American Journal of Applied Sciences 10 (12): 1660-1666, 2013
ISSN: 1546-9239

doi:10.3844/ajassp.2013.1660.1666 Published Online 10 (12) 2013 (http://www.thescipub.com/ajas.toc)

Combating Cyber Terrorism-Assessment of Log for Malicious Signatures

[1]Kamalanaban Ethala and [2]R. Seshadri

[1]Department of CSE, Sri Venkateswara University, Tirupathi, India and
Department of CSE, Vel Tech University, Avadi, Chennai, India
[2]SVU Computer Center, Sri Venkateswara University, Tirupathi, India

Received 2013-07-04, Revised 2013-08-14; Accepted 2013-11-07

ABSTRACT

Enhancing security to the networks and preventing the cyber attacks is a major issue in all domains. In this study, a new class of cyber terrorism is addressed where mischievous and malicious behaviour is the root cause for the modification of network data stored in an open database. An attempt is made in this study to develop an algorithm that screens network, database results and detects anomalies in the input data that could have been revised by cyber-attacks, that is cyber terrorism. Combating Cyber Terrorism (CCT) Algorithm that is developed in this attempt uses multi path navigation based on six degree separation to analyze data flow inconsistency into bound and unbound values. This is the first such attempt made in this communication wherein the results presented clearly denote the reduced rate of cyber terrorism based attacks. Analysis of information in the unbound values determines whether the database value has been compromised for any attacks. Success has been achieved in reducing the false alarm rate. Future enhancement will be attempted in the entropical model for profiling the network agents for better performance.

Keywords: Intrusion, IDS, IPS, Entropical, Cyber Threats, Cyber Terrorism, Anomalies, Signatures, Backtrack Operating System, Backtrack OS

1. INTRODUCTION

The word cyber terrorism is increasingly combined in the popular culture of the interconnected world. Yet a dense definition of the word seems hard to come by, since the network of computers rules the world today. While the phrase of every individuality, that is, instance network or system loosely defined, there is a large amount of partiality in which exactly establishes cyber terrorism. In an attempt to define cyber terrorism more logically (Theuns and Ray, 2002) a study is made of explanations and characteristics of terrorism and terrorist based actions. According to Symantec characteristics a list of characteristics for outdated as well as updated level of terrorism is developed. This characteristic list is then surveyed in detail with the count of the computer network and the internet considered for each attribute. Using this routine, the online world and terrorism is fused to yield a broader but more useful charge of the potential impact of computer terrorists. Most importantly, the concept of outdated cyber terrorism, which landscapes the computer as the target or the tool is evaluated to be only a limited part of the true risk faced (Tian and Gao, 2009).

Cyber terrorism is the merging of terrorism and cyberspace. It generally denotes unlawful attacks and threats of attacks against computers, networks and the information stored therein which is done to threaten or force a government or its people in persistence of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to

Corresponding Author: Kamalanaban Ethala, Department of CSE, Sri Venkateswara University, Tirupathi, India and Department of CSE, Vel Tech University, Avadi, Chennai, India

generate fear. According to the survey of Symantec security solutions, attacks that lead to death or injury in the body. Explosions, plane crashes, water contamination, or severe economic loss would be other examples. Serious attacks against critical infrastructures could be the acts of cyber terrorism, depending on their impact (Ahamad *et al*., 2008).

The intrusion detection has become a research focus area of the network security. The intrusion detection system is used to trace signatures or information that is left by the attackers or intruders. The information or signature may be obtained from the failure of the records of attempts to log on or from the illegal intrusion from outside or inside effectively. The intrusion detection system is the computer system which can realize the intrusion. An attempt is made for the first time to propose a working model for detecting cyber terrorism over the networks.

2. RELATED WORK

The goal of this work is to design and implement intrusion detection system based on signatures, using techniques which are in defending another type of cyber attack. The focus is towards cyber terrorism. The primary requirement for final solution is towards the development of the whole system has to be made. This system should be able to predict the intrusion with less false rate. System should be able to be trained by the user and those trained information should be made use of whenever they are required.

