IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Survey on DDOS attacks on E-Banking Systems

Bhushan Bhonkar[1], Nishant Mehta[1], Rahul Gaikwad[1], Amit Kumar[1], Madhavi Darokar[2]

Bachelors in Engineering, Computer Engineering, JSPM's Imperial College of Engineering and Research, Pune India[1]

Professor, Computer Engineering, JSPM's Imperial College of Engineering and Research, Pune India[2]

Abstract: In the current world the most important threat to servers across the world is Denial of Service attack. DDOS attack often target web based services hosted on high profile servers such as banks or credit card payment gateways. A DDOS attack is analogous or similar to multiple groups of people crowding the entry door or a gate to a shop or business and not letting legitimatize parties enter into the shop or business disrupting normal operations. There is a distinct need of such an application to stop multiple attacks on the system. These attacks originate from a singular point of contact. Being DDOS creates a massive flood of users which can extensively break the system and stop its functioning. This survey paper constitutes in depth study of the problems seen by multiple banks and card based businesses. The major problem seen in banks and their response on the same is studied in depth to provide the required solution to these problems.

Keywords: DDOS, Multiple attack prevention, Banking application, SDN.

I. INTRODUCTION

Denial of service attack programs have been around for many years with growth of internet they have increased. A DDOS streams do not have common characteristics as the currently available intrusion detection system (ids). The aim of DDOS attacks is to make internet based services unavailable to its legitimate users. DDOS attacks is challenging for two reasons.

First, the number of attacks involved in DDOS attacks is very large. If the volume of traffic sent by single attacker is small then the victim host is overwhelming. Second, attacker usually spoofs IP address, which is difficult to trace. Three types of flooding attacks are accessed in it TCP/SYN, UDP & ICMP. TCP /SYN flood is a most dangerous of the DDOS attack.

UDP flood attacks are to exploit the UDP services. UDP packets to different port of a target in random way. ICMP is a smurf attack which is used to put the target resources out of service that results in making the resource stagnate. DDOS attacks network follows two types of architecture. The agent handler architecture and internal relay chat.

The agent–handler architecture for DDOS attack is comprised of clients, handler and agents. The attacker communicates with DDOS client system. The handlers are often software packages located through the internet that are used by client to communicate with the agent.

The system which is being built will help to stop multiple attacks using SDN based protocols.

The system will prevent multiple attacks like SQL injection, Brute force attack, URL injections and cross site scripting attack. Database will be encrypted to create a secure environment for the customers.

II. REVIEW OF RELATED LITERATURE

A. Internet based attacks

There are multiple types of attacks which can be faced by the server and there is a distinct need to stop these web attacks. Hacking using exploits is seen to be major creation or root of these attacks. Every single day there are new exploits which are found by which identity of the users is compromised. New web based attacks coming out every day causes business, community and individuals to take security seriously. These revelations teach everyone the importance of basic security concepts. Multiple books, articles are available on the websites. There need to be credible information on these attacks and how one can protect himself from these attacks.[1]

B. Conceptual framework

According to current trends as mentioned in the "Web site Hacked Trend Report Q2 2016" by Sucuri Security, we see multiple platform is affected like Wordpress, Joomla by malware and exploits. Wordpress experienced a 4% drop from 78% in Quarter 1 to 74% in Quarter2. Joomla experienced a 2.2% increase from 14% in Quarter1 to 16.1% in Quarter2. These analysis indicate increase in malware and viruses in multiple web based servers.

Identification of the attack is the primary focus of this project. The analysis indicate when the type of attack is known is become easier to stop and know exactly where this attack is coming from.

When the type of attack is known defences can be mounted to avoid data loss. There are multiple instances where attacks not detected in their early stages and thereby couldn't be stopped earlier. When attacks are not stopped quickly they tend to create damage and pose a greater threat to the system. Hence, there is a definite need for an application to stop the attack from ever occurring. [2]

DOI 10.17148/IJARCCE.2016.51111

III.RESEARCH METHODOLOGY

The methodology we used was to interact with the stakeholders who will use the application and test the same.

A. Interaction with banking personnel

To understand the exact requirement for banking based application we interacted with multiple employees of a private bank. Following are the generic requirement from these personnel:

1. Implementation of security based application where web attacks are quickly discovered and stopped.
2. Personal information of the client get stored into the database in encrypted format.
3. Dynamic password is created and pin is generated and sent to user on mail.
4. The administrator can check detailed logs of attacks for analysis and studying the same.

