The Puzzle Based Defense Strategy Using Game Theory

Swati Patil[1], Kajal Gaikwad[2], Urvashi Battinwar[3,] Prof.Gunjan Jewani[4]

UG Student, Dept. of Computer Science and Engineering, Nagpur Institute of Technology, Mahurzari, Nagpur,

India[1,2,3]

Assistant Professor, Dept. of Computer Science and Engineering, Nagpur Institute of Technology, Mahurzari, Nagpur,

India[4]

ABSTRACT: Security issues have become a major issue in recent years due to the development of technology in networking. A number of puzzle-based defense strategies have been established to overcome the flooding denial-of-service(DoS) attack which is eminent in the networks. Hence in this paper we suggest a Game theory based strategy to create a series of Defence mechanisms using puzzles.

KEYWORDS: Denial of Service (DoS) Attack, Game Theory, Puzzles.

I.   INTRODUCTION

With the tremendous growth of network technology, network attackers are also rationally increased to disrupt the activities and hacking the data from the network users by the intruder. To provide the security from the intruder is most important one. Many researchers were proposed a different approach for providing security they does not tackle the problem, it leads an untruthful in the network.

This paper utilizes game theory to propose a series of optimal puzzle-based strategies for handling increasingly sophisticated flooding attack scenarios. In doing so, the solution concept of Nash equilibrium is used in a prescriptive way, where the defender takes his part in the solution as an optimum defense against rational attackers.

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.

II.   PROPOSED WORK

to resolve the abovementioned problems, our system has constructed with the client server based approach. the server has the monitoring and puzzle providing process. in this proposed system, a client node sends out a request message to server. the server will receive all details of the client. the system presents two methods to generate puzzles according to the network behavior purposes.

Step 1 *C → S:* sending service request
Step 2 *S:* generation of a puzzle
Step 3 *S → C:* sending description of the puzzle
Step 4 *C:* solving the puzzle
Step 5 *C → S:* sending solution to the puzzle
Step 6 *S:* verification of the solution
If the solution is correct:
Step 7 *S:* continue processing service request.
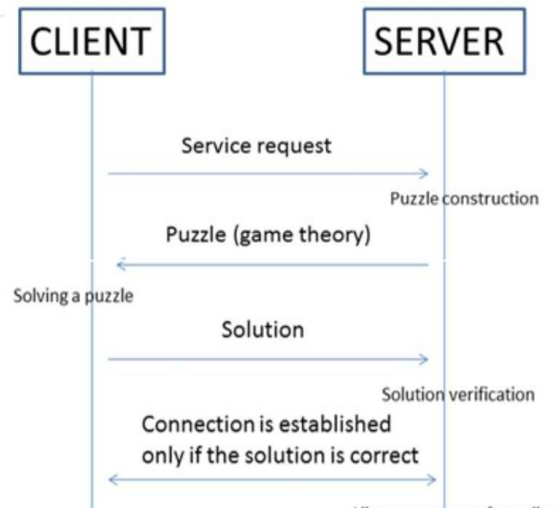
FIGURE 1: CLIENT PUZZLE APPROACH

III.   LITERATURE SURVEY

SR.NO.	TITLE	AUTHOR	APPROACHES
1.	A Defence Strategy against Flooding Attack Using Puzzles by Game Theory.	Ch. V. N. Madhuri, R. V. Krishnaiah.	In this paper, game theory has been used to provide defence mechanisms for flooding attacks using puzzles. Also the interaction between the defender and attacker is considered as an infinitely repeated game of discounted payoffs. The mechanism has been divided into different levels.
2.	Defence Strategy against Flooding Attacks Using Nash Equilibrium Game Theory.	Kumar Dayanand, S.Magesh.	In this paper, game theory has been used to provide defence mechanisms for flooding attacks using puzzles. This paper has also described the architecture of a client puzzle protocol. The algorithm selected for the client puzzle can be implemented on almost any platform.
3.	Game Theoretic Resistance to Denial of ServiceAttacks Using Hidden Difficulty Puzzles.	Harikrishna Narasimhan1,, Venkatanathan Varadarajan1,and C. Pandu Rangan.	This paper have given emphasis on hiding the difficulty of client puzzles from a denial of service attacker.Future direction of work would be to incorporate the proposed defense mechanisms in the Internet Key Exchange (IKE) protocol and to estimate its effectiveness in real-time.
4.	Game Based Analysis of Distributed DoS Attacks Prevention Using Puzzle-Based Defense Strategy.	Varsha Vishwanath, V.Shankar.	The paper showed how to employ game theory to intend a number of puzzle based defenses against flooding attacks. It is revealed that the connections between an attacker who initiates a flooding attack and a defender who counteracts the attack. The solution notions of this type of games are organized to discover the solutions.Like this, the finest puzzle-based defense strategies are developed.

