American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

The Role of Modern Software and Applications in the Protection of Electronic Crimes

Dr. Yasser Elmalik Ahmed Seleman

PhD in Computer Science, Omdurman Islamic University, Degree (Excellent), M.Sc in Information Technology, Newcastle (USA), M.Sc in Information Technology, The National Ribat University.
Email: Dr.yaserking@hotmail.com

Abstract

That scientific development in information and flow techniques in recent years, electronic revolution make a lot of criminals take advantage of scientific inventions and progress of advanced means in the commission of many cyber crimes, and the introduction of other forms of criminality associated with these techniques Which becomes the object of these crimes, or means to commit, and these crimes have increased in the other two, in particular, are led to the dawn of a new criminal phenomenon, known criminality informational or crime-mail, play experience significant role in the proof of cyber crime through the information network, The proof in criminal concept is all that leads to the truth, and for the judgment of the accused in the crime after provable, which means to establish a proof of the crime.

Keywords: Information Security; protection of data and information from loss; unauthorized access; modification; deletion of change; safety and reliability.

1. Introduction

E-crime: a crime includes the use of computer and networking and communications technologies and the Internet and uses a computer to commit the crime and may be the target. Also E-crime can be defined as any offense committed against individuals or groups motivated by Jeremy and the intention of harming the reputation of the victim or her body or mentality, whether directly or indirectly[1], and that is done by using modern means of communication (such as the Internet and chat rooms or e-mail or groups).

---

* Corresponding author. Tel: +249999335599- +24999902580
E-mail address: Dr.yaserking@hotmail.com .

Also modern technology can take place by a group of cyber-crime, and the most dangerous types of computer related crimes are those crimes that affect the morality and defamation and dissemination of information through the criminals illegally to achieve material gains and also political gain. For this to get rid of computer related crimes we must use the information security and must be configured to a special center for information security is intended to be protected in the areas of information technology [2].

The paper discusses the following questions to determine the problem and to clarify the appropriate solutions:

- How are recognized cyber-crimes?
- What are the methods used to prevent such crimes?
- What are the laws that limit such crimes?
- Statistical cyber crime?

1.1 Objectives of this scientific paper

- Control of the security a crime which is the use of computer and information technology in the crimes of terrorism and its organizations and criminal gangs [3].

- Solutions to the problems facing the law in how to prove electronic crime and access to the criminal.

2. Summarize the researcher to lack of the offender at several points including

A- Crimes often leave no visible external impact; they have to be tough in the proof. Adding to the difficulty of proving these crimes also usually committed in the rough, and the absence of any trace of what is being written during the implementation of the operations or criminal acts.

B- Criminal informational or mail does not leave a lot of times the effects reached in order to punish him, and that the crime suburbs World Wide Web, which is described as a virtual world, how the virtual world to remain on the track until its discovery.

C- That cyber-crime is interested environment unrelated to the paper or editors through a simple order could change a lot of information in a short time, it is difficult to draw physical evidence of the crime, because it is in the real world. The paper discusses some of the solutions that will help in the identification of cyber-crime

3. Solutions to the problem of proving cybercrime criminals

The paper reviews the intrusion prevention devices that assist in the electronic crime prevention.

A- Use device Secret Service Electronic Crimes Task Forces (ETFs), which focus on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes. The Secret Service’s Cyber Intelligence Section has directly contributed to the arrest of

Transnational cyber criminals responsible for the theft of hundreds of millions of credit card numbers and the loss of approximately $600 million to financial and retail institutions. The Secret Service also runs the National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cyber training and information to combat cyber crime [4].

B- Prove that the electronic crimes need to experts and specialized cadres provide sufficient evidence to prove the charges against the accused, and the unity of the international crimes in the police service and distribution role in solving many of the issues.

C- Preview and arrest and booking for various devices connected to the Internet and know the title of this person by –IP Address - any device. Once the identity of the Internet connection there address and a certain number of the device that is used by the person.

D- Hacking, theft and cybercrime that are interested institutions that rely on the information system must be suspected users that the program or system and to their knowledge of the security holes found [5].

E- The use of devices to prevent and reduce crime through electronic communications company.

F- Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity [6].