2.1. Cyber Threats and Attacks

The 21st century is an era of internet and emails. The countless dangers and risks that come with them are increasing too. Cyber threats are major risks of 21st century. List of active threats and attacks are listed according to report of 2009 (GTISC, 2012) and 2012 (Yoshinori and Goto, 2002). The different types of cyber attacks over the networks are malware, botnets, cyber warfare and threat to VOIP and mobile devices (Denning, 1987).

The inputs of the cyber attacks are shown in **Table 1**. This table has the potentiality of weakness for each type of instances.

2.1.1. Malware

The malware is a small piece of code for malicious or malevolent software. This is the software used or automated by attackers to interrupt computer operation. This software is also used to gather sensitive information from the computer. Usually Trojan horses are malwares. For example, Netbus is a vital Trojan horse in Networks, Hosts and Servers.

2.1.2. Botnets

The botnets are the type of infection which can occur even through authentic Web sites. The botnets exploit. Malware delivery mechanisms are gaining sophistication. It can be delivered to a system via emails, USBs, Trojans. It can independently switch from one system to another system.

For example, the report had been submitted by Georgia tech, according to a report compiled by Panda Labs, in 2Q 2008 that 10 million botnet computers were used to distribute spam and malware across the internet each day. The Damballa continues to discover that 3 to 5 percent of enterprise assets are compromised on average by targeted threats such as bots even in the presence of the best and most up to date security. Leading industry analysts predict this number to be even higher (GTISC, 2012; Yoshinori and Goto, 2002).

2.1.3. Cyber Warfare

The cyber warfare is a type of attack, which creates physical and cyber attack. This is evident from the report submitted by Georgia Tech. Logs of Distributed Denial of Servicer (DDoS) traffic and changes in network routing indicate that Russian cyber warfare operations coincided almost exactly with the final all clear for Russian air Force attacks sometime between 600 and 700 on August 9, 2008. Both cyber attack targets media outlets and local government communication systems and air force targets were located in the Georgian city in Gori (Denning, 1987). The exact timing of cyber attacks against new classes of targets in Gori and Russian air force attacks indicated coordination between known hacking groups and military operators (GTISC, 2012; Yoshinori and Goto, 2002).

2.1.4. Threats to VoIP and mobile devices

The cell phone is becoming an entirely emerging gadget especially in developing countries like India, where accessing the Internet and usage of internet is huge. In the early days of VoIP, there was no big concern about security issues related to its use. People were mostly concerned with its cost, functionality and reliability. Now that VoIP is gaining wide acceptance and becoming one of the mainstream communication technologies, security has become a major issue.

Table 1. System of the cyber attacks

Agent	Group/Individual	Potentiality in weakness
Place	Networks	Average
Action	Attacks, threads	High
Tool	Any type of Hacking tools	High
Target	Network, Host, System	High
Affiliation	Government/private	High
Motivation	Political, social and economic changes	High

The security threats cause even more concern when we think of this VoIP. This in fact replacing the oldest and most secure communication system the world ever known Plain Old Telephone System (POTS). Let us have a look at the threats for VOIP users face.

Criminals will exploit this social conditioning to perpetrate voice phishing and identity theft (Forrest *et al*., 1996). At the same time, customers will demand better availability from phone service in spite of the threat from DoS attack. This might compel carriers to pay out on a blackmail scam. This is reported by Tom Cross a Researcher with IBM Internet Security Systems, XForce team (GTISC, 2012; Yoshinori and Goto, 2002).

2.1.5. Backtrack Operating System-Penetration Tools

The various tools are used through backtrack operating system to attack the WLAN in various types of firms such as schools, colleges, universities and commercial organizations. Penetration testing is the legal and authorized attempt to exploit a computer system with the intent of making a network or system more secure. The process includes scanning systems looking for weak spots and launching attacks and proves that the system is vulnerable to attack from a real hacker.

Backtrack is intended for all black hat from the most savvy security professionals to early newcomers to the information security field. The widely used tools in backtrack is Airmone-ng, Airodump-ng, Aireplay-ng and Aircrack-ng. The Backtrack is a world's leading penetration testing and information security auditing distribution with hundreds of tools preinstalled and configured to run out of the box.

