Global DDoS Threat Landscape Tracking Network Anomalies using Elliptic Curve Cryptography

[1]K. Ravikumar
[1]Asst.professor,
Dept. of. Computer Science,
Tamil University,
Ravikasi2001@yahoo.com

[2]S. Soundharya
[2] Research Scholar,
Dept. of. Computer Science,
ThanjavrTamil University, Thanjavr
soundharyasankar@gmail.com

Abstract: Devices, such as in mobile devices or RFID. In brief, ECC based algorithms can be easily comprised into existing protocols to get the same retrograde compatibility and security with lesser resources.: Recent variants of Distributed Denial-of-Service (DDoS) attacks influence the flexibility of application-layer procedures to disguise malicious activities as normal traffic patterns, while concurrently overwhelming the target destination with a large application rate. New countermeasures are necessary, aimed at guaranteeing an early and dependable identification of the compromised network nodes (the botnet). This work familiarizes a formal model for the above-mentioned class of attacks, and we devise an implication algorithm that estimates the botnet hidden in the network, converging to the true solution as time developments. Notably, the analysis is validated over real network traces. An important building block for digital communication is the Public-key cryptography systems. Public-Key cryptography (PKC) systems can be used to provide secure substructures over insecure channels without swapping a secret key. Applying Public-Key cryptography organizations is a challenge for most submission stages when several factors have to be considered in selecting the application platform. The most popular public-key cryptography systems nowadays are RSA and Elliptic Curve Cryptography (ECC). The compensations can be achieved from smaller key sizes including storing, speed and efficient use of power and bandwidth. The use of shorter keys means lower space necessities for key storage and quicker calculation operations. These advantages are essential when public-key cryptography is applied in constrained

***KEYWORDS**: DDoS occurrences, Fooling, Detection, Protection, Cryptography, Riddling, Elliptic Curve Cryptography*

*****

I. INTRODUCTION

Distributed Denial of Service (DDoS) is the hurled by large number of distributed attackers in a coordinated manner to interrupt the facilities of the legitimate clients and disproportionately consume the target capitals that prevents the server from responding to legitimate clients. The attack tools are evolving continuously, but there are not enough operative defense mechanisms against such attacks. Protectioninstrument must be able to classify each packet that is nomadic across the router as legitimate or attack and packets identified as the attack packets must not be forwarded to the target. This can avoid the DDoS attack and save valuable target possessions. DDoS attacks with foundation IP address spoofing is of two types. First is direct occurrence in which the attackers send deformed packets with fake source number of compromised hosts in the network.

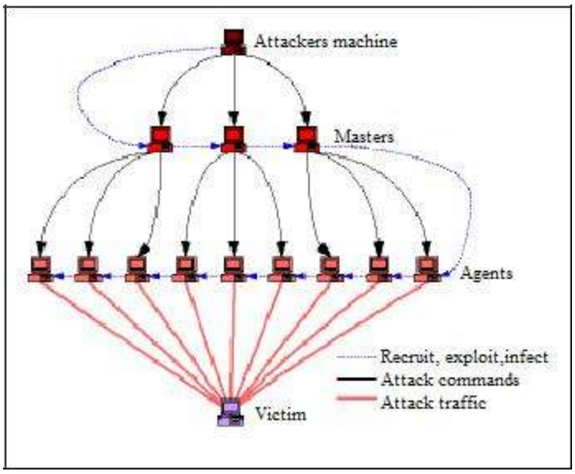

Fig. 1: DDoS attack model.

While forwarding packets near destination only terminus address is often used and source address is never verified. Attackers take benefit of this fact for initiation attack using spoofing of source IP address in order to hide their identity and circumventing the possibility of getting caught. Many protection mechanisms have been plannedin inconsistency of source IP address spoofing such as ingress filtering, hop count-based packet filtering, source speech validity enforcement, etc. that are useful in controlling the spoofed attack packets but complete prevention of deceived IP address attack is still a stimulating problem.

II. RELATED WORK

In this section, review of existing nonfiction on defense devices against Distributed Denial of Service attacks is presented.

