, finding this data, collecting, preserving, and presenting it properly in a court of law is the real challenge. There is a need for use of semantic analysis to discover underlying security policy requirements and internal power structures and institutionalization of anti cyber attack, anti money-laundering and regulatory schemes. The first responders to cyber security incidents often than always are an organization ICT personnel who are technically sound though may be deficient in investigative skill. The scientific standards of cyber forensics dictates the procedure as it promotes objectivity, a precise and well documented analysis, particularly that the findings may be used as evidence against the attacker. This paper aims to contribute to the advancement of the cyber forensics discipline with a view to assist the International community in combating this sophisticated, high-tech, dynamic ever changing phenomenon.

INTRODUCTION

The computer crimes affect our daily lives and national security deeply, especially in this information epoch, the expanding wave of Internet connectivity and digital technologies bring us a lot of convenient, at the same time they also offer criminals more chance to commit crime.

Traditional law enforcement tools, methodologies and disciplines do not successfully address the detection, investigation and prosecution of cyber crime and this dictates for a proactive approach, for timely international cooperation, and for effective public private partnerships to ensure the upper-hand over criminals. Cyber forensic may be defines as the process of extracting and analyzing information and data from computers, network and storage medias and guaranteeing its accuracy and reliability or the process of investigating what has occurred in a computer system, networks etc, how to prevent it from recurring, and establishing the extent of the damage. With the rapid development of electronic commerce and Internet technology, cyber crimes have become more common and sophisticated. Incident response for the purpose of this paper may be defined as structure approach to addressing and managing the aftermath of a security breach of attack and the countermeasures.

BACKGROUNDS

Cyber crime is not actually new , the first recorded cyber crime took place in the year 1820. However, cyber crime is the latest and perhaps the most complicated problem in the world, and comes in different forms and sizes unlike the conventional crime. This high-tech crime compelled the development of cyber forensics and incident response to address cyber security.

CYBER FORENSICS APPLICABILITY

Technology is a double edged sword that can be used in economic sustainability, to assist in the arrest of cyber criminals etc, and there are various tools that can assist law enforcement agencies in investigating cyber crime cases and in cyber crime evidence collection, drafting and creating hard evidence, however the same technology may be used by cyber criminals to commit offences worse still the forensic tools may also be used by these cyber criminals to conceal their tracks for instance a criminal may use the disk wipers to clean the hard disks rendering forensic tools immobilized to recover evidence. There are major investigative contingents that drive the requirements for purpose of this study emphasis is on five categories:

- Law Enforcement : focuses on gathering evidence
- Organization, Business or e-commerce-economics: for use in keeping the business on track using reasonably effective techniques and ensuring safe online purchasing.
- Academia: ensures accuracy of result driven from precise, repeatable methods.
- Prosecution: elaboration of the analysis in a court of law
- Judiciary: scrutinizing the findings against judicial standards

When critical assets and systems come under attack, security professionals must be able to gather electronic evidence and utilize that evidence to bring to justice those who are responsible. Cyber criminals, honest and dishonest employees hide, wipe, disguise, conceal, encrypt and destroy evidence from storage media using a variety of freeware, shareware and commercially available utility programs. Such attacks are often the results of multiple instances or can be just an indicator of something larger. Bank accounts can be hacked and credit card details can be stolen. When such cyber crimes are committed, we need digital evidence for investigators to catch the culprits. Though cyber forensics is doing a great deal to combat this crime, it faces many issues that have to be handled with care.

CYBER SECURITY INCIDENTS RESPONSE

In today's multifaceted digital world it is in exorable to extensively prepare, plan and have well documented procedures and strategies in place for incident response, with the knowledge that the incident may be drastic and finding may be presented before court and the criticality of the incident turnaround time.

Detection And Protection Against Intrusion

The International community's need to be dedicated to fighting cybercrime and helping to protect your online experience. Not only do software vendors develop the world's leading security software to be used worldwide but some even conduct extensive research into the nature and construct of the subversive cybercriminal world. This knowledge is mostly shared internationally to provide global protection against an ever changing battle ground. Internet security and other utilities give business and individuals the power to deny cybercriminal attacks and keep them from wreaking devastation on business, family, finances, reputation, and even life. To best protection are careful system design, the use of products to detect known viruses and system instructions, and user education, and of course the use of Intrusion Detection System(IDS). Each organization's implementation of cyber security arises. The International cyber security is being threatened because an important element in establishing it is not being emphasized enough, citizen awareness and participation is lagging behind. Working against connected but weakly protected computer systems, hackers can steal information, make the systems malfunction by sending them false commands and corrupt the systems with bogus information. Nonetheless, deterrence should be pursued as a mitigation strategy, because even limited accomplishment can prevent some crime incidents and provide some protection from an increasingly serious problem.

