International Journal of Science Engineering and Advance Technology, IJSEAT, Vol. 4, Issue 9
ISSN 2321-6905
September -2016

International Journal of Science Engineering and Advance Technology

A Systematic Puzzle Approach of Deploying Software For Restricting Dos & DDOS Attacks

Gelli Naga Venkata Vinay Kumar[1], Md.Amanatulla[2]
[1]M.Tech (CSE), Nimra Institute Of Science & Technology, A.P., India.
[2]Associate Professor, Dept. of Computer Science & Engineering,
Nimra Institute Of Science & Technology, A.P., India.

Abstract — In the network denial of service (DoS) and distributed DoS (DDoS) attacks intend to prevent legitimate clients from accessing services are considered a serious hazard to the availability and reliability of the internet services. For example, server receives huge number of junk request from malicious client. For each request, server has to waste extra CPU time for completing process of SSL handshakes .Server cannot handle requests of services from its true customers because it may not have enough resources to handle the request. As a result of this attack is vanished businesses and reputation lost. Represented an advance mechanism that refers as the software puzzle, the aim of this mechanism is to prevent DoS or DDoS attacks and provide services to valid clients. The idea is quite simple. When a client wants to acquire a service from the server, client sends a simple request to the server. After getting the client request, the server sends one puzzle challenge to client. Client must first solve a complex structure puzzle correctly and submit it to the server for accessing services. Server verifies this puzzle solution, if it is correct then server agrees to establish connection with client. To solve this puzzle by every client, prevent vulnerable connection. A software puzzle is different kinds of methods or complex structure or problem which uses sequence of steps and solving these steps client can access resources. Timestamp, data length, key length and software puzzle complexity these attributes are used for security purpose in puzzle generation process and generates puzzle dynamically. I have used the SPEKE algorithm for key generation; it provides high level security and thwarts man-in-middle attack by password. Implement the RC7 algorithm for encryption purpose. It provides best result in case of throughput and time consumption and provides high level security .

Keywords — *Software Puzzle , Denial of Service(DoS), Distributed Denial Of Service (DDoS), Security, Encryption, RC7.*

1. INTRODUCTION

In general the transmission of packets uses a protocol such as TCP/IP. The makes themselves as harmful by viruses or any other torgen horse. This will cause the network server will be overload and may sometimes consumes the network resources. This will cause a DDoS Attack that user can obtain a services. These are the key concept that a DDoS occurs. Sometime the botnets will generate a legimate traffic to target server There are different types of method can DDoS will happen Such as bandwidth based attack, traffic based attack, UDP based attack, application based attack. Bandwidth-based attacks – This type of DDoS attack can send mass junk data to cause the server to be overloaded, leading to the consumption of network bandwidth or network equipment. Resource processed by firewall is also limited. Overload traffic leads to failure of network and reduce a quality of service. TRAFFIC-BASED ATTACKS : In this traffic based method the botnets send legimate traffic to target server, which causes a flooding attacks. The server cannot respond and cannot ale to handle a request causes DDoS.

APPLICATION-BASED ATTACKS: This type of attack sends specific data massages to application layers according specific feature. This done for some business specific attack which causes business performance.

UDP FLOOD: This DDoS attack, which causes unreachable packets. This leads to opening a port for large amount of time. This causes host to repeatedly checking and inaccessibility.

A Distributed Denial of Service attacks is implemented on the source of DoS attack and numerous dispersed attack sources. Usually, the attackers use a huge number of controlled bots dispersed in different locations to start on a great number of denial of service attacks to a lone target or several targets. With the quick growth of botnets in modern years, the attack traffic scale caused by Distributed Denial of Service attacks has been rising, with the target system, including not only industry servers, but also Internet infrastructures such as routers, firewalls and Domain Name Server systems as well as network bandwidth. The attack pressure sphere has also become broader. In computer network they use a protocol for called transmission control protocol .The packets are transferred through TCP. The attacker can send one or more attack packets to the network. This will cause the target servers and network resources and also overloads the server. These are the vital principles of Distributed Denial of Service attacks. The key reason is

inflexible avoidance of DDoS attacks deception in the combination up of justifiable traffic and illegitimate traffic. It is difficult to discover the attack packets from the diverse traffic in the avoidance progression, particularly when the harass message packets masquerade to be normal messages. For exemplar, in signature -based pattern corresponding Intrusion Detection system, it is not easy to differentiate illegitimate packets from legitimate messages packets.

2. RELATED WORK

The existing client puzzle scheme assume that the client solves the puzzle using legacy CPU resource only. But this is not always true. A malicious client may solve the puzzle using GPU (Graphic Processing Unit) component is almost a standard configuration in modern desktop computers, laptop computers, and even smartphones. In the proposed system it is possible to track the individual client behaviour through client's IP address.

