International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Prevention of Mobile Botnet in VPN

Sukhwinder Singh[1], Navdeep Kaur[2]

[1]Research Fellow, Sri Guru Granth Sahib World University, Punjab, India

[2]Associate Professor, Sri Guru Granth Sahib World University, Punjab, India

Abstarct: ***Threats are everywhere on the internet, but most significant and crucial threat is Botnet that control and command by a Botmaster. Bot is simply a machine that acts as a zombie and try to effect all other machine available in network and that all machine are comes under control of Botmaster. It can detect by using honeypots, spamming botnet, network based, behavior based techniques. There are techniques to detect botnet but there is no scheme for prevent the network from Bot. In this thesis, prevention of botnet can be done by cryptography. Although two basics algorithms MD5 and Blowfish are used to detect and prevent the compromise node. Botnet cannot be delete from the network but possibility is that, neglect compromised node from the network. So, after detection, simply remove that node from the network then network became reliable to communicate.***

Keywords: Mobile Botnet, vpn, blowfish, md5

1. Introduction

The easily availability and speed of digital communication have become an integral part of home computer use, as well as all other aspect of use from education to business and research [1]. whereas development of network applications, many different kinds of network services are used by users, such as Cyberbank, Instant Messaging, Online Shopping, Blogs, photo albums and so forth. Users can not only do commercial transactions and entertainments in the Internet, but also bring the convenience of the daily life. Thus, much confidential information are transferring in the Internet [2]. While high-speed computer networking and the Internet have brought great convenience, an ample of security challenges have also emerged with these technologies. Amongst different computer network security threats like viruses and worms, Botnets have become the most dangerous [3,4].

A Bot, originating from the term 'RoBot', is an application that can perform and repeat a particular task faster than a human moreover when a two or more than two Bots spread to ample of computers and connected to each other with the help of internet, they form a group that is usually known as a Botnet i.e. network of Bots [1]. Bot is a compromised device as a zombie which can be controlled and coordinated remotely by Botmaster or Botherder through command & control servers[5,6]. Bot is used to infect computers and mobile devices that are well connected to internet and make them a part of network of Bots without any knowledge of user.

Nowadays smart phones very popular and obligatory in human's life, so they become major attractive targets of mobile threats. Attackers use various attack vectors which are useful to routes to get into mobile devices i.e. SMS (short messaging service), MMS (multimedia message), Internet access help of WIFI or 3/4G and Bluetooth[7]. These mobile Bots communicate with C&C Server with the help of C&C Channel through internet and cause of frequently change of logical address (IP Address) during mobility, existing approaches such as take down an active C&C channel cannot apply on mobile Botnet. Thus, build a VPN (Virtual Private Network) which provides a common shared path for both internet access and provide same environment as if wired network. Then, we proposed a work to introduce a new prevention scheme for mobile Botnet. This scheme consists of cryptography algorithms MD5 and Blowfish algorithms. We are expecting that both algorithms provide better prevention.

The rest of the paper is organized as follows. In Section 2, we review related works on mobile Botnet and detection as well as prevention schemes. In Section 3, we propose our network based Botnet prevention scheme. In Section 4, we verify our scheme with results collected under the attacked environment. In Section 5, a conclusion and future scope are provided.

2. Related Work

As mobiles devices such as smartphones, have become broadly used and indispensable in nowadays human lives, these devices are major attractive target of mobile threats. Thus, one of the most crucial threats is Mobile Botnet in the mobile environment. It firstly found in Symbian OS and moved to IOS and Android[8]. Most of the mobile devices connected to NAT gateway due to lack of IP addresses and not easily reachable [9]. In addition to it, IP address changed can be changed frequently.

Mobile infrastructures and Cloud have latterly become a new platform for Botnet activities. Since, they have not explored completely yet. However, clouds are dynamically monitored and secured by cloud vendors and Botnets are easier to shutdown compared to other types[10]. Though on flip side, mobile devices are not properly protected as of computers and computer networks and user of these mobile devices pay less attention towards security updates [11].

To detect Mobile Botnet, detection techniques are classified as signature-based and anomaly-based by detection method. In signature-based, a signature is a unique mark contained in the context of a packet. For instance, Snort is a signature-based open source intrusion detection system(IDS) that monitors traffic of network to find out the signs of intrusion. Like most IDS systems, Snort is configured with a set of rules or signatures to detect Botnet[12]. Anomaly-based

detection aims to detect significant variations from normal behavior[13]. In [14,15,16], anomaly-based detection using Support Vector Machines(SVMs) or Hidden Markov Model(HMM) with Both malicious and normal behaviors find malwares from their partial or incomplete behaviors.

