Journal of Information Security, 2014, 5, 123-135
Published Online July 2014 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2014.53012

Apple's Lion vs Microsoft's Windows 7: Comparing Built-In Protection against ICMP Flood Attacks

Rodolfo Baez Junior, Sanjeev Kumar

Network Security Research Lab, Department of Electrical and Computer Engineering, The University of Texas-Pan American, Edinburg, USA
Email: sjk@utpa.edu

Received 7 April 2014; revised 5 May 2014; accepted 1 June 2014

Abstract

With the increase in the number of computers connected to Internet, the number of Distributed Denial of Service (DDoS) attacks has also been increasing. A DDoS attack consumes the computing resources of a computer or a server, by degrading its computing performance or by preventing legitimate users from accessing its services. Recently, Operating Systems (OS) are increasingly deploying embedded DDoS prevention schemes to prevent computing exhaustion caused by such attacks. In this paper, we compare the effectiveness of two popular operating systems, namely the Apple's Lion and Microsoft's Windows 7, against DDoS attacks. We compare the computing performance of these operating systems under two ICMP based DDoS attacks. Since the role of the OS is to manage the computer or servers resources as efficiently as possible, in this paper we investigate which OS manages its computing resources more efficiently. In this paper, we evaluate and compare the built-in security of these two operating systems by using an iMac computer which is capable of running both Windows 7 and Lion. The DDoS attacks that are simulated for this paper are the ICMP Ping and Land Attack. For this experiment, we measure the exhaustion of the processors and the number of Echo Request and Echo Reply messages that were generated under varying attack loads for both the Ping and Land Attack. From our experiments, we found that both operating systems were able to survive the attacks however they reacted a bit differently under attack. The Operating System Lion was handling both the Ping and Land attack in the exactly the same way, whereas Windows 7 handled the two attacks a bit differently, resulting in different processor consumptions by two different operating systems.

Keywords

Denial of Service (DOS) Attack, Echo Request, Echo Reply, Internet Control Message Protocol (ICMP), Land Attack, Operating System (OS), Ping Attack

How to cite this paper: Baez Jr., R. and Kumar, S. (2014) Apple's Lion vs Microsoft's Windows 7: Comparing Built-In Protection against ICMP Flood Attacks. *Journal of Information Security*, **5**, 123-135. http://dx.doi.org/10.4236/jis.2014.53012

1. Introduction

A Denial-of-Service (DoS) attack is considered an active attack, which attempts to make a computer or network resource unavailable to its intended users. DoS attacks exhaust the computing or communication resources of the victim's computer or server. An increasing number of DDoS attacks happen regularly and have also been used against governments around the world [1]-[3]. This was the case on January 5, 2013 when the US Department of Justice, FBI, and some music.

Corporation had their websites attacked. The attack that was used was a DDoS attack. These days a computer system that are connected on Internet can be used as a BotNet to indirectly aid in DDoS attacks, or itself become a victim of DDoS attacks, where an attacker is intent on disrupting its services or computing performance.

Mac OS X Lion (version 10.7; marketed as OS X Lion) is the eighth major release of Mac Operating system for Apple's desktop and servers [4]. Apple reported over one million Lion sales on the first day of its release [5]. As of October 2011, Mac OS X Lion has sold over six million copies worldwide. According to Apple Inc., it claims that an iMac computer running the latest OS X is reliable, more powerful, and safer than any other computer on the market [6].

Windows 7 is an operating system developed by Microsoft for personal computers, considered to be a major improvement over its predecessors due to increased performance. Windows 7 was a major success for Microsoft, which became generally available on October 22, 2009 [6] [7]. In just six months, over 100 million copies were sold worldwide, and by July 2012 more than 630 million copies were sold.

In order to evaluate security offered against DDoS attacks, we used Apple's iMac platform capable of running Microsoft's Windows 7 and its own Lion OS. The ICMP based Ping and Land Attacks were used to launch DDoS attacks on these two operating systems running on the same hardware platform *i.e.* Apple's iMac platform. ICMP attacks are one of the common DDoS attacks, which intend to exhaust a victim computer's computing resources by sending a flood of ICMP Echo Requests.

Since today's operating systems are deploying built-in attack prevention mechanisms of their own, we intend to evaluate the performance of these two very successful operating systems by deploying them on the same hardware platform *i.e.* iMac computer platform. This will allow us to compare which operating system was more resilient, handled DDoS attacks more efficiently on their own (*i.e.* without external security systems) and managed processor resources more efficiently.

This paper is organized as follows: Section 2 gives some background about the ICMP based Ping and Land attack that were used in experiments presented in this paper. Section 3 provides the information about our experimental setup. Section 4 is about results and discussions. Section 5 presents the conclusion.

2. Background

Internet Control Message Protocol (ICMP) is a layer 3 message protocol that is divided into error-reporting and query messages. The error-reporting messages are used to report any problems in the network like delivery error. While the query messages are used to get specific information from a router or host in the network.