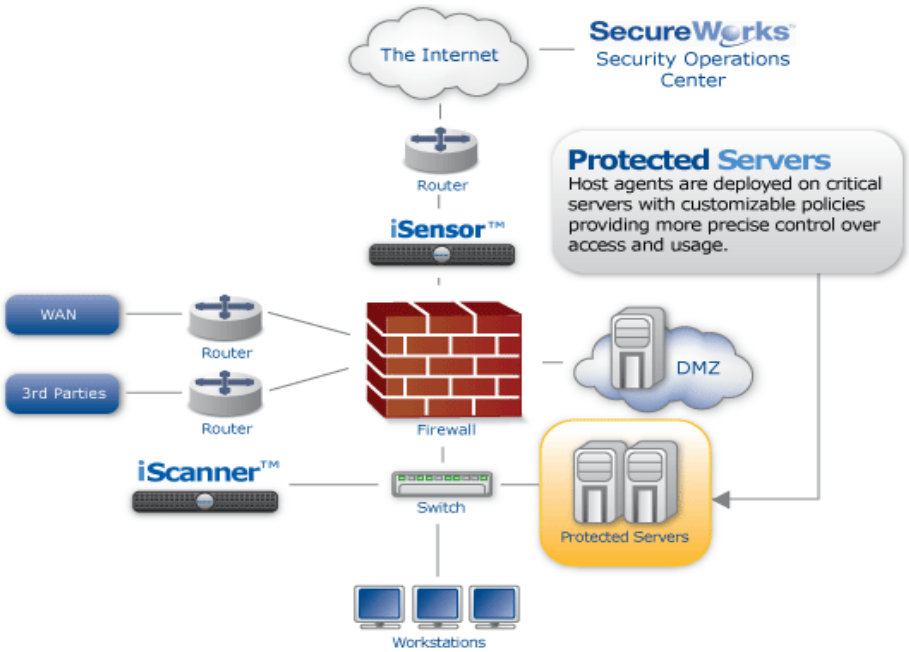

Figure:1 Intrusion Detection and Intrusion Prevention Systems

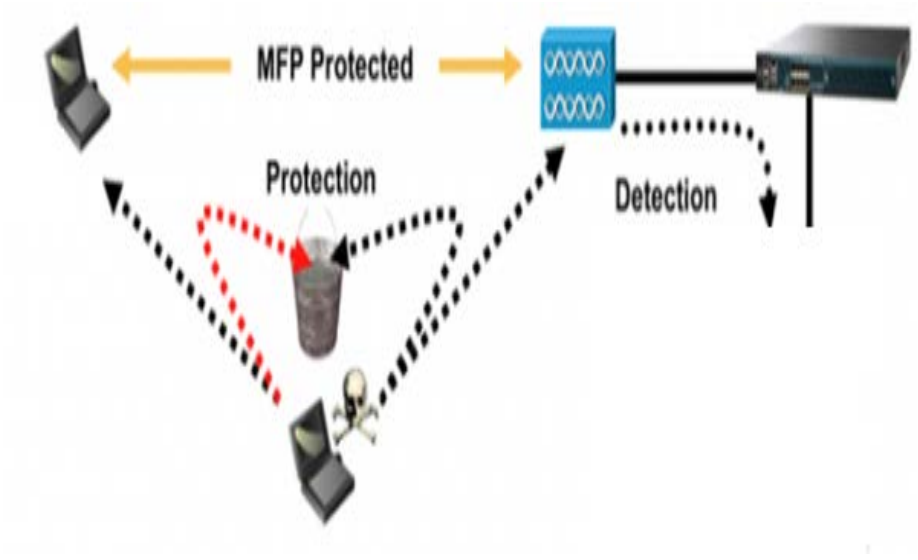

Figure 2: Protection device and detect the breakthrough

The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, and IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options. Through graphics researcher explains some devices that help prevent cyber-crime on the computer networks [7].

4. Conclusions

There are modern methods to keep track of where the sender and determine the offender site through his letters from home, work or anywhere access to e-mail address, and similarly in the mobile phone is now easier, and calling for sanctions in the law to prevent these crimes, which will be deployed and will appear electronic means newer must be taken into account because these crimes harmless and cause panic, especially the proliferation of obscene pictures and exploitation of girls and children through their pictures, which affects the reputation, and must involve experienced specialists in the law to determine Titles and means and to clarify the crime characterization, even to not be there are gaps to access them.

References

[1] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[2] Jump up Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley.

[3] Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley.

[4] Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations.

[5] Richet, Jean-Loup (2012). "How to Become a Black Hat Hacker an Exploratory Study of Barriers to Entry into Cybercrime." 17th AIM Symposium

[6] Kim-Kwang Raymond Choo (2011) The cyber threat Iandscape: challenges and future research direction computer &security, Volume 30, Issue 8, Pages 719-731.

[7] Mohammed Mohammed Al Alfi 2005, the "criminal responsibility for moral crimes online" – the modern Egyptian office.