Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.407 – 412

RESEARCH ARTICLE

Mitigating Risk Using Puzzle-Based Defense Technique to Improve Confidentiality

Ms. Sapna S. Khapre[1], Prof. Shrikant Ardhapurkar[2]
[1]M.Tech.-CSE, Smt. Bhagwati Chaturvedi College of Engg, Nagpur, Maharashtra, India
[2]CSE/IT Department, Smt. Bhagwati Chaturvedi College of Engg, Nagpur, Maharashtra, India

[1] sapnakhapre27@gmail.com; [2] shrikant.999@gmail.com

Abstract— A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. DoS attack is an attack that attempts to cause a failure in a computer system or other data processing entity by providing more input than the entity can process properly. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. To provide prevention against DoS attacks game theory is used. This is mainly owing to the several trade-offs existing in a flooding attack defense scenario. In this defense technique the resources can be used by legitimate users only by login with correct id and password and by solving puzzle correctly. The puzzle is generated randomly for each login. To improve the quality of service for legitimate user and also to improve confidentiality, puzzle based defense technique is used. With the help of puzzle based system we can avoid DoS attack.

I. INTRODUCTION

Availability of services in a networked system is a security concern that has received enormous attention in recent years. Most researches in this area are on designing and verifying defense mechanisms against denial-of-service (DoS) attacks. A DoS attack is characterized by a malicious behavior, which prevents the legitimate users of a network service from using that service. There are two principal classes of these attacks: flooding attacks and logic attacks.

A flooding attack such as SYN flood, Smurf, or TFN2K sends an overwhelming number of requests for a service offered by the victim. These requests deplete some key resources at the victim so that the legitimate users' requests for the same are denied. A resource may be the capacity of a buffer, CPU time to process requests, the available bandwidth of a communication channel, etc. The resources exhausted by a flooding attack revive when the attack flood stops. A logic attack such as Ping-of-Death or Teardrop forges a fatal message accepted and processed by the victim's vulnerable software and leads to resource exhaustion at the victim. Unlike flooding attacks, the effects of a logic attack remain after the attack until some appropriate remedial actions are adopted. A logic attack can be thwarted by examining the contents of messages received and discarding the unhealthy ones. This is due to the fact that an attack message differs from a legitimate one in contents. In flooding attacks, on the contrary, such a distinction is not possible. This causes defense against flooding attacks to be an arduous task. This paper will focus solely on flooding attacks.

In puzzle based defense mechanism, the server generates randomly three puzzles out of which the user have to solve one puzzle, the hint for solving which puzzle is given to only an authorized user who login correctly. After solving the puzzle by the user, the server verifies whether the puzzle is correct or not. If puzzle is correct then user can use resources, if puzzle is not correct then that user is prevented for using the resources.

A preventive mechanism enables the server to avoid the attack without denying the service to legitimate users. This is usually done by enforcing restrictive policies for resource consumption. A method for limiting resource consumption is the use of puzzles.

II. PUZZLE BASED DEFENSE STRATEGY SYSTEM

The CAPTCHA consists of a picture with some degraded or distorted image, which will take up a lot of valuable bandwidth especially in the case of the attack. In the case of DoS attack, sending those images from the server to the client for authentication actually consumes quite considerable bandwidth. The CAPTCHA is very easy to solve by opponent and it is not very secure. These mechanisms have not been designed through formal approaches and thereby some important design issues such as effectiveness and optimality have remained unresolved.

Puzzle based defense approach on other hand provide more security and difficult puzzles. It provide defense against DoS attack by allowing only authorized user in the system. The puzzle-based defense approach has three main components: Sender, Server and Receiver. Here we apply login and puzzle at sender side so that the authorized user can only transmit file or use resources, due to this there will limitation in resource consumption. In this approach the user who want to use resource first have login to system as shown in figure 1. User enters his login id and password then click on puzzle button. The server verifies the login id and password; if both are correct then only puzzle is generated. If any one entry is not correct then user can't access further.

Figure 1. Login Page

After successful login three puzzles generated with hint to solve which puzzle out of three as shown in figure 2.

