RESEARCH REVIEW JOURNALS
Volume-03
Issue-08
August-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Flow-based programming approach to mitigate the Denial of Service Attack on Internet of Things Application

[1]Anup Ingle, [2]Dr. Avinash Gour and [3]Dr. Ketki Kshirsagar

[1]Research Scholar, Dept. of Electronics and Communication Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal Indore Road, Madhya Pradesh, India
[2]Research Guide, Dept. of Electronics and Communication Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal Indore Road, Madhya Pradesh, India
[3]Research Co-Guide, Dept. of Electronics and Telecommunication, VIIT, Pune, Maharashtra, India

ARTICLE DETAILS

Article History
Published Online: 07 August 2018

Keywords
DOS, IP Spoofing, Internet of Things, Embedded, Flow-based programming.

ABSTRACT

Due to integral part of day today life and increasing demand in computer system, mobile, smart phones, tabs, electronic gadgets and internet application leads to the growth of smart controlling devices, smart watches, and smart application as a part of Internet of Things with the Ethernet and wireless application; which enforce the invader to offers the controlling of physical access to the device and correspondingly breeding the undesirable internet traffic. Flow-based programming approach will improve the performance of traditional IDS and provide the ultimate solution to secure the objectionable traffic by ascertaining and confining it at its Origin.

1. Introduction

Smart Cities Mission is a metropolitan rebirth and retrofitting program by the Government of India (GOI) with a mission of developing 100 cities all over the country fabricating them for resident benefit. The Union Ministry of Urban Development is accountable for implementing the assignment in association with the state governments of the corresponding cities. The GOI under Prime Minister of India has a vision of developing 100 smart cities as satellite townships of superior cities and by remodeling the existing infrastructure.

In 2014 Union budget of India, Finance Minister allocated 70.16 billion (US$1.0 billion) Indian rupees for the development of 100 smart cities, which are projected to be equipped with basic infrastructure offering a good quality of lifecycle through smart solution to the civilian, secure water supply, power supply, sanitation and solid waste management, well-organized urban mobility and public transport, robust IT connectivity, e-governance and citizen participation along with safety of citizens[1]-[5].

New Internet technologies endorsing cloud based services, [6] the Internet of Things (IoT), real world user interfaces, use of smart phones and tablets, networks of sensors, GSM and GPS based solutions and RFIDs, and more accurate communication based on the semantic web, open new ways for collective action and provide collaborative solution to the problem. But, this infrastructure development will cause the invader to compromises the directing of physical access to the device and subsequently advanced the undesirable internet issues like Denial of Service (DOS).

Numerous solutions are providing by the various developers and designer of IT infrastructure development (includes routers, switches, gateways, etc.), but many issues (like vulnerable spoofing attacks) are still persists and no optimistic solution is available to devour this violence. FBPA will give remarkable solution to accomplish this sort of threat [7]-[12].

2. Attacks and Recognition

Attacks are basically categorized into two parts, i.e. active and passive attack. Active attacks are used basically to amuse and distract the device leading to strike or drain the system which enforces the machine towards denial of service (DOS) application. Passive attacks are used to spy or monitoring application in legal as well as illegal mode. These attacks are done for the purpose of seeking advantage from the victim. Whereas there is no intention of the server to deny the service; it's happen due to the network traffic is jammed at its node due to heavy volume of illegal traffic generated by the invader.

Both the attack categories are basically having two detection approaches, i.e. Signature and Anomaly based recognition. Signature based approach is pre-defined feature approach, in which characteristic based features are used to detect the threat. And anomaly is volume based deviation approach, in which sudden changes in normal traffic based on bandwidth utilization is used to discover the threat. This anomaly traffic is most dangerous traffic in the network because of its execution with high bandwidth of traffic from the attacker. In this attacker is using the normal machines which are from the school, colleges, industry which are not having practice to follow the normal internet or network guidelines. Now a day, the invaders are using the smartphones, android device, tablet to initiate such type of application. In early days, invaders were using the desktop from private internet café. It was easy to target this machine as it is handled by various customers. It is most compromise and vulnerable machine to use for initiating the huge volume of traffic as most probably it is found in ON condition.