3. SIX DEGREE SEPARATION OF DATA FLOW

In our methodology we use six degree separation of data flow, where the data sets are refined frequently and iteratively. Degree one sets the proper data set values. Degree two is the internal set design. Degree three focuses on design evaluation. Degree four focuses on the key term and metadata values. Degree five holds on the log data files and classifier. Finally sixth degree checks for the integrity of data sets. Inbound values are maintained by the layers of up to level five. Outbound values are maintained by the level six. Our degree of separation for various data sets are analysed by each and every value and the results with the accuracy of nearly between 3.43 to 3.65, it is between two data sets of identical type of normal plus anomaly. Level six which is responsible for detecting intrusions are shown in **Fig. 1**.

3.1. Multi path Navigation

Multi path navigation's scope is to reduce false alarm rate. An alarm is triggered when there is no attack takes place. This widely happens due to mobile node for a particular channel. This is exactly our proposed method for our multi path navigation that is employed throughout all the connected nodes in active networks (Hofmeyr *et al*., 1998). Index of each node is flooded in all nodes. This is essential to withstand even in the case of node failure. Whenever a mobile node trespasses or in bound to the IDS boundary it calculates the likelihood for the particular node. It tracks the signature, builds in details. It updates the channel with these details and the particulars are flooded in the index of each node within the boundary (Inagaki, 1999). If the likelihood value is 1 then the node has a primary malicious action. It is then navigated to a particular path in another channel. This process is iterated until the node value is decreased to 0. If the likelihood value is 0 then the node is not considered to be an intrusion. It is updated in first channel of the active node. The pseudo code of the Combating Cyber Terrorism (CCT) is shown below:

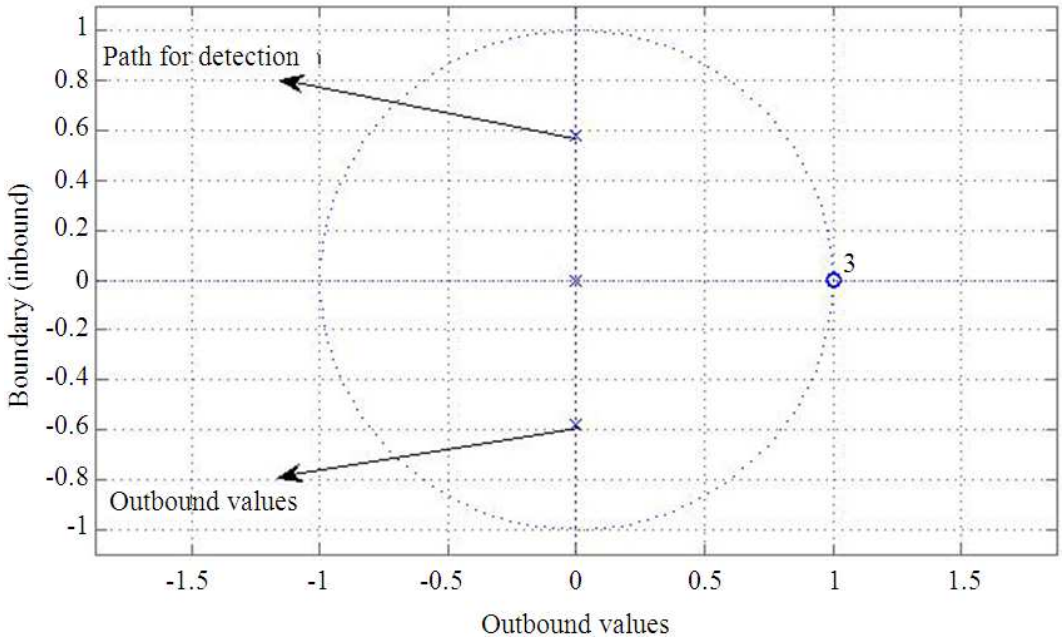

Fig. 1. Six degree separation of data flow in logs

Pseudocode of CCT algorithm

```
Function CCT (log, inbound, outbound, TriggerAlarm)
begin
Initialize the entire path
For all the nodes
Set connected parameter=1
Set mobility node=1
Check all the nodes in same path
Set connected parameter =1
Set unconnected parameter =0
Set channel values=Inf
For all the connected nodes
Prune inbound values
Apply six degree separation
Classify the inbound values
If node=(level2 &&level 3)
TriggerAlarm(1);
Else
Update (log);
End;
End;
Timestamp(1);
Sleep(1);
Update(log);
End function
```