Nonetheless, if IP tracking is effective to thwart the GPU inflation, IP filtering can be used to defence against DoS attacks directly without utilizing client data. In other words, their defence against GPU-inflated DoS attacks may not be attractive in practice. A new type of client data, called software puzzle, to defend against GPU-inflated DoS and DDoS attacks. Unlike the existing client data schemes which publish a puzzle function in advance, the software puzzle scheme dynamically generates the puzzle function P(•) in the form of a software core C upon receiving a client's request. Specifically, by extending DCG technology which produces machine instructions at runtime, the proposed scheme randomly chooses a set of basic functions, assembles them together into the data core C, constructs a software data C0 x with the data core C and a random challenge x.

If the server aims to defeat high-level attackers who are able to reverse-engineer software, it will obfuscate C0 x into an enhanced software puzzle. After receiving the software puzzle sent from the server, a client tries to solve the software puzzle on the host CPU, and replies to the server, as the conventional client data scheme does. However, a malicious client may attempt to offload the data task into its GPU. In this case, the malicious client has to translate the CPU software puzzle into its functionally equivalent GPU version because GPU and CPU have totally different instruction sets designed for different applications.

Note that this translation cannot be done in advance since the software puzzle is formed dynamically and randomly. As rewriting/translating a software puzzle is time-consuming, which may take even more time than solving the data on the host CPU directly;

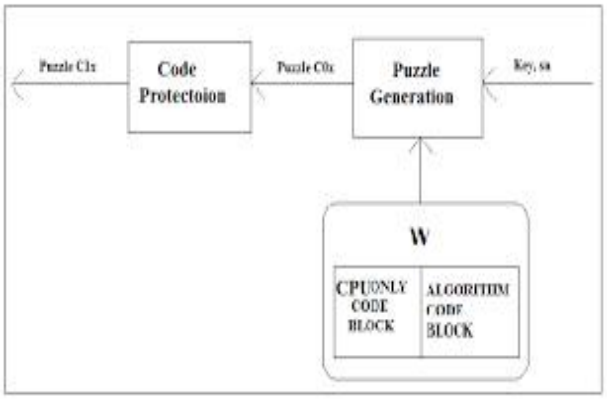

Fig. 1 Overview of System Architecture

3. PROPOSED METHODOLOGY

Software puzzle mechanism contain code block warehouse at the server side. This warehouse stores different types of software instruction blocks. Implementation is done in two parts that is first generate the puzzle C0x and provide high level security to C0x and generate secured puzzle C1x. Puzzles are generated using different mathematical operations with various attributes for security purpose. The goal of this work is to defense against DoS attacks and provide efficiency. First system architecture is presented and then working of each module is described. Figure 1 demonstrates that different steps. All compiled instruction blocks are stored in warehouse which is in java byte code format. This instruction blocks save server time otherwise server has to spend lot of time in converting source code into compiled code. In this warehouse, each block is depended on security parameter and size of each puzzle is in fixed size. If the block size is smaller then it provides more security level. Because of smaller block size attacker has to spend extra time to understand puzzle in question. In warehouse block structure, code block contain two categories: CPU code block and algorithm code block.

1. CPU code block: It contains all instruction set which is required in puzzle generation process. Which different activities are performed during puzzle generation process is presented in CPU code block.
2. Algorithm code block: It contains all operations related to encryption algorithm and stores all mathematical operations.
3. Code Protection: Provide code protection using code obfuscation technique. Code obfuscation means creating something which is lesser to clear and harder to understand. Here, for code protection RC7 algorithm is used.
4. Puzzle Solver: Here, puzzle solved by client is verified using puzzle solver to save the server time.

Puzzle solver is implemented at client side and it will allocate resources to the client if the client finds out correct puzzle solution.

RC7 Algorithm:
Input: Plaintext
Six w-bit input registers are "H, I, J, K, L and M".
R is a number of rounds
W indicates word size in bits.
r - Number of rounds.
W -bit round keys "C [0 . . . 2r+1]"
Output: Cipher text
Output stored in H, I, J, K, L, M.
Procedure: {
RC7 algorithm is a new extension of RC6 algorithm. As compared to RC6 algorithm RC7 has to takes less compilation time and encryption time.RC7 provides best performance as compared to other algorithm. RC7 algorithm is more flexible and provides efficiency in all application.

4. LITERATURE REVIEW

The paper "Effective approach towards intrusion Detection system using data mining technique" [1], In this paper DDoS attack is carried out by intrusion prevention system. The Intrusion Detection System (IDS) plays a vital role in detecting anomalies and attacks in the network. In this work the concept of data mining, this is to be integrated with IDS to identify the relevant, hidden data for the user effectively and with less execution time. In this approach they combine intrusion prevention system along with data mining concepts.

This paper "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks"[2],The FireCol which is an algorithm by which they detect DDoS attacks. The core of FireCol is composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. This detects flooding DDoS attacks as far as possible from the victim host and as close as possible to the attack source protection It maintains a virtual ring and it is composed of of intrusion prevention systems same distance from customer. Score manager which awards a score for according to traffic profile. According to threshold score it is marked as high potential and low potential attacks.