B. Active users

Multiple users based could use the application to quickly perform any banking or any financial task. Here quality and integrity of information is of paramount importance.[3]

IV. SYSTEM ARCHITECTURE

A. Basic architecture

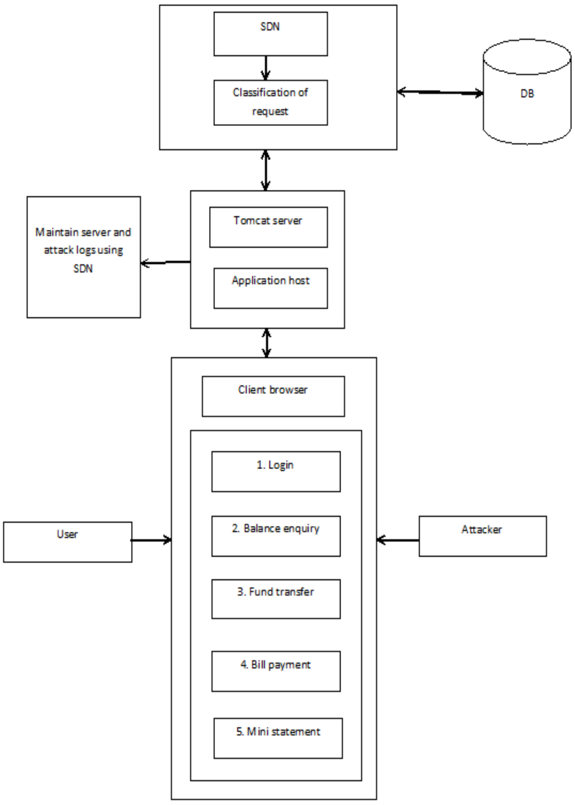

Fig.1 System Architecture

Fig. 1 shows us the basic functionality which will be attacked by the attacker and how SDN will help to stop this attack.

B. Activity Diagram

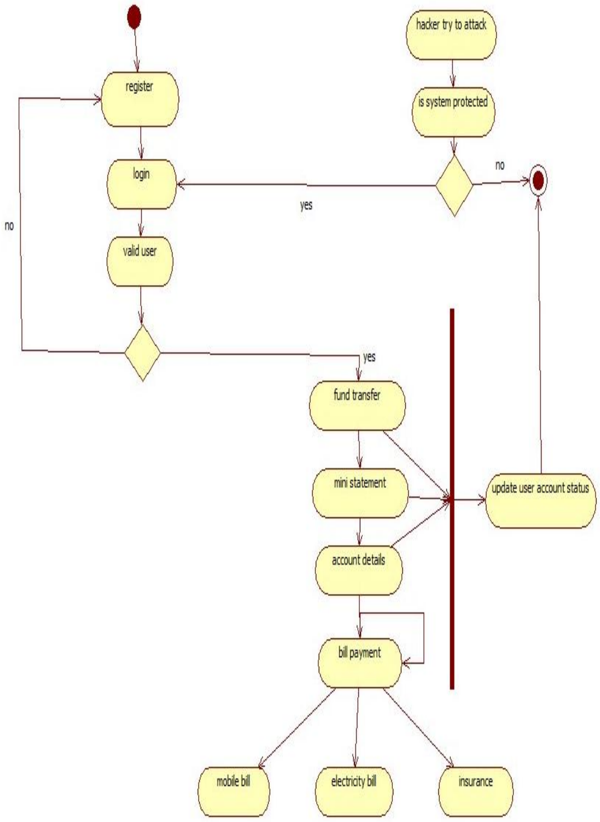

Fig.2 Activity Diagram

V. DISCUSSIONS

Every single banking application must be encrypted and secured for better usage. There is a requirement for such tools and applications to stop suspected attacks and give detailed log get how it happened. The overall result of the application to be built is cause root cause analysis and the better protection from such attacks. When implementation of such application is done quality based analysis creates a widened gap to affectively delivered important and system based information.

VI.CONCLUSION

Using this application we try to overcome multiple security problems and attacks which may lead to information and security leakages. A comprehensive work for protecting integrity of the information stored in the databases is a primary purpose for the application. Detection of multiple attacks will create a barrier for stealing or manipulating information in the system. Such a solution is an important breakthrough to effectively and efficiently stop the attacks.

ACKNOWLEDGEMENT

We thank our colleagues who provided insight an expertise that greatly assisted the research. We thank our mentor **Akash Bhojraj** for his guidance. We thank our **Prof. Madhavi Darokar** inspiring us to do this project and her comments in the manuscript.

REFERENCES

[1] https://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-shah.pdf

[2] https://sucuri.net/website-security/hacked-reports/Sucuri-Hacked-Website-Report-2016Q2.pdf

[3] https://securityintelligence.com/the-10-most-common-application-attacks-in-action/

[4] https://en.wikipedia.org/wiki/Software-defined_networking

[5] https://www.cs.northwestern.edu/~ychen/classes/msit458-w10/WebBasedAttacks.ppt

[6] Y. Zhang, "An adaptive flow counting method for anomaly detection in sdn," in Proceedings of the ninth ACM conference on Emerging networking experiments and technologies. ACM, 2013.

[7] "A covariance analysis model for ddos attack detection," in Communications, 2004 IEEE International Conference on IEEE, 2004, by S. Jin and D. S. Yeung

DOI 10.17148/IJARCCE.2016.51111