3.1.1. CCT performance analysis

The Detection Rate, that is the number of intrusion cases detected by the system (True Positive) divided by the total number of intrusion cases present in the test set, is shown in Equation 1:

$$\text{CCT} - \text{DR} = \text{Intrusion cases detected/total number of intrusion} \quad (1)$$

The False Alarm Rate is the number of normal outlines classified as attacks (False Positive) divided by the total number of normal outlines and it is represented as shown in Equation 2:

$$\text{CCT} - \text{FR} = \text{False classification/Total number of outlines} \quad (2)$$

The True Positive is a type of a real attack which activates the IDS to create an alarm and it is represented as shown in Equation 3:

$$\text{CCT} - \text{TP} = \text{Real Attack} * \text{Alarm instance} \left(\text{Default alarm instance is one}\right) \quad (3)$$

The False Positive is a type of an event signing, that is IDS can create an alarm when no attack has taken place and it is represented as shown in Equation 4:

$$CCT - FP = CCT - TP(1)/CCT - FR(0) \quad (4)$$

The False Negative is a type of failure of IDS to detect an actual attack and it is represented as shown in Equation 5:

$$CCT - FN = CCT - TP(0) * CCT - DR(0) \quad (5)$$

The True Negative is a type of system when no attack has taken place and no alarm is raised as shown in Equation 6:

$$CCT - TN = CCT - FP(0) * CCT - TP(0) \quad (6)$$

The *Noise* is a type of data or intrusion that can activate a false positive as shown in Equation 7:

$$CCT - N = CCT - FP(1) \quad (7)$$

4. ENTROPHICAL APPROACH

We use entrophical approach for profiling the data log files. We generate profiles for each data log users in active network or for network based profiles or host based profile that is for individual system oriented (Inagaki, 1999). So we use the profiling technique entrophical at real time and it does not utilize large amount of resources (Guojun and Zhiqiang, 2008). The attacker ultimate goal is to gain the root of the host or to gain privilege to the centralized servers to retrieve the information or to exploit the server. Thus we need to prepare separate profiles for privileged user in order to avoid the intruders to gain the access (Qinglin and Huibin, 2008).

4.1. Profiling Environment

Organising the profiles for each privileged users is a bit toughest job. We use random ordering techniques to daemon the profiles. The host and logs are updated in the profiles and maintained thoroughly for all centralized domains. Profiling is done for two main categories namely base category, daemon category and user category.