S. Yu, et al. [1], proposed a self-motivated resource allocation technique for defensive individual customers of cloud during DDoS attack safeguarding quality of service during attack. The cloud environment is capable of controlling the reserve allocation because it has large number of resources to allocate to individual user. The resource allocation approach used in clouds plays vital role in justifying the influence of attack by giving access to resources. In cloud setting the success of attack or defense be contingent upon who is holding more resources, attacker or cloud user. The dynamic extra resource allocation prevents hunger, thus defending against DDoS attack. They also presented queue-based model of resource allocation under various attack situations. They used real world data set available on DDoS attack for analysis of reserve allocation.

B. Liu, et al. [2], proposed mutual egress filtering for provided that protection against IP spoofing-based flooding attacks using real internet dataset for obtaining simulation results. Access control list of autonomous systems (AS) is used which encompasses list of rules for applying ingress/egress filtering. This method protects the schemes which deploy the mechanism while preventing non-deplorers from freely using it. On-demand filtering is providing and the global registry is maintained that contains peering relations and policies of deplorers. False positive rate reduces by using mutual egress filtering.

In [3], R. Maheshwari, et al. applied distributed probabilistic hop count filtering based on round trip time. Thedevice was organized in intermediate system system for exploiting detection rate of attack traffic and minimizing the calculation time for filtering packets. The imitation results using Matlab 7 showed up to 99% detection of malevolent packets. It is advantageous for solving problems network bandwidth.

In [4], A. Compagno, et al. presented protection against interest flooding dispersed denial of service attacks in NamedData networking. Interest inundating requires limited resources to launch attack. Pending interest table is maintained at rters for avoiding identical interests. Poseidon framework is introduced for detection and extenuation of interest flooding attacks. The evaluation of the framework over network simulation atmosphere using NS3 showed that it is possible to utilize up to 80% available bandwidth during attack using this outline.

J. Francois, et al. [5], proposed cooperative architecture, FireCol which is composed of Intrusion Prevention Systems at the Internet Service Providers level. It uses the rings of interruption prevention systems around a host as single deterrence system is not sufficient to defend flooding-based DDoS attacks. The bouts are detected by observing the detection window for finding out the deviation of traffic from standard traffic pattern. Based on the percentage of deviation, the attacks are classified as low or high possible attack. FireCol system has some rules defined for subscribers that match a pattern of IP addresses. The packet processor in the system inspects the incoming traffic and update counter and frequencies whenever a rule is coordinated. Metrics manager compute entropies and relative entropies. Assortment manager checks whether the traffic delivery was within the outline.

III. Existing Approach

The aptitude for botnets to information a great and miscellaneous range of attack methods, to continueunidentifiedat the same time as doing so and to adapt to the altering cyber safekeeping environment has shaped significant difficulty for researchers in developing a solution. No current mitigation or detection method has been able to offer anything fully adequate or permanent [1]. As a result, there are a number of passive solutions that do not sufficiently address the botnet threat environment [11]. Honeypots as an instance allow researchers to study and analyze behavioral characteristics of malicious entities within a controlled environment. However, whilst successfully giving the ability to collect and analyze bot malware, they agonize due to a number of passive features [11][12]. Not only are they required to wait for an attacker, but they are only able to report information about the infected machines placed as traps so there is very little room for in-depth analysis [8]. This method unfortunately offers little deterrent to malicious behavior. As discovered largely in the botnet solution literature, this restriction with honeypots is also exacerbated by the nature of the research itself, much of which is conducted on a limited collaborative basis. The resourcing needed to fully research every propagation, attack, and communication method obtainable to a botnet hinders the ability of singular or small-group research. As both the potential victim pool and occurrence capability pool rises, this type of research will suffer further. If the research centered approach of honeypots is adapted to a more encompassing and a more collaborative model however, a solution (or solutions) may be calmer to develop. To broaden the scope of research, testing should be conducted on not only the victim machine but also the attacking machine. This is why a framework to develop a more research focused and collaborative approach that could hypothetically be adopted on a wider-scale basis is necessary. This would seek to mitigate some of the issues that are currently faced, predominantly with honeypot research, and would allow a much larger pool of instructive knowledge to be collated in order to develop a solution. After all, thorough, in-depth research and education is realistically the only way an explanation will be developed.