IV.   PROPOSED METHODOLOGY

Our proposed system handling below said modules to achieve the security in the network.

(i)   Handling Client:

Clients are the users who will send the data to the receiver and they also can get the responses of their request from the server. Mainly clients are connected the data with their puzzle. The client phase contains three steps,
- Registration with the puzzle
- Login
- Connect the server

So that client can access the data by playing the correct method.

(ii) Server Responses:

Admin is the main controller of the network communication. Admin is just like the puzzle authority. Server is the databases which will responses to the client's request. According to the following rules the server will send response.
- Puzzle selection
- Request processing

The puzzle based service provider is used to provide the resource to the requested client. The client information detail is checked before providing resource to the requested client.

(iii) Game Theoretic settings:

The puzzle generation module is used to display the puzzle game. The puzzle game is displayed only when the user enters the details and clicks the puzzle button. Then the instructions are displayed to user for rearranging the puzzle. Similar the same operation about the previous function but in order to added the user register page. It has information about the registered user information. When the user connects the server, the server will provide a puzzle with default instructions. The users have to register with their personal data and selected puzzle are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

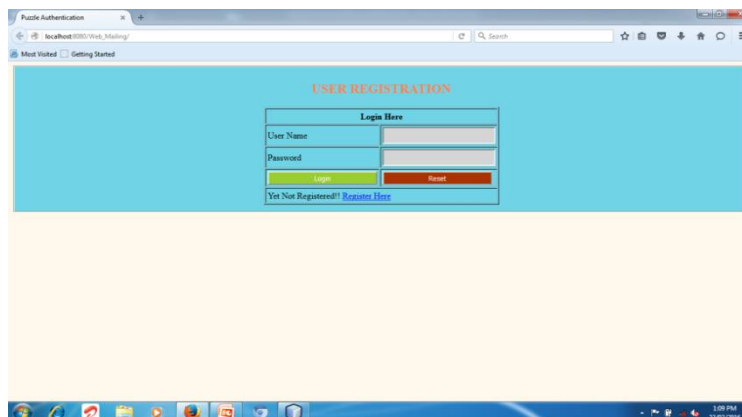## V.   SCREEN SHOTS

1.   Login Page

Fig1: Login Page

The above form shows the users login form. Using this form the user can login into the system using his user name and password. Different types of users use their particular username and password provided to login on the system.