3. Flow-based Programming Approach

An algorithm was invented by J. Paul Morrison in the early 1970s based on flow-based programming approach (FBPA). It gives the remarkable solution in the industries and huge demand of the leading industries like IBM (term also referred as Data Flow), Facebook, Goggle, Apple, etc. Previously, it

was not adopted in breeding the application for the websites and others, also not been considered while developing the TCP/IP protocol suite. Now day's flow-based solution is one of the integral part of the programming for designing and emerging the end to end application used by the programmer to cultivate cloud based websites platform in generating the smart controlling devices and smart application as a part of Internet of Things.

In flow-based programming approach the predefined programs are deploy to define the predefined connection at the computers; like one of the applications is socket programming. In such a way that programmer has to integrate the designed program into the chip which leads to the development of Application Specific Integrated Circuits (ASIC) at network layer or kernel layer at itself in development of Ethernet application or the wireless application like Wi-Fi and Bluetooth or there is a solution to write the code at the application layer; which we have done in our programming.The predefined connections are like 'black-box' process, which is used in discovering the machine within the network and also to send query/ messages to other machine in the network. Domino effect is that, process running at every machine within the network will interrelate with each other and works like strainers which correspondingly eliminate the undesirable internet traffic. Conjointly all the machine in the network or at the age of network will secure the objectionable traffic by confining it at its Origin. Correspondingly it is shown in the figure 3.1 [13]-[15].

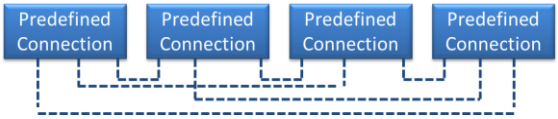

Figure 3.1 Flow-based Programming Approach

Figure 3.1, shows the computers in the network with Predefined Connection (PDC) process, all the machines are connected through Ethernet switch in LAN environment and interacting and query sharing with each other's.

4. IP Spoofing Attack

Spoofing attack is a most perilous traffic in the field of cyber-attack; in which invader devour the bandwidth of the network by bombarding the heavy traffic into the network by pretending one of the legitimate users among the network and accomplish the illegitimate advantage. Many categories and sub-categories of spoofing attacks areattainable in the market and easily endeavored (like IP/ ARP/ referrer/ Caller ID/ Voice mail/Email/ GPS spoofing, etc.) in Ethernet and wireless application.

IP Spoofing takes the advantage of vulnerable TCP/IP protocol suite in which respective traffic (ICMP, UDPand TCP-SYN) has been generated to spoil the network bandwidth which accomplishes the Denial of Service (DOS) attack [16]-[19].

5. Execution and Real solution

To demolish the IP spoofing attack from the network - the ultimate proposed solution is to write the application specific code called Pre-defined Program (PDP) and integrated or inbuilt it on ASIC gives the Pre-defined Connection (PDC) on each and every machine of the network varies from computer, layer-2 or layer-3 switches to routers and gateways which are interacting with each other via Information and Query Sharing; shown in figure 5.1 and 5.2.

It results, that the devices are comparing and analysis the results on the basis of volume of bandwidth utilization of each terminal and generating the alert for the same to the user by popups on the terminal or via alarm. Also judgment and investigating the origin of attack packet source port via stress back mechanism and edge the traffic at its origin which shrinks the bandwidth utilization at the user terminal. The ports are pre-programmed in such a way that it endorses as like ingress and egress filter to devour the undesirable and unwelcome traffic towards it origin in the network by dropping the packets. [20]-[24]