IV. Proposed Approach

Regular checking should take place to further ensure that hateful activity is not being conducted. In the case of DDoS, individual researchers should collate a list of the websites they intend to bout, and either provide proof that particular organizations have decided for it to take place or prove that a targeted website is owned by them. As data will be fed back into a central database, scanning against the organized list, which could potentially become an automated process, should take place to ensure no hateful activity is being conducted. If an organization is found to be using the software for malicious activity, they should be mechanically banned and access detached. Upon entering the DDoS plugin, or any other bout vector plugin for that matter, there could also be a pop-up message that re-iterates that malicious use will not be tolerated, auditing will take place, and somebody found to be using the software for malicious purposes will be banned. Again, this won't necessarily stop individuals leading malicious activity, but would act as a deterrent to the vast majority of members. Indeed, even if the creating research center due diligently checks every application from each investigator, there is always the possible for manipulation, predominantly as there would be little control over organizations' employees that may be by means of the software

4.1 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a public key cryptography. Where each user or the expedient taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the certain user knows the private key whereas the public key is distributed to all users enchanting part in the communication. Public-Key cryptography (PKC) systems can be used to provide secure infrastructures over insecure frequencies without exchanging a secret key.

The most popular public-key cryptography systems today are RSA and Elliptic Curve Cryptography (ECC). Due to directness of wireless sensor networks, secure announcement between nodes is necessary. The Elliptic Curve Cryptography(ECC)] is based on algebraic concepts related with elliptic curves over limited fields Fp or F2m. Elliptic Curve encryption and decryption system requiresemploy G and an elliptic group E_q (a, b)as some parameters.

Encryption using ECC

To encrypt and send a communication Pm to B, A chooses a random positive integer k and harvests the cipher text Cm as given by equation containing of the pair of points.

$Cm = [k*G, Pm + k*P_B]$

Here A has used B's public key P_B.

Decryption using ECC

To decrypt the cipher text, B multiples the first point in the pair by B's private key nB and subtracts the result from the second point as shown by equation.

$Pm + k*P_B - n_B (k*G) = Pm + k (n_B* G) - n_B (k*G) = Pm$

A key exchange between users A and B can be explained as following steps: -

A select an integer $n_A < n$ as A‟s private key.

A generates a public key $P_A = n_A*G$ which is a point in

E_q (a, b).

B select an integer $n_B < n$ as B‟s private key.

B generates a public key PB= nB*G which is a point in E_q (a, b).

.Public keys are exchanged between A and B. A generates the secret key K= nA* PB and B generates the secret key $K = n_B * P_A$

V. CONCLUSION

In this work presented that aninsubstantial cryptographic technique for defending against spoofing attacks that requires no additional overhead on the routers and no changes in the internet routing protocols. By providing substantiation to each packet at the client side and authenticating the packet identity at the routers near the board server can professionally identify the attack packets with fake source IP address. Attack packets are separated from normal packages and dropped before reaching the target server while standard packets are forwarded genuine thus allowing the. The mechanism against DDoS occurrence with 99.9% accuracy, 0% false positives results.

VI. FUTURE SCOPE

It is of course supreme that further research is conducted before application, particularly with the number of potentially adverse variables that need to be considered. Whilst positively there could be a number of possible benefits enabled through the instructive botnet, there are also a number of possible pitfalls, particularly surrounding the ethical nature of the botnet's attack capabilities. What needs to be unspoken however is that despite a wealth of independent research, very little has been talented thus far. This idea, whilst having the potential to be used unethically if payments and balances are not industrialized, does give a greater capability to perform actual attacks; and thereby eliciting a more robust data set for analysis. This in turn gives a capability for further, more in-depth investigation to take place, which may not only resolve the botnet problem but also the wider malware issue.

REFERENCES

[1] S. Yu, Y. Tian, S. Guo, D. Wu, "Can We Beat DDoS Attacks in Clouds?", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2245-2254, 2014.