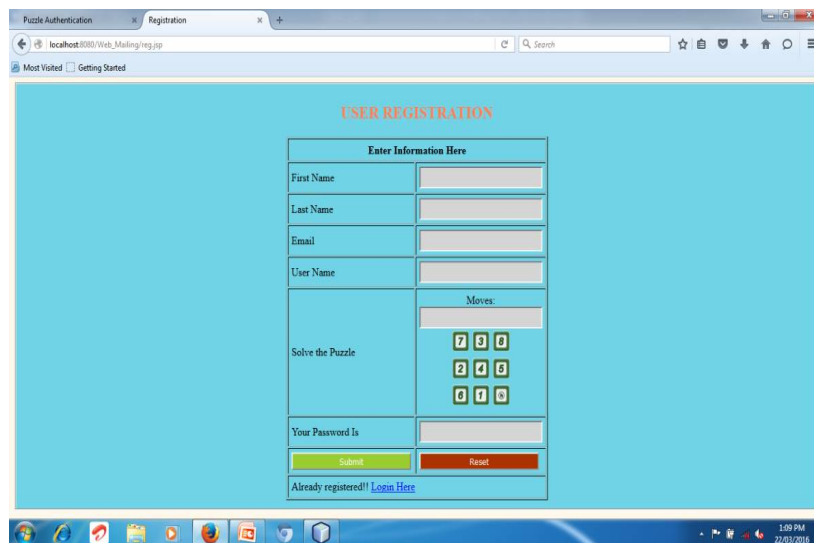### 2.   Registration page

Fig2: Registration Page

The above figure shows the registration form. Using this form the new user can create his new registration into the system. All the fields shown in the above form are compulsory to be filled. The user has to solve the puzzle from different types of direction provided for the server.
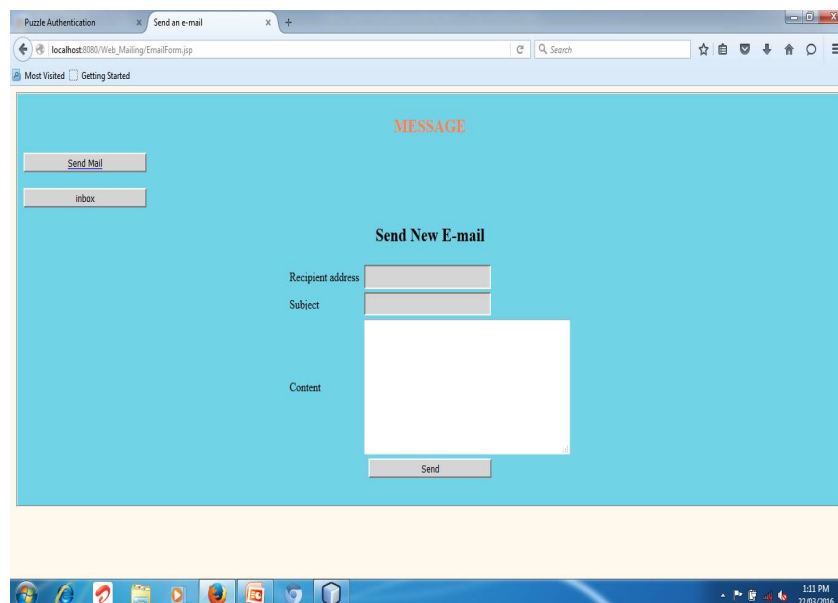
3.   Mail forwarding

Fig3: Mail forwarding

The above form shows the mail forwarding. Here the user can send mail to the receiver. The user can enter the recipients address. And system is provided facilities of subject, content and attach file an after send mail.
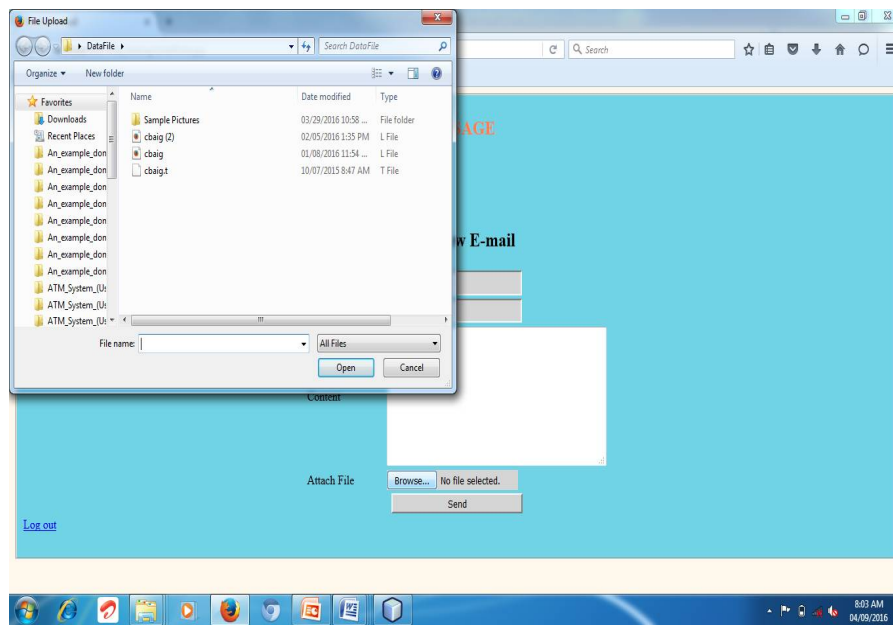
4.Attach file

Fig4: Attach file

The above form shows the attach file. The system is provided facilities of large information very easily form sender to receiver. The user can forward for text files, .img file, .doc file etc.
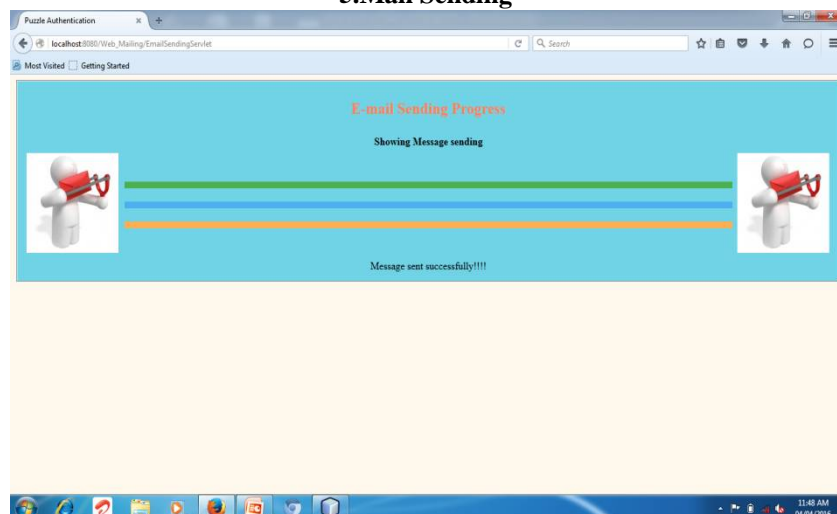
5.Mail Sending