In previous work [5] it is impossible to monitor all the traffic through internet access in the C&C channel. So, build a VPN between a Bot and a C&C server, which provide a shared path for both 3/4G and WiFi traffic. A VPN is a private network that uses a public network to connect remote sites of same or various networks together using security procedures such as encryption [17]. By implementing one end of VPN at IDS, whole traffic to/from the Bots must go through IDS and a mobile device is placed at another end of VPN. IDS detects malicious packets to/from a mobile device from/to the C&C server. To detect C&C traffic, VPN IDS provides the function of PPTP(Point-to-Point Tunneling Protocol) routing and server. It enables the communication from mobile to a VPN server. VPN IS provides routing by permit the communication between a PPTP server and Internet using NAT. VPN IDS works as a gateway in the same way as in wired network/infrastructure, and detect mobile C&C channel.

3. Proposed Work

In our proposed work to introduce a new prevention scheme for mobile Botnet. This scheme consists of MD5 and Blowfish algorithms. We are expecting that both algorithms provide better prevention.

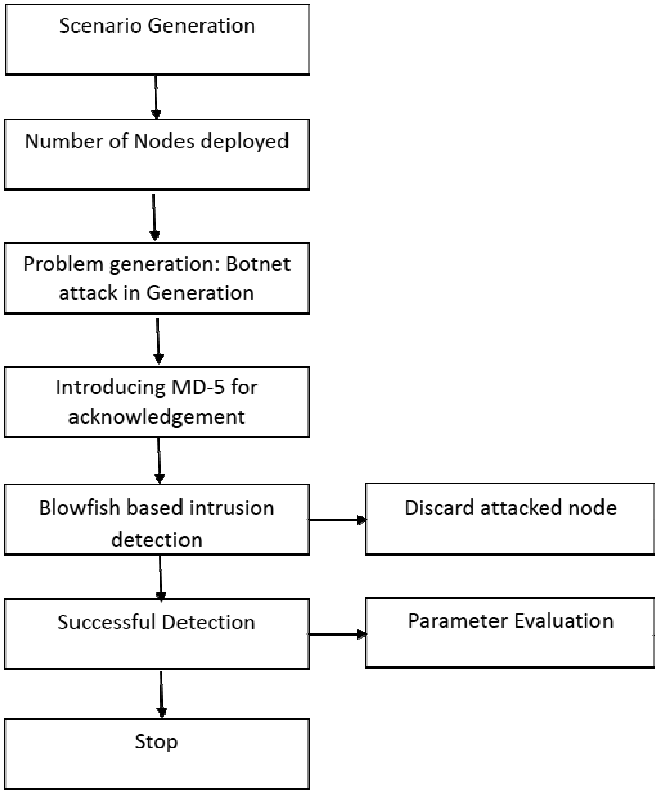

Figure 1: Flow Chart of Proposed Work

In flow chart, scenario of virtual private network in generate on a Network Simulator tool with a numerous nodes that are inter connected to each other. MPLS (multiprotocol label switching) is enable on each and every node on demand, whenever a node wants to send data to another node, it works in short path labeling rather than long network addresses avoiding routing table. Now, problem generation takes place with the help of Botnet on a VPN. Botnet tries to get control of whole network nodes using fake packets, here we introduce MD5 algorithm for encryption of acknowledgment. Moving further, whenever Botnet attacks on vpn network or node then it send a hello packets firstly then VPN node send a encrypt message to Bot with the help of md5 and blowfish, if node able to decrypt message then it will join the network either unable of take long time then node will suppose to a threat and discard from network.

4. Experimental Results and Analysis

Generating a scenario on Ubuntu with the help of NS2, every time and scenario is different layout because the nodes are deployed randomly. Red packets show when a node or system is compromised by Bot whereas blue packets foe reliable communication. On each and every node MPLS (Multiprotocol Label Switching), MPLS is scalable, protocol-independent transport. In a MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol.Here node number 1 and node number 10 are having red color which show that there is delay in the traffic and node number 0 and 9 are of blue color which show that traffic is sending without delay. Other nodes having black color shows there is no traffic between nodes or these are communicate nodes for both red and blue nodes.

