RESEARCH PAPER | Engineering | Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

Intrusion Detection Using Collaborative Network Security Management System in Cloud Computing

KEYWORDS: collaborative network security management; ACO optimization; anti-botnet; anti-phishing, anti-flooding.

Prof. Krishnakumar L
Professor, 1Department of Computer Science and Engineering, Nehru Institute of Technology, Coimbatore

Ms. Nisha Mariam Varughese
Post Graduate Scholar, 2Department of Computer Science and Engineering, Nehru Institute of Technology, Coimbatore

ABSTRACT *Security is one of the major challenges of open network. To address the security problems collaborative network security management system is introduced with collaborative Unified Threat Management (UTM), traffic prober and cloud based security center. The security center can instruct each collaborative UTM and prober to collect raw traffic and this huge traffic is given to the data center which classifies the data in parallel. Security center will deeply analyze the classified data and generates new security rules. These security rules are carried out by collaborative UTM and the feedback events of such rules are given back to the security center. The cloud storage is used to store the huge amount of internet traffic data and then processing it with cloud computing platform to detect the malicious attacks. Security center analyze the data and when any attack is detected it will generate new rules. These rules are given to the network and feedback is evaluated. Then it will remove the invalid rules to make the system more efficient and reliable.*

INTRODUCTION

Internet Security has become a major challenge in the current world due to the increasing size of the network. By matching malicious attacks to known threats, the attacks which have fixed patterns can be easily identified. But the attack which does not have a fixed pattern is difficult to identify. For example, DDoS attacks. A bot is malicious software that can intrude on the computer. Botmaster infects victims with bot, then this bot connects to control and command server. Botmaster sends commands to bot through the C & C server. This process is repeated and soon the botmaster has an army of bots to control from a single point. The backbone of botnet is command and control(C&C) channel that is responsible for setting up the botnet, controlling the activities of the bots, issuing commands, and ultimately reaching the goals. The main difference between Botnet and other kind of malwares is the existence of Command-and-Control (C&C) infrastructure. The Botmaster computer communicates with its bots by a command and control (C&C) channel, which passes commands from the botmaster to bots, and transmits stolen information from infected machines to their master. [1] By suppressing the Command and Control server of Botnet the victim is prevented from the attack. For that the cloud based security center will generate security rules and these rules are enforced into the networks.

Flooding attacks is accomplished by broadcasting a bunch of packets, usually the ping packets. The idea is to send large amount of data to the victim at the same time, so that the victim slows down so much and gets disconnected because of timeouts. Flood attacks attempt to fill a network by sending continuous series of echo requests over a high-bandwidth connection to a target host on a lower-bandwidth connection. The receiver sends back an echo reply for each request.

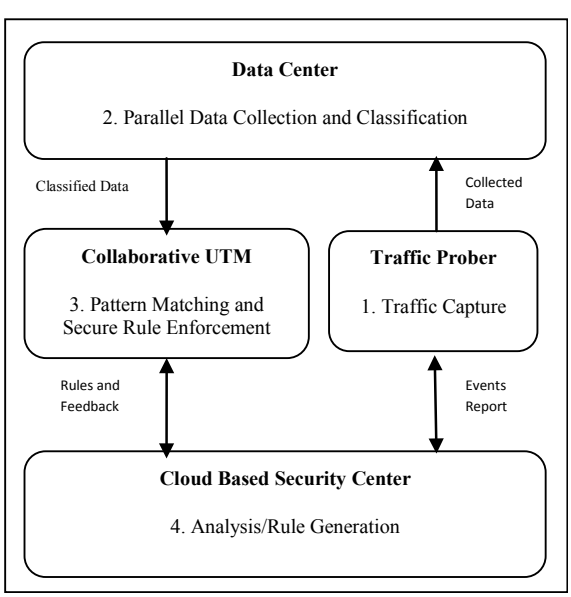

Figure 1: Work Principle of High Speed Vulnerability Analysis for CNSMS in Cloud Computing

Collaborative Network Security Management System (CNSMS) performs the forensic analysis of huge data and this data is classified by using parallel processing. This will increase the speed of vulnerability analysis of traffic data that are stored in cloud based security center.