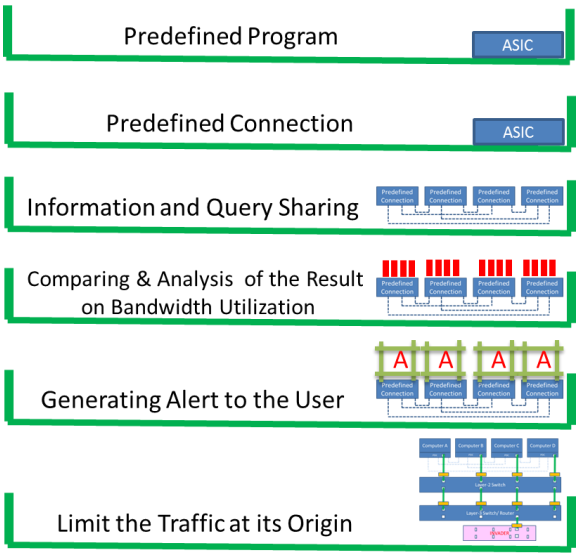

Figure 5.1 Real time solutions at each node in the network

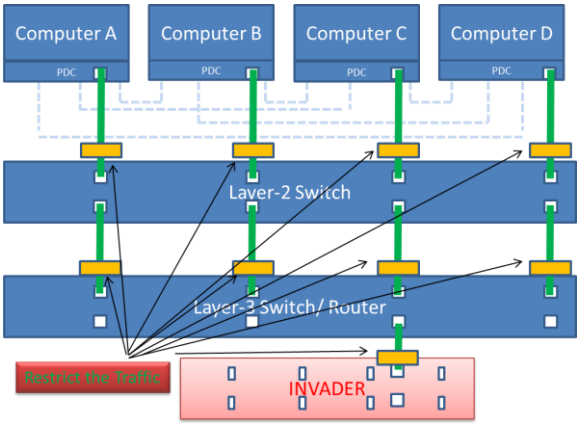

Figure 5.2 Ingress and Egress filtering

6. Implementation and Result

In our laboratory setup, we have executed the one of the defenseless attack; i.e. IP spoofing attack. As shown in figure 6.1, the Lab consist of twenty computers (Intel (R) Core (TM) i3-2100 CPU @ 3.10 GHz, 4GB RAM, etc.) attached to 2-layer switch; which is also approachable to the 3-layer switch and one of the attacker machine is attached to 3-layer switch to simulated the IP spoofing attack; it includes the ICMP, UDP and TCP/ SYN traffic.

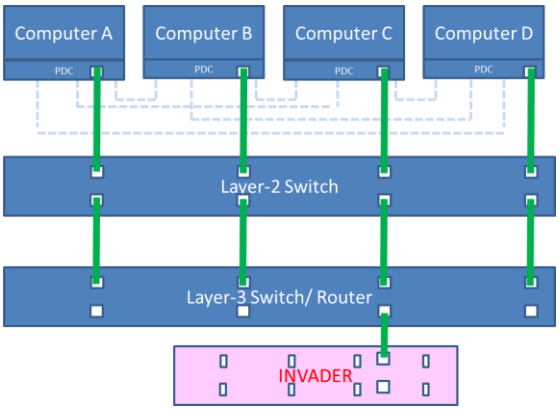

Figure 6.1 Laboratory setup

Figure 6.2 PDP Approach for Comparing and Analysis of the Result on Bandwidth Utilization

The invader chose the any one of the above traffic and sends this traffic to other computers in the network by selecting the random IP address of computers from the laboratory network.

The predefined program developed in JAVAis installed on every next computers of network has programmed for information and query sharing. This predefined connection are comparing and analyzing the results on the basis of bandwidth utilization at each terminal and similarly validate the alert messages to the user. The results are displayed in figure 6.2, 6.3, 6.4