This paper "Flow level detection and filtering of low-rate DDoS"[3],In this approach flow level detection and filtering which detects and filters the low-rate DDoS attacks. It normally occurs in TCP congestion control mechanism. It causes a packet lose and timeout of user. It will not send traffic directly to the network. It will send traffic to the network at regular interval of time. The packets are monitored with threshold value and detect the attack.

The paper "Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts"[4], normally DDoS attacks are happen due to clock drift problem. This can be eliminated by using an algorithm called Hopping Period Alignment Adjustment algorithm. The vulnerability of DDoS attack can also be eliminated by this approach.

This paper "On a Mathematical Model for Low-Rate Shrew DDoS"[5], normally this low rate attack is done by attacker sending traffic at particular interval of time. By using a mathematical model, which estimate the effort of attack and may reduce the vulnerability and DDoS attacks.

5. CONCLUSION & FUTURE WORK

In implementation of different software puzzle methods against DDOS attack, software puzzle mechanism is provided to prevent DDoS attack. It reduces servers puzzle verification time by implementing software puzzle mechanism in advance. In this mechanism, puzzle solved by client is verified automatically at client side so no need to send puzzle solution at server side for verification. In existing system, puzzle solved by client sent at server side for verification due to server spent extra time for verification. Sometimes attacker was sending unsolved computation to server and server has to spend some time for verification. If for each verification server takes 2 minutes and an attacker sends 60 unsolved computation then server will take 120 minutes extra. In this system, three puzzle formation methods are used which are very important for DoS prevention. An attacker unable to solve puzzle because for solving puzzle human presence is required and an attacker is a tool which is not human. This system provides strong authentication, security and efficiency and prevents DoS attacks. Compared to existing system server served all client request so system will not fail due to number of bogus request. In future scope user can access multiple resources at a time within specific time period by solving only one puzzle.

REFERENCES

[1] Yongdong Wu, Zhigang Zhao, Feng Bao, and Robert H. Deng "Software Puzzle: A Countermeasure to Resource-Inflated Denial-ofService Attacks" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015.

[2] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time-lock puzzles and timed-release crypto," Dept. Comput. Sci. Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep. MIT/LCS/TR-684, Feb. 1996.

[3] A. Juels and J. Brainard, "Client puzzles: A cryptographic countermeasure against connection depletion attacks," in Proc. Netw. Distrib. Syst.Secur. Symp, 1999.

[4] T. J. McNevin, J.-M. Park, and R. Marchany, "pTCP: A client puzzle protocol for defending against resource exhaustion denial of service attacks," Virginia Tech Univ., Dept. Elect. Comput. Eng., Blacksburg, VA, USA, Tech. Rep. TR-ECE-04-10, Oct. 2004.

[5] W.-C. Feng and E. Kaiser, "The case for public work," in Proc. IEEE Global Internet Symp., May 2007, pp. 43–48.

[6] D. Keppel, S. J. Eggers, and R. R. Henry, "A case for runtime code generation," Dept. Comput. Sci. Eng., Univ. Washington, Seattle, WA, USA, Tech. Rep. CSE-91-11-04, 1991.

[7] E. Kaiser and W.-C. Feng, "mod_kaPoW: Mitigating DoS with transparent proof-of-work," in Proc. ACM CoNEXT Conf., 2007, p. 74.

[8] NVIDIA CUDA. (Apr. 4, 2012). NVIDIA CUDA C Programming Guide, Version 4.2. [Online]. Available: http://developer.download.nvidia.com/

[9] X. Wang and M. K. Reiter, "Mitigating bandwidth-exhaustion attacks using congestion puzzles," in Proc. 11th ACM Conf. Comput. Commun. Secur., 2004, pp. 257–267.

[10] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols," in Proc. IFIP TC6/TC11 Joint Working Conf. Secure Inf. Netw., Commun. Multimedia Secur., 1999, pp. 258–272.

[11] Y. I. Jerschow and M. Mauve, "Non-parallelizable and non-interactive client puzzles from modular square roots," in Proc. Int. Conf. Availability, Rel. Secur., Aug. 2011, pp. 135–142.

[12] J. Green, J. Juen, O. Fatemieh, R. Shankesi, D. Jin, and C. A. Gunter,"Reconstructing Hash Reversal based Proof of Work Schemes," in Proc. 4th USENIX Workshop Large-Scale Exploits Emergent Threats, 2011.

Mr. G.N.V VINAY KUMAR is a student of Nimra Institute of science and Technology, Jupudi, Nimra nagar , VIJAYAWADA. He is presently pursuing His M.Tech degree from JNTU, Kakinada. He has obtained B.Tech, degree from JNTU, Kakinada.

Mr. MD. Amanatulla is presently working as Associate professor in CSE department. Nimra Institute of Science and Technology, Jupudi, Nimra nagar , VIJAYAWADA. He has obtained M.C.A degree from JNTU, Kakinada and M.Tech, degree from JNTU, Kakinada. He has published several research papers in various national and international Journals.