ANALYSIS OF CNSMS

A CNSMS aims to develop a new collaboration system to integrate a well deployed Unified Threat Management (UTM) such as NetSecu. In CNSMS, a hierarchical architecture of three levels is implemented. The third level of the hierarchy is basic NetSecu nodes. The second level consists of domain NetSecu nodes to manage the membership in corresponding sub-domains. [2] And to have a big picture of the whole network, the rule set library is stored in the Central Management System, which is the first level.

Figure 1 illustrates the whole procedure of network security events processing. The traffic prober and collaborative UTM captures the traffic data and given to the data center. The data center classifies the huge traffic data in parallel. The data collection and classification is carried out by parallel processing. A peer-to-peer communication protocol is used in the UTMs collaborative module and connects them virtually to exchange network events and security rules. During the systems operation, the collaborative mechanism runs as ex-

Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

pected to share security events and rulesets to the network, and new rulesets are distributed on demand as instructed by the security center.

- **Collaborative UTM**

The CNSMS aims to develop a new collaboration system to integrate a well deployed UTM such as NetSecu.

There are mainly two tasks for UTM:

Internal protection: The network flows between Internet and Enterprise Network are filtered and monitored, by taking advantage of its ability of firewalling, intrusion detection and anti-virus.

Server protection: In order to protect the resources, by setting up the corresponding firewall settings the UTM should disallow any access to server network from outside and restrict access from internal users. [6]

- **Security Center**

The key function in the security center is the forensic analysis of the collected traffic and network security issues. It generates security rules for enforcement in the UTM to suppress the communication between bots and botmaster. The most important feature of this system is its close loop control characteristics, i.e., gathering the feedback events resulting from the deployed rules, processing and analyzing in control nodes, removing invalid rules to make the system more efficient and reliable and the rules are redistributed.

- **Traffic Prober**

A traffic prober is the building block for recording the raw Internet traffic at connection level. The traffic probe can be designed to focus on specific traffic occasioned by certain security events when needed. It can be designed to focus on special traffic incurred by security event. [5]

Figure 2 shows the sample data traffic from HTTP traffic account. A typical 512MB of collected data block consists of about 40k HTTP URLs.

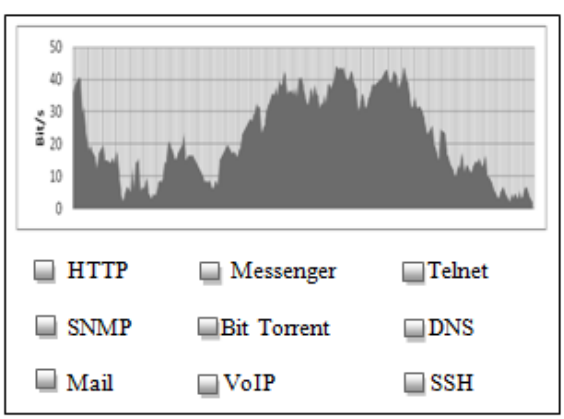

Figure 2: Traffic observed by traffic prober

VALIDATION

- **Analysis of ACO and PSO**

Ant Colony System (ACS) is an agent-based system, which develops mechanisms of cooperation and learning on the basis of the natural behavior of ants. Based on pheromone trails updating, ACO is differ from the classical ant system in two ways. Firstly, when ants construct a tour they locally change the amount of pheromone on the visited paths. Secondly, a global updating rule is applied to modify the pheromone level on the paths after all the ants have built their individual tours. [7]

Particle swarm optimization (PSO) is an algorithm developed on swarm intelligence to find a solution to an optimization problem and predict social behaviours. The PSO is a random, population-based computer algorithm modelled on swarm intelligence.

The ACO is inspired by the aging behaviours of ant colonies. At the core of this behaviour the indirect communication between the ants enables them to find short paths from their nest to food sources. To find solution for discrete optimization problems, the features of real ant colonies is used in ACO algorithm. The PSO algorithm developed on the social behaviours observed is animals or insects; PCO has gained increasing popularity among researches and practitioners as a robust and efficient technique for solving difficult robust and population n based stochastic optimization problems.