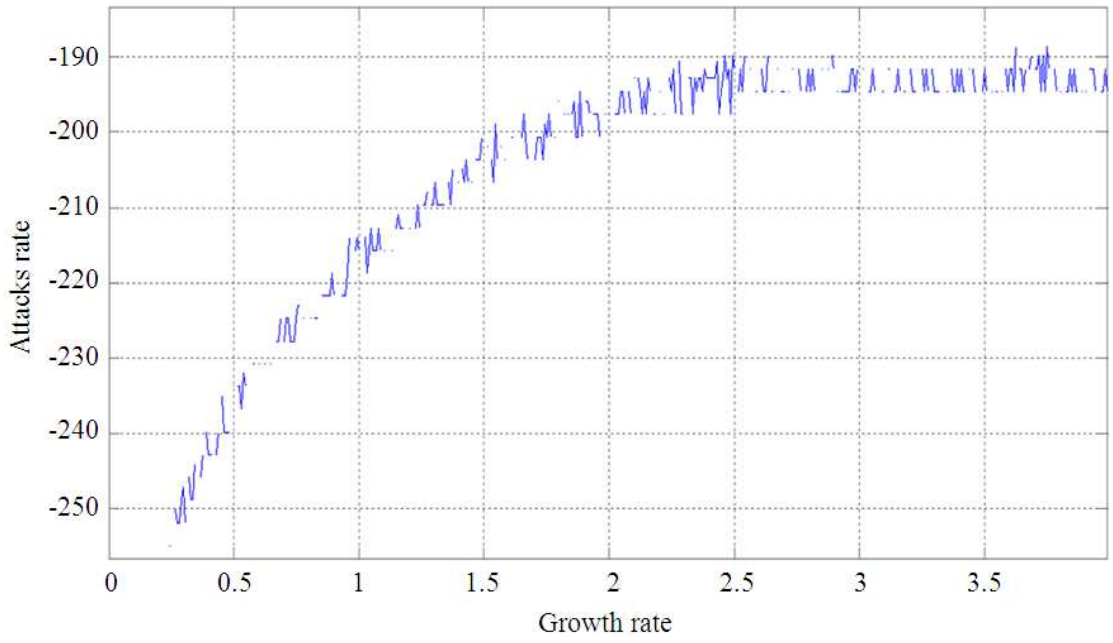

Fig. 2. Attacks rate Vs growth rate

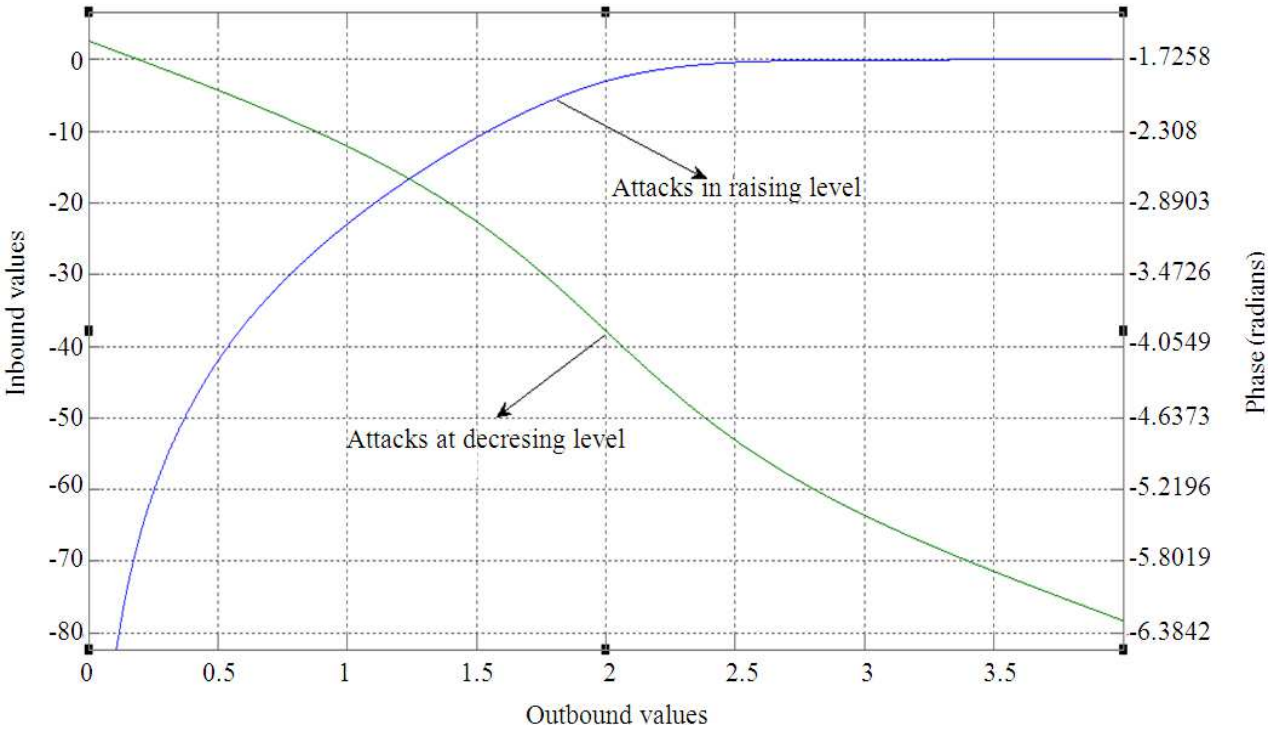

Fig. 3. Analysis of real time results for proposed method

4.1.1. Base Category

In base category the system processes and individual user log are captured generally. In this profile the system call and its frequency are ranked individually (Zhenning and Yongmao, 1996). Large value occurs for rare occurring and small value for reputations.

