ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Software Puzzle Counterstrike for Denial of Service Attack

Atul Rathod[1], Amogh Mahale[1], Ramprasad Makne[1], Sunil Pawar[1], Yogesh Magar[1], Prof. A.V.Almale[2]

B.E. Students, Dept. of Computer Engineering, JSPM'S BSIOTR, Wagholi, Pune, Maharashtra, India[1]

Asst. Professor, Dept. of Computer Engineering, JSPM'S BSIOTR, Wagholi, Pune, Maharashtra, India[2]

ABSTRACT: This paper reports on a project in which we propose a software puzzle scheme to deal with Denial of Service (DoS) attacks of certain types. When a client request comes in, the server generates a software puzzle for the client to solve. The algorithm is such that an attacker is unable to solve the puzzle in time. This approach looks promising based on the results presented and thus this paper is addressing the issue of network security. In this paper we study how to prevent DoS/DDoS attackers from inflating their puzzle-solving capabilities. To this end, we introduce a new client puzzle referred to as software puzzle. Unlike Existing user can already define puzzle scheme in that publish puzzle algorithms in advance and when client give request puzzle scheme generate puzzle randomly. 1) an attacker is unable to prepare an implementation to solve the puzzle in advance, and 2) the attacker needs considerable effort in translating a CPU (Central Processing Unit) puzzle software to its functionally equivalent GPU version such that the translation cannot be done in realtime. Moreover, we show how to implement software puzzle in the generic server-browser model.

KEYWORDS: Denial of Service attack, software puzzle, client puzzle, GPU programming.

I. INTRODUCTION

A Denial of Service (DoS) attack does not steal or damage the server but blocks or prevents access to the server or website. Such DoS attacks target the network bandwidth or connectivity. Such attacks floods the network degrading the service provided to a genuine user who is not able to send or receive response from server. The attacker consumes most or all of the resources of the computer and operating system. A counterstrike is an action or process that prevents or mitigates the effects of the attack. In this paper we report on a project we have implemented based on the ideas of Yongdong Wu, Zhigang Zhao [13] where a software puzzle based counterstrike is used to deal with DoS attacks. There are basically three Types of DOS attacks: Smurf, UDP flood and SYN flood attacks. Despite the significant varieties of attacks there is a common objective amongst all types of DoS attacks. The attackers aim to exhaust the resources of the system that includes CPU cycles, memory, disk space and network bandwidth. The attackers generate too many requests which is feasible since they pay very little or nothing to request a service. Often their cost is only of sending the request on the network. However the attack can vary significantly in many aspects including the target and protocol layer of the network, distribution of attack sources, the strategy employed and the impact. In this paper we propose cryptographic puzzles as a counterstroke on the attackers which brings a better balance to the computational load of the client and server. In a cryptographic puzzle scheme, a client is required to solve a cryptographic puzzle and submit the puzzle solution as proof of work before the server commits substantial resources to its request. The malicious client that does not follow the rules of the puzzle scheme. Requires moderate amount of cryptographic operations from the solver, and the amount of work required is guaranteed by the security of both the puzzle construction method and the cryptographic algorithm used. In most puzzle schemes, each puzzle requires an approximately fixed number of cryptographic operations, such as hashing, modular multiplication, or modular exponentiation, to compute the puzzle solution. Thus, the more an attacker wants to overwhelm the server, the more puzzles she has to compute, consequently the more computational resources of her own she needs to consume. The construction and verification of the puzzle are designed to be very efficient to avoid DoS on the puzzle scheme itself.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

II. RELATED WORK

Christos et.al presents a structural approach to the DDoS problem by developing a classification of DDoS attacksand DDoS defense mechanisms [1]. Furthermore, important features of each attack and defense system category are described and advantages and disadvantages of each proposed scheme are outlined. The goal of the paper is to givesome order into the existing attack and defense mechanisms, so that a better understanding of DDoS attacks can be achieved and subsequently more efficient and effective algorithms, techniques and procedures to combat these attacks may be developed.