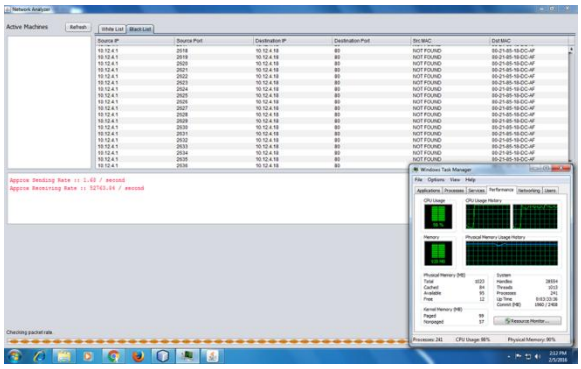

Figure 6.3 Bandwidth utilization of single system

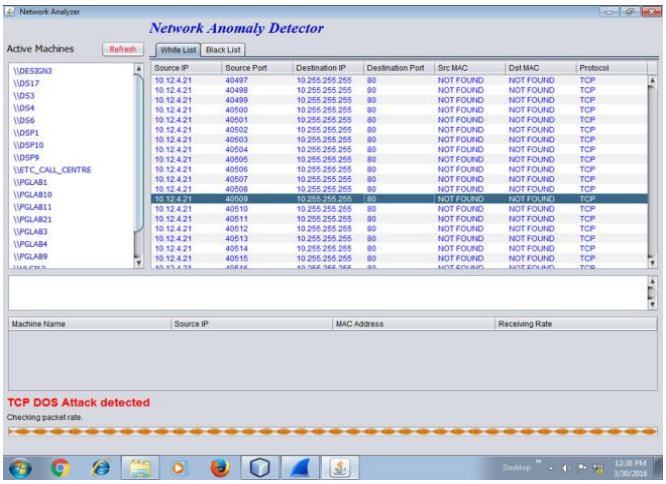

Figure 6.4 Alerting - TCP DOS Attack Detection

7. Conclusion

The attack recognition and confiscating solution is proposed in this paper. The first one by flow-based programming approach (FBPA) and another one is chain-of-reporting(CoR) application integrated on chip. The predefined connection in FBPA is the ultimate solution in finding any of the traffic varies from the slow to heavy rate circulation; even it is applicable to handle the legitimate traffic as well. And the chain-of reporting by corresponding port of every device attached in the network to confine the traffic at its origin. FBPA solution to detect attack is successfully implemented in our laboratory experiment to recognize the most vulnerable IP spoofingattack traffic (like ICMP, UDP and TCP-SYN, etc.) generated from self-coded program and readymade tools like hping3.

8. Future Scope

Further scope of this research is to identify other pattern of attack and detect the attack at the network node and use the mitigation technique by dropping the packet which are coming from the invaders or other source by implementing it at the various layer of node;

- At the kernel layer
- At the network layer
- At the application layer

9. Acknowledgment

I put my sincere gratitude towards my PhD center ‘Sri Satya Sai University ofTechnology & Medical Sciences’ and my Guide ‘Dr. Avinash Gour’ and my Co-guide‘Dr. Ketki Kshirsagar’ for given freedom to choose this subject for PhD and implement the same, also put my sincere gratitude towards my institute ‘Vishwakarma Institute of Information Technology’ for providing consistent encouragement; to do the further education and skill enhancement. Also, my colleague and students those help me in understanding the concept and to simulate and executed the experiments in the laboratory.

References

[1] “Mission Statement and Guidelines - Smart Cities” (PDF). Ministry of Urban Development, GOI. Retrieved 1 February 2016.
[2] “Narendra Modi launches smart city projects in Pune”, *Live Mint*, 25 June 2016

