Analysis of Cyber Criminology and Intruder: An Attempt to Explore Cyber Menace

Kanika Jethwani*
Supriya Jolly**

Abstract

With the growing usage of Internet, the world is coming closer day by day. The World Wide Web is global wide spectrums that brings the world closer and make its users feel like closer to each other. Along with bringing its users closer, it has also managed to create problems of "cybercrimes". Various law enforcement agencies are constantly trying to tackle with this problem, but it is rapidly growing and many people have become victims of theft, hacking and malicious software. This paper explains about insider threats, then cyber-criminal profiling, how we can identify cyber-criminal, after that various methods of detecting cyber-crimes and preventing cyber-crime.

Keywords: Cyber-crime, Attacks, Attackers, Intruders, Cyber-criminals

Introduction

The growth of the internet has brought the world closer, but it has also resulted in origination and growth of cybercrime. Through internet culprits can put in contact with victims. It also provides various individuals with the means of committing various cyber-crimes. Now days, cyber-crime is a major issue being faced by society. Hence, law makers and law enforcement agencies are required to take action. It has a big impact on businesses, governments and individuals and hence it deserves the attention of researchers.

Users today are facing problems of cyber-crime. The number of internet users has exponentially increased in the last twenty years and are growing day by day. The researchers have begun to study this problem only from the last decade. The purpose of this paper is to understand various concepts related to cyber-crime and how we can identify cyber-criminals and after that various methods of detecting cyber-crimes and preventing it.

Insider Threat

An insider threat is defined by the Computer Emergency Response Team (CERT), at Carnegie-Mellon University as "a malicious insider who is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system or data, and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information system" [4]. The attacks may be caused from such malicious insiders who cause harm intentionally for any personal gain or revenge, this threat can also be posed by trusted employees who unintentionally, cause financial or reputational damages to the organization may be through negligence.

Insider threat has become a significant issue. There have been considerably more reported insider threat incidents over the past few years. According to the 2009 e-Crime Watch Survey in which 523 organizations were involved, 51% of the organizations experienced an insider attack, which increased from 39% three years ago[7]. Since these were only reported incidents of attacks; it is likely more than 51% of organizations experience such attacks. From the recent Cyber-Ark Global Survey conducted in the spring of 2011 with 1,422 IT staff and C-level professionals, 16% of the surveyed individuals believe that insiders have stolen highly sensitive and valuable intellectual property, such as customer lists and product information, which have been transferred or sold the organizations' competitors. [5].

Kanika Jethwani*
IINTM, GGSIPU
Supriya Jolly**
IINTM, GGSIPU

As per the analysis done in [5], it can be seen that insider threat has always been there in organizations, and hence, it has increasingly become an important issue that must be better managed. It may be difficult to manage insider threat because they are influenced by a combination of behavioral organizational and technical issues. The organizations must devise layered defense plans incorporating various policies, technical controls and procedures.

Cyber Criminal Profiling

Cyber Criminal profiling, is also known as offender profiling or criminology profiling or behavioral profiling or criminal investigative analysis. According to Bartol and Bartol criminal profiling can be defined as "the process of identifying personality traits, behavioral tendencies, and demographic variables of an offender based on characteristics of the crime" [2].

As per the author in [6], 'offender profiling' is a term given by the FBI in the 1970's to describe their criminal investigative analysis work. He maintained in [6] that "when FBI agents first began this work they invented a new term to grace their actions: offender profiling. By doing so they created the impression of a package, a system that was sitting waiting to be employed, rather than the mixture of craft, experience and intellectual energy that they themselves admit is at the core of their activities.

The author sees offender profiling as 'criminal shadows'. He maintained in [6] that a criminal "leaves psychological traces, tell-tale patterns of behavior that indicate the sort of person he is. Gleaned from the crime scene and reports from witnesses, these traces are more ambiguous and subtle than those examined by the biologist or physicist. They cannot be taken into a laboratory and dissected under the microscope. They are more like shadows, which undoubtedly are connected to the criminal who cast them, but they flicker and change, and it may not always be obvious where they come from. Yet, if they can be fixed and interpreted, criminal shadows can indicate where investigators should look and what sort of person they should be looking for.

The author in [11] defined, offender profiling as "the process of using all the available information about a crime, a crime scene, and a victim, in order to compose a profile of the (as yet) unknown perpetrator. According to Davies in [1], "offender profiling (more technically known as Criminal Investigative Analysis) is the name given to a variety of techniques whereby information gathered at a crime scene, including reports of an offender's behavior is used both to infer motivation for an offence and to produce a description of the type of person likely to be responsible.