4.1.2. Daemon Category

Daemon profile registers huge structures of system calls, UID processes and system processes in a daemon process running on a system. A daemon process waits for a call from external processes (Grefenstetle, 1986). Daemon profile treats idle state as Delimiter of profiles. A profile starts recording when a client connected to a daemon. Again, the base profile is used to make the daemon profile. Daemon process can be recorded in a small amount of data. This method also simplifies the comparison of profiles.

4.1.3. User Category

User category is used at the interface level, a privilege to the users is given by the administrators. Various user privileges are set by the DBA's.

4.2. Behavioural Analysis

The advantages over signature based intrusion detection system are (i) fast updating of log, (ii) Multipath navigation for better performance and Reliability, (iii) entrophical model for profiling the network agents, (iv) reduced system load due to six degree separation and (v) quality of Log data is relatively small in size (Licheng, 1995).

The attack rate versus growth rate is shown in **Fig. 2**. This result shows that the attack rate is reduced based on the proposed algorithm. The real time results of CCT are shown in **Fig. 3**, that is, the attacks in rising and decreasing level are also shown with outbound and inbound values.

5. CONCLUSION

Experimental results of our algorithm clearly denote the reduced rate of cyber terrorism based attacks. They also show the exact flow of attack analysis in the network domain. Our proposed intrusion detection model uses multi path navigation for reducing false alarm rate. We have achieved

success in reducing false alarm rate in the range between 3.43 to 3.65. Future enhancement will be done over the entrophical model for profiling the network agents for better performance. The result of the experiment clearly shows the reduced rate of intrusions like backtrack OS penetration tools by using the six degree separation approach followed first time in this study. In future, the present model CCT-IDS can be actively used to detect the Polymorphic and Covert channel attacks in active networks.

6. REFERENCES

Ahamad, M., D. Amster, M. Barrett, T. Cross and G. Heron *et al*., 2008. Emerging Cyber Threats Report for 2009. Georgia Institute of Technology.

Denning, D.E., 1987. An intrusion-detection model. IEEE Trans. Soft. Eng, SE-13: 222-232. DOI: 10.1109/TSE.1987.232894

Forrest, S., S.A. Hofmeyr, A. Somayaji and T.A. Longsta, 1996. A sense of self for unix processes. Proceedings of the IEEE Symposium on Security and Privacy, May 6-8, IEEE Xplore Press, Oakland, CA., pp: 120-128. DOI: 10.1109/SECPRI.1996.502675

Grefenstetle, J.J., 1986. Optimization of control parameters for genetic algorithms. IEEE Trans Syst. Man Cyber., 16: 122-128. DOI: 10.1109/TSMC.1986.289288

GTISC, 2012. Emerging cyber threats for 2012. Georgia Tech Information Security Center.

Guojun, W. and Y. Zhiqiang, 2008. Application research of support vector machine in the intrusion detection. Guangxi J. Light Indus., 7: 51-52.

Hofmeyr, S.A., A. Somayaji and S. Forrest, 1998. Intrusion detection using sequences of system calls. J. Comput. Security, 6: 151-180.

Inagaki, T., 1999. Measurement of network performance inmbone. MSc Thesis, Graduate School of science and Technology, Waseda University.

Licheng, J., 1995. Neural Network System Theory. Xi an Electronic Science and Technology University Press, Xian.

Qinglin, L. and L. Huibin, 2008. Research of intrusion detection based on neural network optimized by adaptive genetic algorithm. Comput. Eng. Des., 29: 3022-3025.

Theuns, V. and H. Ray, 2002. Intrusion detection techniques and approaches. Comput. Commun., 25: 1356-1584. DOI: 10.1016/S0140-3664(02)00037-3

Tian, J. and M. Gao, 2009. Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing, (CTC' 09).

Yoshinori, I.S. and S. Goto, 2002. Proceedings of the Symposium on Applications and the Internet, (SAI '02).

Zhenning, Z. and X. Yongmao, 1996. Introduction to Fuzzy Theory and Neural Networks and Their Application. 1st Edn., T.Singhua University Press, Beijing.