[3] "Bhubaneswar leads Govt's Smart City list, Rs 50,802 crore to be invested over five years", The Indian Express (New Delhi), 29 January 2016
[4] Cabinet nod To Rs 1 lakh cr for urban renewal, 98 smart cities to take off, New Delhi: Business Standard, BS Reporter, 30 April 2015
[5] Smart City – Mission Statement & Guidelines, Ministry of Urban Development, Government of India, June 2015.
[6] Michael Vogler, "Migrating Smart City Applications to the Cloud", published in IEEE Cloud Computing, Vol-3, Issue-2, 2016, DOI: 10.1109/ MCC.2016.44.
[7] Nanda Kumar Thanigaivelan, "Distributed internal anomaly detection system for Internet-of-Things", 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016, DOI: 10.1109/ CCNC.2016.7444797
[8] Chordia Anita S.,"An effective model for anomaly IDS to improve the efficiency", International Conference on Green Computing and Internet of Things (ICGCIoT), 2015 , DOI: 10.1109/ICGCIoT.2015.7380455
[9] Audrey Ann Gendreau, "Situation Awareness Measurement Enhanced for Efficient Monitoring in the Internet of Things",Region 10 Symposium (TENSYMP), 2015 IEEE, DOI: 10.1109/TENSYMP.2015.13
[10] Chen Jun; Chen Chi, "Design of Complex Event-Processing IDS in Internet of Things", 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation, DOI: 10.1109/ICMTMA.2014.57
[11] Tein-Yaw Chung; Ibrahim Mashal; Osama Alsaryrah; Chih-Hsiang Chang; Tsung-Hsuan Hsu; Pei-Shan Li; Wen-HsingKuo, "MUL-SWoT: A Social Web of Things Platform for Internet of Things Application Development", Internet of Things (iThings), 2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing(CPSCom), IEEE, DOI: 10.1109/iThings.2014.53
[12] Abhishek Gupta; Om Jee Pandey; Mahendra Shukla; Anjali Dadhich; Samar Mathur; Anup Ingle, " Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2013, DOI: 10.1109/ICCIC.2013.6724156
[13] Martin Andreoni Lopez; Otto Carlos M. B. Duarte, "Providing elasticity to intrusion detection systems in virtualized Software Defined Networks", 2015 IEEE International Conference on Communications (ICC),DOI: 10.1109/ICC.2015.7249462
[14] Pin-Jui Chen; Yen-Wen Chen, "Implementation of SDN based network intrusion detection and prevention system", International Carnahan Conference on Security Technology (ICCST), 2015, DOI: 10.1109/CCST.2015.7389672
[15] ZonglinGuo; Ram Bhakta; Ian G. Harris, "Control-flow checking for intrusion detection via a real-time debug interface", International Conference on Smart Computing Workshops (SMARTCOMP Workshops), 2014, DOI: 10.1109/SMARTCOMP-W.2014.7046672
[16] Francisco de AsísLópez-Fuentes; Salvador Balleza-Gallegos, "Investigation of Effects of Spoofing Attacks in P2P Online Social Networks", 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2016, DOI: 10.1109/WAINA.2016.124
[17] VahidAghaei-Foroushani; A. NurZincir-Heywood, "Autonomous system based flow marking scheme for IP-Traceback", IEEE/IFIP Network Operations and Management Symposium, 2016, DOI: 10.1109/NOMS.2016.7502804
[18] Opeyemi. A. Osanaiye; MqheleDlodlo, "TCP/IP header classification for detecting spoofed DDoS attack in Cloud environment", International Conference on Computer as a Tool (EUROCON), IEEE, 2015, DOI: 10.1109/EUROCON.2015.7313736
[19] Shashi Shaw; Prasenjit Choudhury, "A new local area network attack through IP and MAC address spoofing", International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015, DOI: 10.1109/ICACEA.2015.7164728
[20] Jaehyun Nam; Muhammad Jamshed; Byungkwon Choi; Dongsu Han; Kyoungsoo Park, "Scaling the performance of network intrusion detection with many-core processors", ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), 2015, DOI: 10.1109/ANCS.2015.7110135
[21] Santosh Kumar Sharma; Debnath Bhattacharyya; ManasRanjan Patra; Tai-Hoon Kim, "A New Parallel Hybrid Model - Intrusion Prevention Systems", 8th International Conference on Security Technology (SecTech), 2015, DOI: 10.1109/SecTech.2015.17
[22] Miltos D. Grammatikakis; Polydoros Petrakis; AntonisPapagrigoriou; George Kornaros; Marcello Coppola, "High-level security services based on a hardware NoC Firewall module", 12th International Workshop on Intelligent Solutions in Embedded Systems (WISES), 2015.
[23] XiaojunZhai; Kofi Appiah; Shoaib Ehsan; Gareth Howells; Huosheng Hu; DongbingGu; Klaus D. McDonald-Maier, "A Method for Detecting Abnormal Program Behavior on Embedded Devices", IEEE Transactions on Information Forensics and Security, 2015, Volume: 10, Issue: 8, DOI: 10.1109/TIFS.2015.2422674
[24] Nagesh Vaidya; ParikshitGodbole, "Hardware implementation of key functionalities of NIPS for high speed network", International Conference on Computing and Network Communications (CoCoNet), 2015, DOI: 10.1109/CoCoNet.2015.7411296