Implementing Cyber Attack Detection Techniques

The best detection is the strength of the implemented security controls, since attackers always target vulnerabilities and weaknesses therefore security controls offer detection of the potential attacks, deterrence, prevention and corrective capabilities in addition to reduction of the attack probability and may minimize the impact of the attack. For cyber crime to be detected a team of professionals need to work together and these include but not limited to law enforcement agencies, cyber forensic scientist, lawyers, and computer security professionals also there is appalling need for organization to perform risk analysis and mitigation. Organization should emphasize secure systems at development stage and software patching if some flaws are realized during systems usage. Detection helps organizations to determine whether or not someone attempted to break into the organization's most critical asset which is systems and communication infrastructure, and what they may have done, if the attempts were successful. Almost daily, new techniques and procedures are designed to provide information security professionals a better means of finding electronic evidence, collecting, preserving, and presenting it to client management for potential use in the prosecution of cyber criminals.

A need has arisen for global synchronization of the laws especially binding business, organization and industry to implement security in their systems and organizations failing to comply with the regulation be penalized. Legislation alone cannot adequately combat the prevalence of cyber crime we face today. Private industry want to protect their business and customers provide the first line of Government on the latest technology, and must be willing to cooperate with law enforcement agencies for this war to be won. Technology holds the key to the future, and private businesses are leading the way in innovation and products, but if left unchecked, cyber crime will stifle that progress thus suppress e-commerce.

Collecting And Preserving Digital Evidence

While collecting electronic evidence, it is always best for law enforcement officers or security professionals to consider the rules of evidence to support an action against a cyber criminal. Admissibility of evidence and compliance with any existing standards for evidence for which a strong evidence trail is indispensable. Law enforcement agencies need training on how to retrieve information from computer system networks, cell phones and there digital devices in a criminal investigation, the availability of tools that help first responders deal with crimes involving digital evidences sush as malware and botnets in relation to complex international cybercrime is a breakthrough. The principle by which the cyber forensics is evaluated, accepted into legal proceedings and credited vary from one country to another and this challenges organization and law enforcement agencies inter-nationally and inhibit organization from reporting cyber security incidents to relevant investigating authorities.

Cyber Forensics Process

The increase in computer related has caused law enforcement agencies to seize digital evidence in the form of network logs, text documents, videos and images. In specific cases like those involving terrorism, the need to extract and analyze every possible bit of evidence becomes crucial. Scientifically, the result of the cyber analysis should be able to withstand legal scrutiny. Details of imaging always play a crucial role in a cyber crime case. When investigating the crime scene, the forensic experts can only see a computer, several telephone lines, etc. The computer, the network and the mobile device are only device that evidence begins to play a significant role at this time, and this is the high-tech scene of crime that the likely non technical law enforcement has to respond to. Knowledge of how to retrieve digital evidence is a prerequisite, how to recover deleted or damage information, how to preserve digital evidence, by its very nature, is very fragile and can be altered, damaged, or destroyed because of improper handling or examination. So it is important digital evidence should be conducted by experienced computer forensic investigators. The expert then examines the digital evidence and give a final report about the act complained of as a crime. This report is a determination of whether an act on a computer was a breach of any legislation or not. The report must be objective, based on indisputable facts, because law enforcers will connect the suspect beyond reasonable doubt to the crime, and this dictates for professional legal advice especially at this stage. The existence of a regulatory framework and laws catering for cyber crimes in the country are quite different, what may constitute a crime may not necessarily be a crime in the country that the cyber criminal resides or instigated the crime.