Jeff Green et.al examines various such schemes in view of GPU-based attacks and identifies characteristicsthat allow defense mechanisms to withstand attacks[2]. In particular, they demonstrate hash-reversal schemes whichadapt solely on server load are ineffective under attack by GPU utilizing adversaries; whereas, hash reversal schemeswhich adapt based on client behavior are effective even under GPU based attacks.

Yves Igor et.al introduces a novel scheme for client puzzles which relies on the computation of square roots modulo a prime[3]. Modular square root puzzles are non-parallelizable, i.e., the solution cannot be obtained faster than scheduled by distributing the puzzle to multiple machines or CPU cores, and they can be employed both interactively and non-interactively. There puzzles provide polynomial granularity and compact solution and verification functions. Benchmark results demonstrate the feasibility of our approach to mitigate DoS attacks on hosts in 1 or even 10 GB it networks. In addition, they also show how to raise the efficiency of our puzzle scheme by introducing a bandwidth basedcost factor for the client.

Qiang Tang et.al have proposed such a security model and formally define two properties, namely the determinable difficulty property and the parallel computation resistance property[4]

III. PROPOSED ALGORITHM

We are proposing puzzle based scheme for DOS defence. In our proposed system, before engaging in any resource consuming operations, the server first generates a key to the client and a puzzle and then sends its description to the client that is requesting service from the server. The client has to solve the puzzle and send the result back to the server. The server continues with processing the request of the client, only if the client's response to the puzzle is correct.

A. *KEY GENERATION:*

When a client request service from the server initially server creates a key to the client using two different keys onepublic and one private. The public key can be shared with everyone, whereas the private key must be kept secret.

B. *PUZZLE SEEDS GENERATION:*

The puzzle seeds are a sequence of pseudo-random numbers generated by a server, which periodically releases anewseed to the overlay network. Also server estimates the time required to solve to the puzzle i.e., time lock puzzle. Requested client as to solve the puzzle within the estimated time.

C. *GENERATING AND SOLVING PUZZLES.*

After receiving the latest puzzle seed s, the client picks a random puzzle and tries to solve it. At this time severgenerates encryption for this sequence and use it as puzzle.

D. *ENCRYPTION USING AES:*

Cryptography is the art of implementing science for providing information and communication security. Cryptography produces secret codes for enabling the security for the data through communicating through an insecure channel. It protects the information from unauthorized parties by preventing unauthorized alteration of use.The encryption process consists of the combination of various classical techniques such as substitution, rearrangement and transformation encoding techniques. The encryption and decryption modules include the Key Expansion module which generates Key for all iterations. The modifications include the addition of an arithmetic operation and a route transposition cipher in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

the attacks iterative rounds. The Key expansion module is extended to double the number of iterative processing rounds in order to increase its immunity against unauthorized attacks

E. ***PUZZLE VERIFICATION.***

Upon receiving a connection setup request with a puzzle solution, an overlay node first verifies that the puzzleseed s contained in the request packet is one that has been recently released by the server. Server verifies the resultgenerated whether it is correct and decrypted within the time estimated .if so secure communication is established.