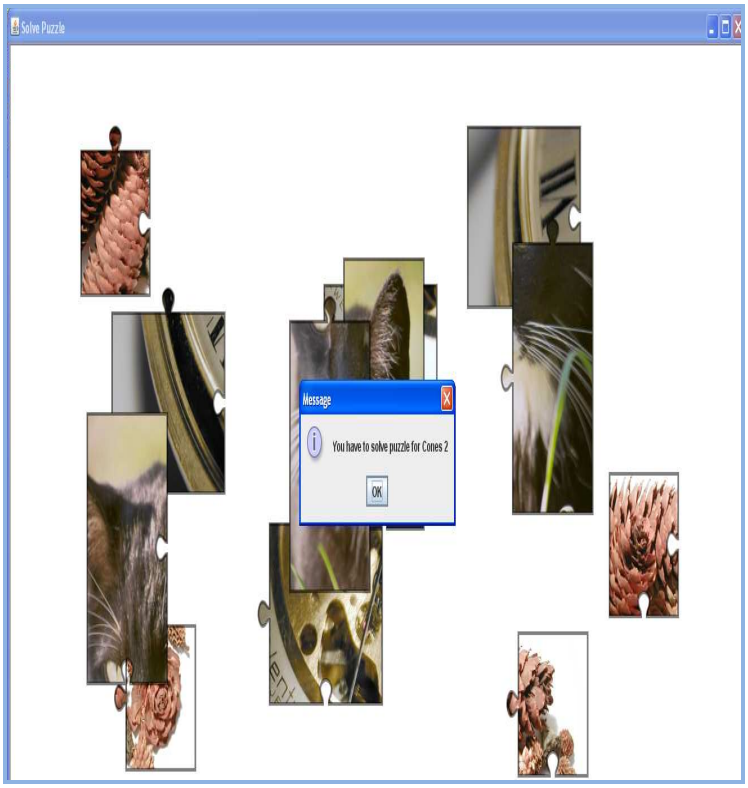

Figure 2. Puzzle

Each puzzle consist of four pieces, the user have to joint these pieces correctly. After solving puzzle correctly, the message box show message that puzzle is correctly solved. The server continues with processing the request of the user.