The author sees in [15], a criminal personality profile as "an educated attempt to provide investigative agencies with specific information as to the type of individual who may have committed a certain crime.

The author, from a behavioral evidence analysis point of view in [3], defined offender profiling as "the process of inferring the personality characteristics of individuals responsible for committing criminal acts.

In simple words, it does the analysis and validates the information on which the profile is based on. It is a tool that is used in investigative psychology. Put simply, criminal profiling is a crime investigation technique in which information is drawn from the crime scene. A rough idea is made about the person who could have committed that crime through various witnesses, victims, autopsy reports.

Identifying A Cyber Criminal

Various researchers have identified various types of cyber criminals. Here are few of the types of attackers:

1. **Hacktivists:** These types of attackers make use of computers system and networks, to express social protest, or to promote a political ideology. These type of activists or groups (like

WikiLeaks) seeking to steal data and release it publicly.

2. **Cyber Terrorists:** A programmer who breaks into computer systems with the intention of stealing or changing or destroying information.
3. **Professional Cybercriminals:** These types of attackers damage the most, particularly to retailers, e-commerce businesses, financial institutions, governments, etc. This group actually creates more remediation, fraud and reputational damage than the other types of cybercriminals.

The authors in [10] have divided cyber criminals into four types:

1. **Espionage:** These types of attackers mainly seek some kind of secretive information. These are mainly employed by a competitor to get that information. They are high in position in the organization and are mostly older in age.
2. **Theft:** These attackers have the intention of stealing confidential or proprietary information from the organization and use it as an advantage for business. These are generally current employees at technical (scientists, programmers and engineers) or sales positions who attempt this for their personal financial benefit.
3. **Sabotage:** These types of attackers are those who are former employees at technical levels within the organization who had access to systems with the intention of harming organization's data or specific individual or some business operations. They are mostly younger in age and they do this to take revenge from their peers or employers. For example at some point if an employee has been discouraged by higher authorities.
4. **Personal abuse of the organizational network:** These types of attacks are done by those individuals who use the computer network for their personal use like checking emails, reading news, gambling etc. These attackers may regularly break the rules.

Irrespective of which type of attacker you are dealing with, the important thing to, find the attacker. There is always need of securing the information from the attackers in an enterprise. For this enterprise security intelligence is used. This technology is new and is powered by big data, which helps you to find and take legal actions against a particular cyber-criminal.

Detecting Cyber Crime

We know that the above information has made us aware about the studies related to cybercrime but still, various authors have not provided us ways of detecting the insider crimes.

One of the most popular frameworks for cybercrime detection was given by Schultz in [12] that is known as **Schultz Detection Framework**. According to his detection framework there are six parameters to identify any intrusion behavior. These parameters are: personality traits, correlated usage patterns, preparatory behavior, deliberate markers, verbal behavior and meaningful errors.

1. **Personality traits:** According to Schultz although different attackers possess different personality characteristics, still some commonly identified traits are *"computer dependency, a sense of loyalty, lack of empathy ethical flexibility, and, entitlement"* [14]. Various writers have also laid out a correlation between computer dependency and cybercrime [9]. As far as ethical flexibility is concerned, usually the intruders become incapable of identifying what is wrong and right and their flexibility increases for committing these crimes. As the benefits of these attacks outweighs the sufferings. Hence their hunger for these benefits increases and they lose their empathy judgment. These traits are mostly seen in younger generation that will impact the upcoming generation employees.
2. **Correlated usage patterns:** Patterns provides similar type of signs that the attackers adopt to

attack various machines. These patterns can be identified after introspecting multiple systems.

3. **Preparatory behavior:** In this case the attackers have a plan of attack beforehand. These planning include obtaining someone else's credit information without authorization, looking at other's files without authorization, obtaining administrative password etc. These types of attacks are mainly committed by those that have the intention of financial benefits.
4. **Deliberate markers:** These types of attackers leave some marks after their attack to make their presence feel. These attacks are done to show the frustration after some personal grudges.
5. **Verbal behavior:** This behavior is identified when there is a sudden change in the verbal tone of the insider as he becomes more angry and aggressive.
6. **Meaningful errors:** In this case the attackers leave some clues or some evidence of their attacks behind and these can be visualized in errors logs by some specialists.