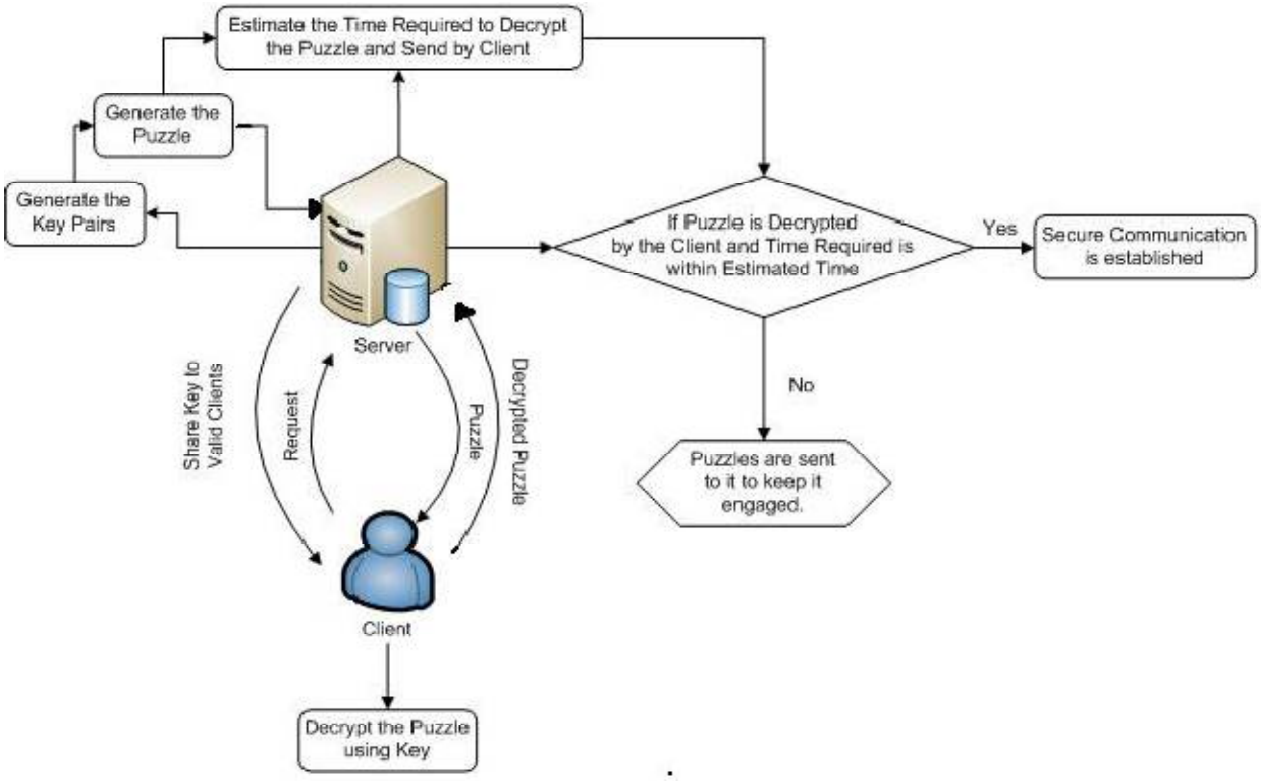

Fig. 1 System Architecture

F. ***FINDING ATTACKER NODE:***

Initially the key is generated only to the valid clients, and the puzzles must be solved within the estimated time.Using these two parameters we can find malicious client.

IV. CONCLUSION AND FUTURE WORK

We have presented the results of our project which aims to defend a server against Denial-of-Service attacks using a technique based on client puzzles. We developed a new model for puzzle distribution using a robust service and solutions to the puzzles allow clients to access communication channels. Here we also generate the key only for the valid clients and clients must solve the puzzle within the estimated time. Using these two we can find the spoofing node. This is shown by our experimental results.

REFERENCES

1. J. Larimer. (Oct. 28, 2014). *Pushdo SSL DDoS Attacks*. [Online]. Available: http://www.iss.net/threats/pushdoSSLDDoS.html
2. C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Comput. Netw.*, vol. 44, no. 5, pp. 643–666, 2004.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

3. A. Juels and J. Brainard, "Client puzzles: A cryptographic countermeasure against connection depletion attacks," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 1999, pp. 151–165.
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. R. Shankesi, O. Fatemieh, and C. A. Gunter, "Resource inflation threats to denial of service countermeasures," Dept. Comput. Sci., UIUC, Champaign, IL, USA, Tech. Rep., Oct. 2010. [Online]. Available: http://hdl.handle.net/2142/17372
5. 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.
6. 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.