[2] B. Liu, J. Bi, A. V. Vasilakos, "Toward Incentivizing Anti-Spoofing Deployment", IEEE Transactions on Information Forensics and Security, vol. 9, no. 3, pp. 436-450, 2014.

[3] R. Maheshwari, C. R. Krishna, M. S. Brahma, "Defending Network System against IP Spoofing based Distributed DoS attacks using DPHCF-RTT Packet Filtering Technique", IEEE International Conference on Issues and

Challenges in Intelligent Computing Techniques (ICICT), pp.206-209, 2014.

[4] A. Compagno, M. Conti, P. Gasti, G. Tsudik, “Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking”, IEEE 38th Conference on Local Computer Networks, pp. 630-638, 2013.

[5] J. Francois, I. Aib, R. Boutaba, “FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks”, IEEE/ACM Transactions on Networking, vol. 20, no. 6, pp. 1828-1841, 2012.

[6] F. Soldo, K. Argyraki, A. Markopoulou, “Optimal Source-Based Filtering of Malicious Traffic”, IEEE/ACM Transactions on Networking, vol. 20, no. 2, pp. 381-395, 2012.

[7] K. Verma, H. Hasbullah, A. Kumar, “An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET”, IEEE 3rd International Advance Computing Conference (IACC), pp. 550-555, 2012.

[8] S. Khanna, S. S. Venkatesh, O. Fatemieh, F. Khan, C. A. Gunter, “Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks”, IEEE/ACM Transactions on Networking, vol. 20, no.3, pp. 715-728, 2011.

[9] L. Kavisankar, C. Chellappan, “A Mitigation model for TCP SYN flooding with IP Spoofing”, IEEE International Conference on Recent Trends in Information Technology (ICRTIT), pp. 251-256, 2011.

[10] J. Mirkovic, E. Kissel, “Comparative Evaluation of Spoofing Defenses”, IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 2, pp. 218-232, 2011.

[11] Y. Ma, “An Effective Method for Defense against IP Spoofing Attack”, IEEE International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), pp. 1-4, 2010.

[12] P. Du, A. Nakao, “Mantlet Trilogy: DDoS Defense Deployable with Innovative Anti-Spoofing, Attack Detection and Mitigation”, 19th International Conference on Computer Communications and Networks (ICCCN), pp. 1-7, 2010.

[13] B. KrishnaKumar, P. K. Kumar, R. Sukanesh, “Hop Count Based Packet Processing Approach to Counter DDoS Attacks”, IEEE International Conference on Recent Trends in Information, Telecommunication and Computing, pp. 271-273, 2010.

[14] “A Hash-based Path Identification Scheme for DDoS Attacks Defense”, IEEE 9th International G. Jin, F. Zhang, Y. Li, H. Zhang, J. Qian, Conference on Computer and Information Technology, pp. 219-224, 2009.

[15] M. Nagaratna, V. K. Prasad, S. T. Kumar, “Detecting and Preventing IP-spoofed DDoS Attacks by Encrypted Marking based Detection and Filtering (EMDAF)”, IEEE International Conference on Advances in Recent Technologies in Communication and Computing, pp. 753-755, 2009.

[16] Y. Xiang, W. Zhou, M. Guo, “Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks”, IEEE Transactions on Parallel and Distributed Systems, vol. 20, no. 4, pp. 567-580, 2009.

[17] B. R. Swain, B. Sahoo, “Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method”, IEEE International Advance Computing Conference (IACC), March pp. 1170-1172, 2009.

[18] I. B. Mopari, S. G. Pukale, M. L. Dhore, “Detection and Defense Against DDoS Attack with IP Spoofing”, International Conference on Computing, Communication and Networking (ICCCN), pp. 1-5, 2008.

[19] Y. Shen, J. Bi, J. Wu, Q. Liu, “A Two-Level Source Address Spoofing Prevention based on Automatic Signature and Verification Mechanism”, IEEE Symposium on Computers and Communications, pp. 392-397, 2008.

[20] Z. Duan, X. Yuan, J. Chandrashekar, “Controlling IP Spoofing through Interdomain Packet Filters”, IEEE Transactions on Dependable And Secure Computing, vol. 5, no. 1, pp. 22-36, 2008.