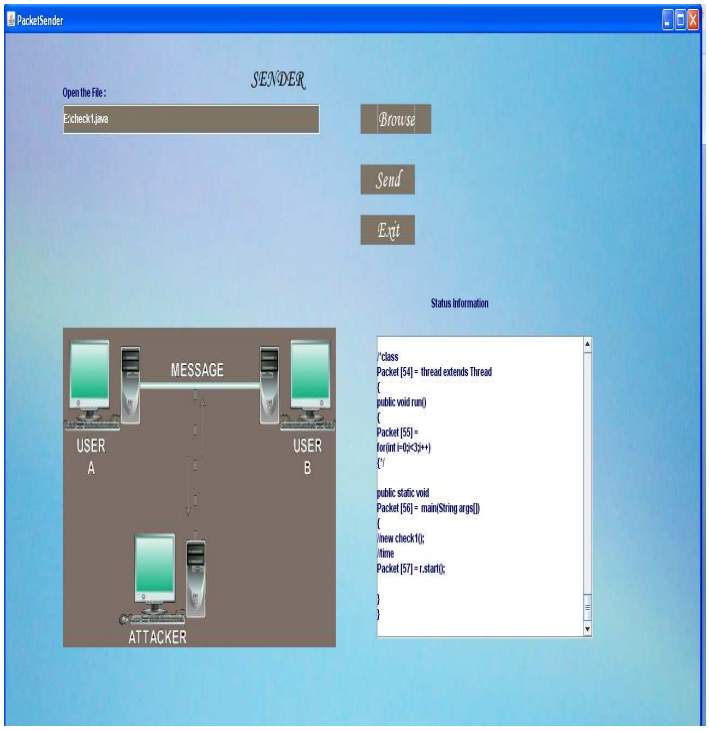

Figure 3. Sender

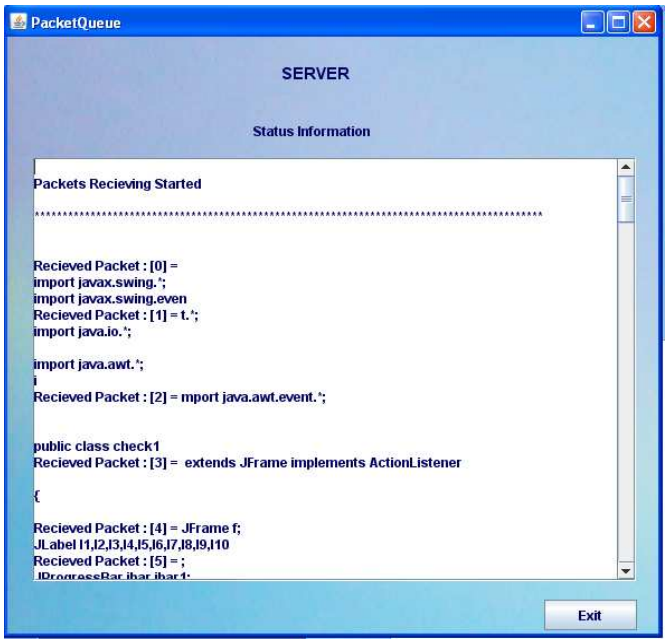

Figure 4. Server

Then user press submit button, after that *Sender* user interface will display which consist of *Browse* button for browsing files which user want to send as shown in figure 3. By pressing *Send* button user can send file, Server will show the status of sent file as shown in figure 4.The *Receiver* user interface will show the status of receiving file and also time taken to transmit that file as shown in figure 5.In this way puzzle-based defense approach provide defense against DoS attack as viruses cant login and can't solve puzzle.

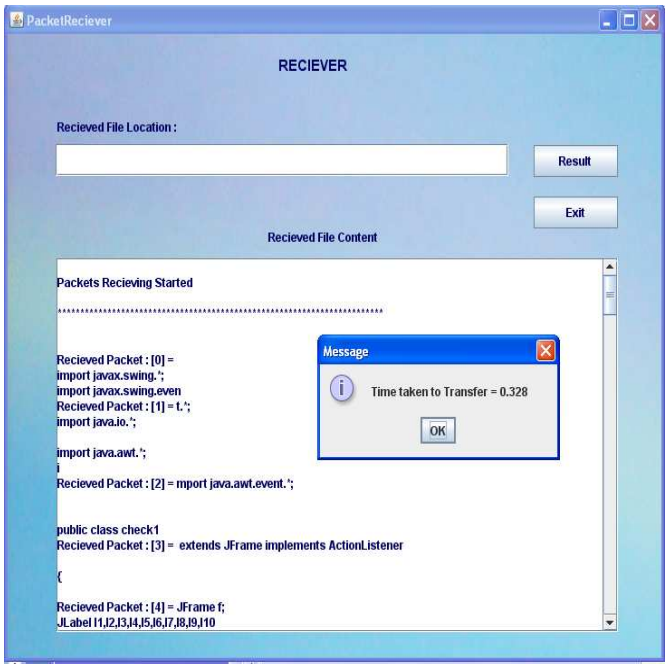

Figure 5. Receiver

III. OUTPUT

The figure 6 shows the output of transmitted file. It is generated by pressing *Result* button of *Receiver* user interface. It consists of transmission details like transfer time, transfer rate, total packet size, lost size etc. In this case the transmission time is 0.328 seconds, transfer rate 0.805Kbps, total packet size 2.691KB and lost size 0.047KB. The transmission time is less because server is free of DoS attacks due to which server provides quality of services to the authorized users and this happens because of puzzle-based defense approach.