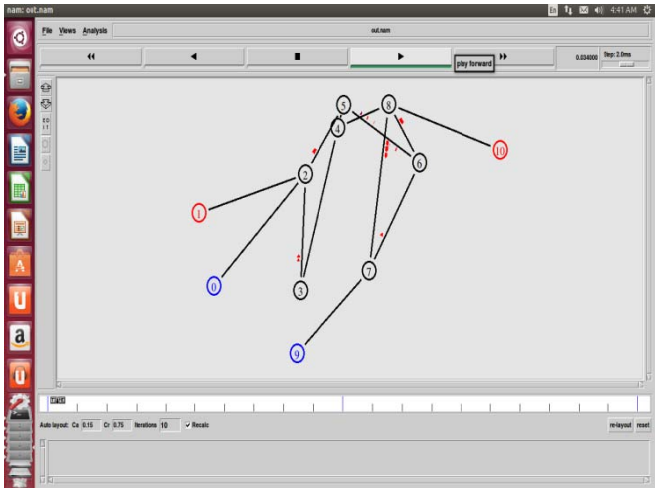

Figure 1: Experimental Scenario

5. Results

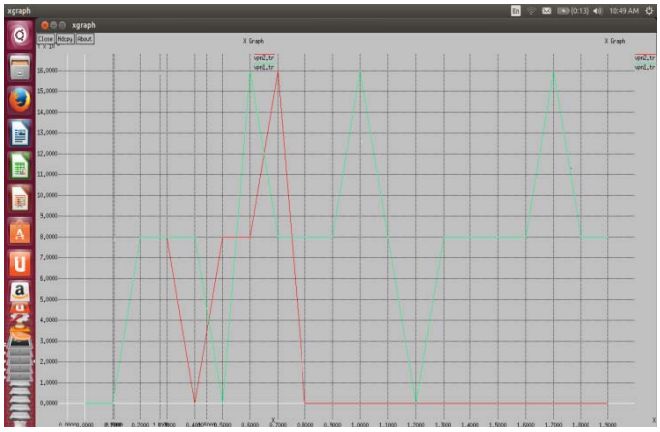

Figure 2: Represent Signal Communication Strength

In Fig. 2: represents signal communication strength here red line is showing strength during attack and green line show after detection the\of attack the lifetime is increased. Here x-axis denotes the time and y-axis denotes iteration of data for the detection of attack. It shows the prevention of the attack on the system. When attack on network (red lines) then original signal strength (green lines) interrupted by attacker's signal strength that make network slow for a while as well as signal also fluctuate because red lines share bandwidth of network though after prevention the green lines strength remain as usual as before attack.

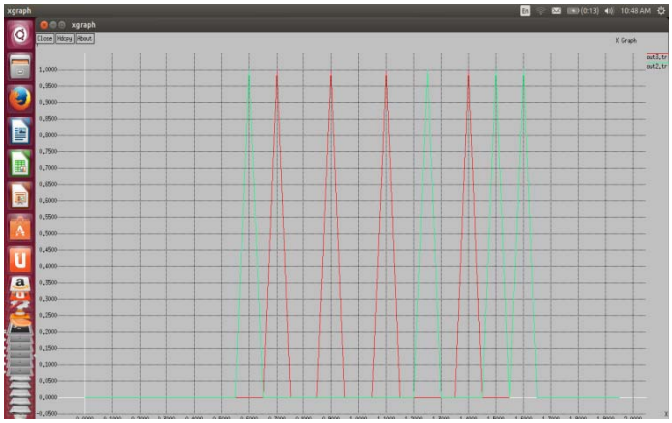

Figure 3: Represent System Distortion

In Fig. 3: the red line is for attack and green line is for detection these two lines show the peak values for the system. In this x-axis shows the time and the y-axis define the distortion occurred in the network and less will be the distortion more reliability is there. When system start up after some time red lines of attack distort the system with its peak value but after prevention the red lines disappear from figure and original system frequency (green lines) retain peak value after neglecting red lines of attack.

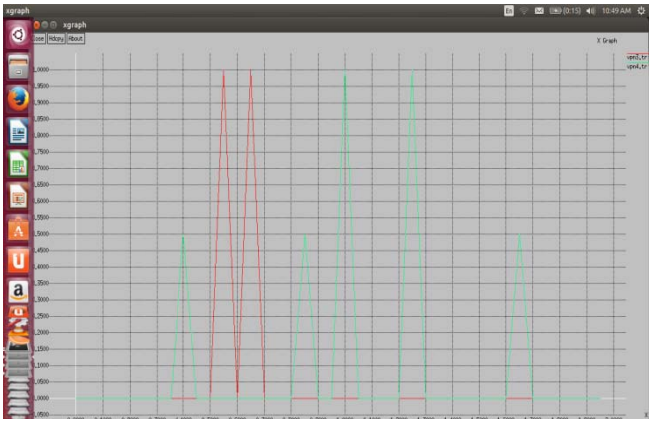

Figure 4: Represent Actual System During and After Attack

In Fig. 4: the red line represent system during attack and green line represent system after attack. Here x-axis shows the time and y-axis shows the performance of the system. In given figure, when system under attack its performance goes down as red lines show where green lines at zero level it original performance at minimum value but after prevention performance of system become reliable because attack performance now at zero level that depicts prevention is done.