Apart from the above model there are various other detection techniques suggested by various researchers.

Crime Pattern Detection Using Data Mining [13]**:** In this clustering techniques are used for identifying the crime patterns. In this crime pattern detection can be viewed as machine learning task and hence data mining is used to support detectives to solve the crimes.

Insider Threat Prediction Model [8]**:** It categorizes employees as potential accidental threat that means they intentionally don't attack the system rather it is accidental.

Prevention of Cyber Crime

1. **Choose Strong Passwords**: One should choose different user ID or password combinations for various accounts and avoid writing them down. Passwords should be made complicated by using various combinations of special characters, numbers and letters and one should keep them changing.
2. **Protect your computer**
   - o *Activate firewall:* Firewalls are the first step for filtration of unwanted threats. They do not allow any communication with fake site that has threat of any malicious content.
   - o *Use anti-virus/malware software:* It monitors all online activities and shields your computer from viruses, worms, Trojan horses, and other types of malicious programs. It should be regularly updated.
3. **Protect your Data:** One should make sure regarding encryption the confidential files and must regularly take the backups of important data files.
4. **Psychological screening:** As they say "Prevention is better than cure" so before the hiring of the employee, his psychological screening must be done to understand the psychology of the employee regarding his motives.
5. **Accessing Background:** Managers should try to access if there is any criminal background history before hiring an employee.

Conclusion

Cyber-crime is a vast field of study. Although we have tried to incorporate many aspects of it but still there is a much scope of further study and research. In terms of cyber-criminal profiling, there is disagreement regarding what an "insider" is, with a lot of authors using such a broad definition that it is difficult to develop a common profile. It is unclear whether a common profile even exists for insider criminals. Various categories of cyber criminals have been identified by various researchers and authors but with the rapid growth of technology new criminal personalities are emerging day by day that needs to be researched upon and hence new ways of prevention and detection could be developed.

References

1. A. Davies, “Rapists Behavior: A three Aspect Model as a Basis for Analysis and Identification of a Serial Crime”, Forensic Science International, 173 (1992)
2. Bartol, C. R., & Bartol, A. M. (2012). ”Introduction to Forensic Psychology”, Research and Application (3rd ed.). Thousand Oaks, CA: SAGE Publications Inc.
3. B. Turvey, “Criminal Profiling: Introduction to Behavioral Evidence Analysis”, 1 (2002)
4. Cappelli, Dawn, A. Moore, R. Trzeciak, and T. J. Shimeall “Common Sense Guide to Prevention and Detection of Insider Threats.” CERT, Jan, 2009.
5. “Cyber-Ark; Cyber-Ark Global Survey Shows External Cyber-Security Risks Will Surpass Insider Threats.” Investment Weekly News, 30 Apr. 2011: ABI/INFORM Trade & Industry, ProQuest.
6. D. Canter, “Criminal Shadows: Inside the mind a/the serial killer”, 12 (1994)
7. Maxi, Merritt, “Defending against Insider Threats to Reduce Your IT Risk.” Security and Compliance, Jan. 2011
8. Magklaras, G., & Furnell, S. (2001). “Insider threat prediction tool: Evaluating the probability of IT misuse”, Computers & Security, Volume 21. Issue 1, pp. 62-73
9. Nykodym, N., Ariss, S., & Kurtz, K. (2008), “Computer Addiction and Cyber Crime”, Journal of Leadership, Accountability and Ethics.
10. Nykodym, N., Taylor, R., & Vilela, J. (2005), “Criminal profiling and insider cyber-crime”, Computer law & security report, Volume 21, pp. 408-414.
11. P. B. Ainsworth, “Offender Profiling and Crime Analysis”, 7 (2001)
12. Schultz, E. (2002). “A framework for understanding and predicting insider attacks”, Computers & Security, pp. 526-531.
13. S. V. Nath, “Crime Pattern Detection using Data Mining” 2004. WI-IATW ’06 Proceedings of the 2006 IEEE/WIC/ACM international conference on Web Intelligence and Intelligent Agent Technology, Pages 41-44
14. Shaw, E., Ruby, K. G., & Post, J. M. (1998) “The Insider Threat to Information Systems”, Security Awareness Bulletin. Issue 2 , pp. 170–186.
15. V. J. Geberth, “Practical Homicide Investigations: Tactics, Procedures, and Forensic Techniques”, 4th edition, 46 (1996)