Both the ACO and PSO algorithm are the data classification algorithms by implementing swarm behavior. The ACO is more applicable for problems for which source and destination are predefined and specific. PSO is a clustering algorithm in the areas of mutli-objective, dynamic optimization and constraint handling. The ACO is more applicable for problems that require sharp results and PSO is applicable for problems that are indistinct in nature.

TABLE.I TIME COMPARISON OF ACO AND PSO

Optimization	Accuracy	Time Taken
PSO Optimization	88%	10ms
ACO Optimization	90%	8ms

TABLE.I shows that the ACO produce more accuracy and less time taken than PSO. When selected 900 URLs are randomly used for 10 fold cross validation test, 858 URLS are classified correctly and the remaining 42 URLS are classified incorrectly. Based on these details percentage of prediction accuracy is calculated. Thus ACO algorithms are more accurate for classifying huge amount of data efficiently.

SUPPRESSION OF BOTNET

Suppressing botnets is increasingly difficult because the botmaster will keep their own botnets as small as possible not only to hide themselves but also to spread the botnets in an easy way. Additionally, bots can automatically change their Command and Control server (C&C) in order to hide and rescue themselves. Collaborative Network Security System can be used for a distributed botnets suppression system, automatically collecting network traffic from every collaborative UTM in a distributed mode and then processing these collected data in the security center. The detection algorithm proposed is based on behavior features of botnets so the system will generate and distribute rules when botnets are detected in processing. [3]

PHISHING ATTACK PREVENTION

Cloud computing platform was used for offline phishing attack forensic analysis. First, our CNSMS collected the network trace data and reported to the security center. Then the security center distributes the security rules to each node in the network. All phishing filtering operations were based on cloud computing platforms and run in parallel with a divide and conquer scheme. [4]

FLOODING ATTACK PREVENTION

The CNSMS will detect attacks and generates rules to prevent the attack, these rules are distributed to the network and feedbacks are evaluated. After that the invalid rules are eliminated and the new rules are distributed to the network. Whenever the attacks are detected, these processes are repeated.

CONCLUSION

High speed classifications and detection of vulnerabilities for

Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

CNSM in cloud computing will detect the malicious attacks in parallel. By using the parallel processing for the traffic collection and classification will increase the performance speed. Vulnerabilities can easily analyze from the classified data. Increasing the speed of collecting the data and its classifications is done by using the ACO optimization technique. Botnet suppression, forensic analysis of phishing and flooding attacks are present in this paper. This solution is economical for large scale forensic analysis for traffic data in parallel.

REFERENCE [1] Jignesh Vania, Arvind Meniya, H. B. Jethva. "A Review on Botnet and Detection Technique", International Journal of Computer Trends and Technology- volume4 Issue1- 2013 | [2] B. Mu, X. Chen, and Z. Chen, "A collaborative network security management system in metropolitan area network", in Proc. the 3rd International Conference on Communications and Mobile Computing (CMC), Qingdao, China, 2011, pp. 45-50. | [3] F. Han, Z. Chen, H. Xu, and Y. "Liang, Garlic: A distributed botnets suppression system", in Proc. IEEE ICDCS workshop on the First International Workshop on Network Forensics, Security and Privacy (NFSP), Macau, China, 2012, pp. 634-639. | [4] Radha Damodaram & Dr.M.L.Valarmathi "Phishing Website Detection and Optimization Using Particle Swarm Optimization Technique", International Journal of Computer Science and Security (IJCSS), volume (5): Issue (5): 2011. | [5] Zhen Chen, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen, "Cloud Computing-Based Forensic Analysis for Collaborative Network", Zhen Chen, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen, TSINGHUA SCIENCE AND TECHNOLOGY Volume 18, 2013. | [6] F. Deng, A. Luo, Y. Zhang, Z. Chen, X. Peng, X. Jiang, and D. Peng, "TNC-UTM: A holistic solution to secure enterprise networks", 9th IEEE International Conference for Young Computer Scientists(ICYCS 2008), Zhangjiajie, China, 2008, pp. 2240-2245. | [7] Dr.R.Umarani, V.Selvi, "Comparative Analysis of Ant Colony and Particle Swarm Optimization Techniques", International Journal of Computer Applications (0975 – 8887) Volume 5– No.4, August 2010. |