Fig5: Mail sending

The above form shows the mail sending. The data is send for multiple paths. The information is send for divided form I n 3 ways. The user can view the information send by the graphically in this form.
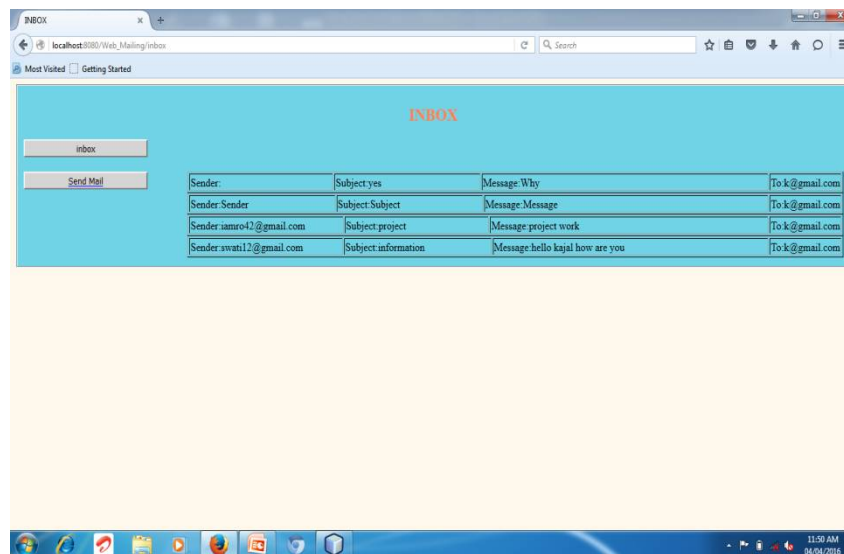
6.Inbox

Fig6: Inbox

The Above form shows, here the client can view the inbox of which will be all details saved in the database. The number of information can be seen by the client in this page.

VI.   ADVANTAGES

1.Effectiveness and optimality of this mechanisms have remained resolved.
2.Reactive mechanisms does not suffer from the scalability problem and difficulty of attack traffic identification.
3.Existing system is fully secure.

VII.   APPLICATION

- This proposed system used in Mailing.
- Proposed system handling increasingly sophisticated flooding attack than in existing.
- This system use in multiple organizations for sending crucial information securely.

VIII.   CONCLUSION AND FUTURE WORK

Normally conventional system we use maximum manual applications. It consumes lots of time and paper. But this system totally Web based, it means that customer can enter into the system very easily. This system is totally user friendly and time saving and cost effective system. All the modules are designed in a way that a can understand the system very easily. This system is designed in such a way that addition of new modules can be done in a very simple and efficient manner. Some likely enhancements could be added in the future to enhance the capability of this system. In this system puzzle theory provided the password in the registration time and user can login account on this password. The system totally secure from the puzzle password protection method. In future work it will be expanded to the other game theory.This system may used to provide authentication in cloud computing.It is securing the communication link between client and server with a puzzle mechanism.

REFERENCES

[1]. Ch. V. N. Madhuri, R. V. Krishnaiah,"A Defence Strategy against Flooding Attack Using Puzzles by Game Theory." International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 9, September 2013.

[2]. Kumar Dayanand, S.Magesh, "Defence Strategy against Flooding Attacks Using Nash Equilibrium Game Theory", ACS – International Journal in Computational Intelligence, Vol–4, Issue – 1 March 2013

[3]. Raju Neyyan , Ancy Paul, Mayank Deshwal ," Game Theory based defence mechanism against Flooding attack using Puzzle **",** *International Conference on Recent Advances and Future Trends in Information Technology (iRAFIT2012).*

[4]. Harikrishna Narasimhan1,, *Venkatanathan Varadarajan1,*and C. Pandu Rangan," Game Theoretic Resistance to Denial of ServiceAttacks Using Hidden Difficulty Puzzles**",** J. Kwak et al. (Eds.): ISPEC 2010, LNCS 6047, pp. 359–376, 2010.c Springer-Verlag Berlin Heidelberg 2010.