RECOMMENDED PROBABLE SOLUTIONS

The best that the International community can do is defending humanity's digital rights to help them have complete control of their online experience, through annual training of the public on the Cyber Security. The public equipped with this kind of information may know how to implement better online security and ultimately be safe and secure on cyber space. When law enforcement agents enter computer crime scene, they must know where to look for useful information, where operations history is maintained, how files are deleted and how to use forensic tools to gather or recover deleted files or damaged files. Moreover, computer forensic professionals must know how to protect and preserve digital evidence; they also need to know how to present the digital evidence in court. In this digital era, computer forensic filed is in great need of this kind of professionals and this can only be afforded with proper and thorough training of all concerned being adjudicators, law enforcement agents and prosecutors. Cyber criminals will go to great lengths to obscure their tracks, as such drawing a definitive map of cyber crime is the exact science and assuming any country has sole rights to any crime would be a mistake. The lack of continuity and completeness of evidence can compromise the legal position.

It is also required that the court be satisfied that the evidence has not been modified and is absolutely reliable. For this, hi-tech technical facilities, production of access control measures, time stamps or other supporting evidence should be used for digital evidence integrity assurance. There is dire need for constant review of current legislation on international level, an examination of how government interact with the private sector and a consideration of the prospects for international cooperation and treaties. Although the world enjoys tremendous economic benefits from Internet development, the respective governments have to try to maintain tight control over the telecommunications industry, and public usage of Internet, to fight escalating cyber crimes. In order for the world to win the against cyber crime, there is an astounding need to establish a dedicated cyber cell in each country and region which will not primarily detect but also prevent various cyber crimes that are committed daily. It is also essential for countries around the globe, academia, business/industry and the international community to come up with an International Cyber Research Unit to keep Best Practice, policies, training , let alone the Research and Development abreast with the ever changing technology.

The business and or Industry, academia alike need better support and research on how to meet information security requirements as dictated by the legislation or regulatory agencies including the government. There is a need for better understanding that virtually no investigation, either civil or criminal, comes without digital evidence in some form, clear reporting of crimes and subsequent investigations provide a basis for understanding the nature and extent of cyber crime problem. The development of a strategic approach to dealing with this International issue will allow investigators to collaborate better on investigations over the long term. Additionally, the development of policy will help to guide investigators and information security professional through the complicated process of cyber crime investigations and intrusion detection.

The current situation, whereby many organizations refrain from reporting incidents to protect their own interests and thereby harming the interest and thereby harming the interest of all businesses, need ti be changed because unless more incidents are reported, cyber crimes are unlikely to be controllable. The benefits and determents of a mandatory reporting system are debatable, but a reporting requirement would certainly benefit international efforts to manage cybercrimes. This would put law enforcement agents in the position to decide which cases to devote their attention and resources to, rather than be dependent on the willingness of organization to report their case for investigations.

CONCLUSION

Cyber crime is an international phenomenon that compels international cooperation, international harmonization of legislation and implementation of future technology provisions in actual legislation. There is a need for a balanced international strategy to combat cybercrime also for round-the lock cyber patrol and to equip the law enforcement officials with cyber forensic expert to enable them to collect legally defensible digital evidence that will withstand legal scrutiny and subsequent successful prosecution. A need has arisen for the International community to work in partnership with industry, business academia to address cybercrime and security, where challenges can be discussed and effective solutions and ideas such as the implementation of cyber intelligence programs by organizations, government etc, that do not pose a threat to individual privacy developed.

REFERENCES:

1. Amol Vyavhare, Cyber Forensic tools http://www.articleswave.com/computerarticles/top-cyber-forensic-tools.htmlAccessed on 02/11/2009
2. Barkha et al, Cyber Law and crimes, LawBooksellers, Publishers and Distributers, 2007
3. Cashmore C. et al, Business Information systems and strategies, British library Cataloguing in Publication Data, 1991
4. Chong K. et. Al., Digital Evidence search kit http://www.computer.org/portal/web/csdl/doi/10.1109/SADFE.2005.10 Accessed on 30/10/2009
5. Computer Forensics, Cybercrime and Steganography http://www.forensics.nl/links/ Accessed 02/11/2009
6. Computer Forensics World http://www.computerforensicsworld.com Accessed on 01/11/2009
7. Cyber Forensics http://www.cyberforensicsindia.com Accessed on 06/09/2009
8. Cyber Forensics: A Military Operations Perspective http://www.ijde.org.html Accessed on 11/09/2009