6. Conclusion & Future Work

VPN network traffic is controlled by using security algorithm Blowfish and MD5. Blowfish provides a good encryption rate in software and no effective crypt analyzing it has been found till date. Blowfish has a 64 bit block size and variable key length from 32 up to 448 bits and MD5 is message digest having version 5 which is used for encryption procedure. It provide more security to the system. This is implemented by using simulator NS2 and in results various scenarios are discussed and figures are shown during attack, after detection and prevention of attack. These figures conclude that the system become efficient by applying security algorithms.

In future we can make network more reliable with the help of backup node, having address of all nodes available in the network. Whenever a node compromised or detected as a bot then node will be deleted from network. On the place of deleted node, back up node will placed to make network available for communication with interconnect nodes of deleted node.

References

[1] MeisamEslahi, RosliSalleh, Nor BadrulAnuar, "**Bots and Botnets: An Overview of Characteristics, Detection and Challenges**" IEEE International Conference on Control System, Computing and Engineering, pp. 349-354, 23-25 Nov 2012.

[2] Nam-Yih Lee, Hung-Jen Chaing, "**The Research of Botnet Detection And Prevention**" Computer Symposium (ICS), IEEE, pp. 119-124, 16-18 Dec 2010.

[3] M. La Polla, F. Martinelli, and D. Sgandurra, "A **Survey on Security for Mobile Devices**," IEEE Communications Surveys & Tutorials, 2012, doi:10.1109/SURV.2012.013012.00028.

[4] L. Chao, J. Wei, and Z. Xin, "**Botnet: Survey and Case Study**," in Proceedings of the Fourth International Conference on Innovative Computing, Information and Control (ICICIC), 2009, pp. 1184-1187.
[5] ByungHa Choi, Sung-kyo Choi, Kyungsan Cho, "**Detection of Mobile Botnet Using VPN**" Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 142-146, 3-5 July 2013.
[6] N. Hachem, Y. Ben Mustapha, G. G. Granadillo, and H. Debar, "**Botnets: Lifecycle and Taxonomy**," in Proceedings of the Conference on Network and Information Systems Security (SAR-SSI), pp. 1-8, 2011.
[7] M. Chandramohan and H. Tan, "**Detection of Mobile Malware in the Wild**", *Computer*, vol. 45, pp. 65-71, 2012.
[8] Juniper, "**Malicious Mobile Threats Report**" 2010/2011, 2011.
[9] GuiningGeng, Guoai Xu, Miao Zhang, YanhuiGuo, Guang Yang, and Cui Wei, "**The Design of SMS Based Heterogeneous Mobile Botnet**," Journal of Computers, Vol 7,Nno. 1, 235-243, Jan 2012.
[10] Y. Chen, V. Paxson, and R. H. Katz. (2010). "**What's New About Cloud Computing Security?**"[PDF]. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf
[11] E. Yuce, "**A Literature Survey About Recent Botnet Trends**," GÉANT Network, ULAKBIM,Turkey, Rep. JRA2 T4, 2012.
[12] M. Feily, A. Shahrestani and S. Ramadass, "**A Survey of Botnet and Botnet detection**," Procs of Third International Conference on Emerging Security Information, Systems and Technologies, pp. 268 - 273 Jun. 2009.
[13] F. Giroire, J. Chandrashekar, Nina Taft, Eve Schooler, and Dina Papagiannaki, "**Exploiting Temporal Persistence to Detect Covert Botnet Channels**," Procs. of the 12th International Symposium on Recent Advances in Intrusion Detection, RAID '09, No. 20, pp. 326-345, 2009.
[14] Byungha Choi, and Kyungsan Cho, "**Detection of Insider Attacks to the Web Server**," Jounal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 3, No. 4, pp. 35-45, 2012.
[15] L. Xie, X. Zhang, J.-P. Seifert, and S. Zhu, "**pBMDS: A Behaviorbased Malware Detection System for Cellphone Devices**," Procs. of the 3rd ACM conference on Wireless Network Security, WiSec Oct. 2010.
[16] A. Bose, X. Hu, K. G. Shin, and T. Park, "**Behavioral Detection of Malware on Mobile Handsets**," in Procs. ofMobiSys, pp. 225 - 238 Jun. 2008.
[17] K. Grewal, and R. Dangi , "**Comparative Analysis of QoS VPN Provisioning Algorithm on Traditional IP based VPN and MPLS VPN using NS-2**," International Journal of Computer Applications, Vol. 48, No.1, pp.43-46, June 2012.