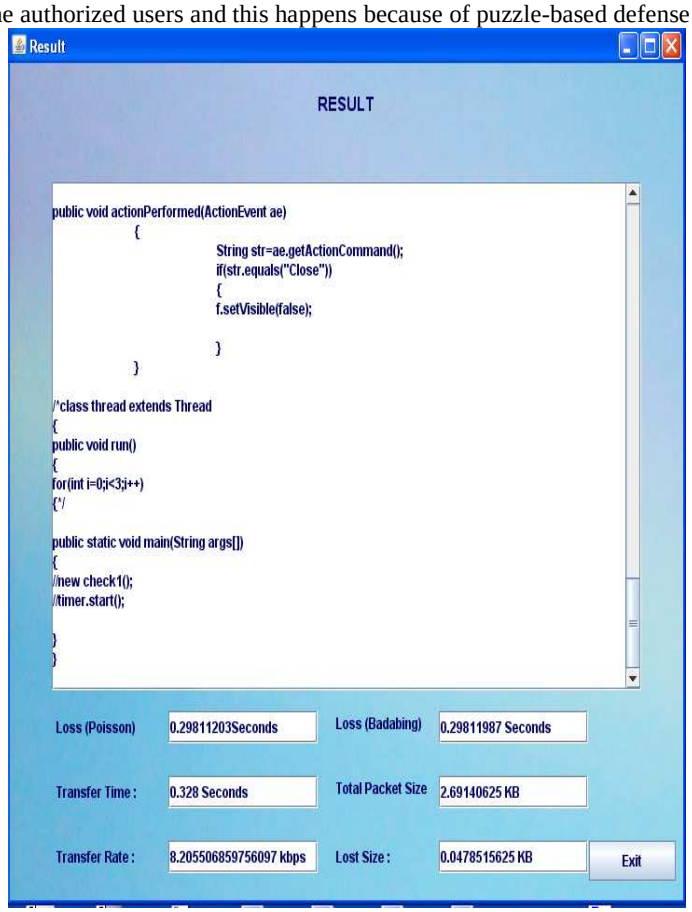

Figure 5. Result of transmitted file

If puzzle-based defense approach is not used then there are chances of DoS attacks due to which the resources get exhausts and there will be degradation in the performance of server and transmission time will be more.

IV. CONCLUSION

Puzzle-based defense mechanism provide defense against Denial of Service attacks. In Puzzle-based defense mechanism we provide login and puzzle mechanism so that authorized user can only use the resources. It shows the interaction between user and system. After successful login and correct solution to the puzzle, user can access resources provided by the system. Unauthorized can't solve puzzle because hint for solving the puzzle is given to the authorized users only. It provide defense against DoS attack by allowing only authorized user in the system. In this way the puzzle-based defense mechanism provide three level securities against DoS attack.

REFERENCES

[1] Kumar Dayanand and S. Magesh, "Defence Strategy against Flooding Attacks Using Nash Equilibrium Game Theory", International Conference on Computing and Control Engineering (ICCCE 2012), April 2012.

[2] Raju Neyyan, Ancy Paul, Mayank Deshwal and Amit Deshmukh, "Game Theory based Defense Mechanism against Flooding Attack using Puzzle", Emerging Trends in Computer Science and Information Technology, pg 5-10, no. 1, April 2012.

[3] Tanmay Sanjay Khirwadkar, "Defense Against Network Attacks Using Game Theory", University Of

Illinois At Urbana-Champaign, May 2011.

[4] Mehran S. Fallah, "A Puzzle-Based Defence Strategy Against Flooding Attacks Using Game Theory", IEEE transactions on dependable and secure computing, vol. 7, no. 1, pg 5-19, 2010.

[5] D. Moore, C. Shannon, D.J. Brown, G.M. Voelker, and S. Savage,"Inferring Internet Denial-of-Service Activity," ACM Trans.Computer Systems, vol. 24, no. 2, pp. 115-139, May 2006.

[6] Jelena Mirkovic, Janice Martin and Peter Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communication, Vol. 34, no. 2, pp. 39 – 53, April 2004.

[7] E. Bursztein and J. Goubalt-Larrecq, "A logical framework for evaluating network resilience against faults and attacks", Lecture Notes in Computer Science, Vol. 4846, 2007.

[8] T. Aura, P. Nikander, and J. Leiwo. "DoS-Resistant Authentication with Client Puzzles", Lecture Notes in Computer Science, vol. 2133, 2001.