ICMP is defined by RFC 792 [9]. The ICMP packet format is made up of an 8-byte header and a variable-size data section. The general format of the header is different for each ICMP message; however, the first 4 bytes are common to all. These are the TYPE, CODE, and CHECKSUM fields. Depending on how these fields are set will determine which ICMP message is being used. **Figure 1** shows the packet format for an echo request/reply message. For instance, the ICMP Echo Request message, the TYPE field is set to 8 and the CODE field is set to 0.

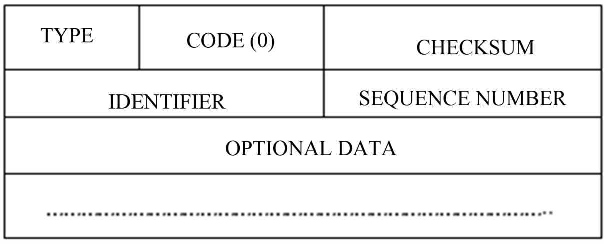


Figure 1. ICMP echo request/reply header format.

2.1. Ping Flood Attack

ICMP Ping is a type of diagnostic message used by a user to verify the end-to-end path of a host on a network. It relies on the ICMP Echo Request and Echo Reply messages to accomplish this. According to RFC 1122, every computer is required to implement an ICMP Echo server function which receives Echo Requests and sends corresponding Echo Replies [10]. Accordingly, when a computer receives an ICMP Echo Request message it responds with an ICMP Echo Reply message. In a DDoS attack scenario, the attacker abuses this protocol and floods the victim computer with echo request messages, which are actually sent from multiple computers in its BotNet. When this is done in a Cyber warfare, it is considered a Ping Flood attack. There are two methods commonly used to prevent this type of attack—First, to completely disable ICMP from entrusted sources, and second is to monitor and regulate the rate of transmission of ICMP requests and resulting replies to mitigate the degrading effect of such attacks on the computer system.

2.2. ICMP Based Land Attack

In an ICMP based Land attack, the attacker uses the ICMP Echo Request message just like in a Ping Flood attack mentioned above, however the difference is that the destination and source IP addresses are kept the same as that of the victim's computer. In doing so, such a modified Ping message when sent to a victim computer causes the victim computer to reply to itself for every echo request that it receives. Just like in the Ping Flood attack, the flood of modified Ping messages will cause the victim computer to significantly use up the processor resource besides the bandwidth. **Figure 2** shows how a land attack works. Since the source and destination addresses are the same as that of the victim, both the echo request and echo reply messages are sent to the victim computer, which is intended to exhaust the computing resource of the victim computer a bit faster.

In this experimental paper, we simulate the real attack scenario in a controlled environment of a lab to find out how the built-in prevention mechanisms (if any) of these two popular operating systems from Apple computers and Microsoft perform under these two ICMP based attacks on their own (which means without the use of external prevention systems typically used in a network).

3. Experimental Setup

In a controlled lab environment of the Network Security Research Lab (NRL) at The University of Texas-Pan American, the performance of two different Operating Systems were evaluated under ICMP based Ping and Land attack traffic up to a maximum load of 1 Giga bit per sec (Gbps). Low attack loads were sent in Kbps but not exceeding 100 Mbps, where as the high attack loads were sent in the range of 100 Mbps up to 1 Gbps for an equal duration. A Linksys SRW2024 24-port Gigabit Ethernet switch and CAT6 Ethernet cables were used to create the network for the experiment. The experimental setup used in the lab is shown in **Figure 3**.

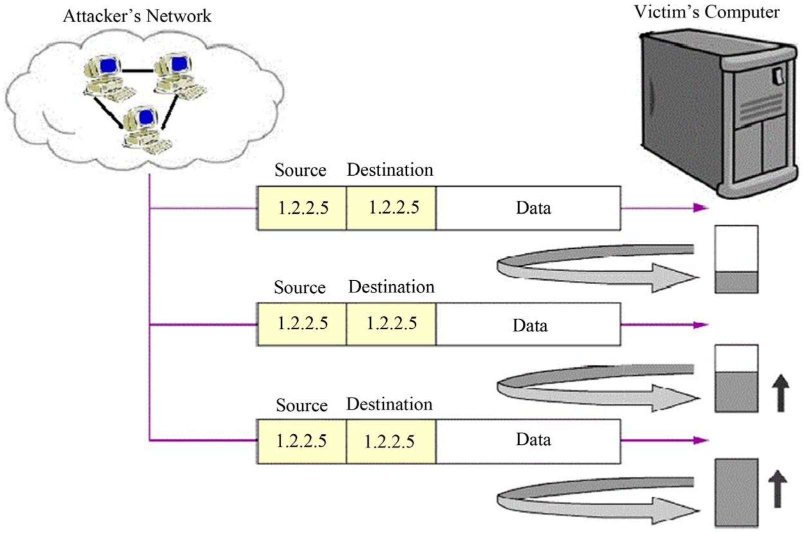


Figure 2. ICMP based Land attack.

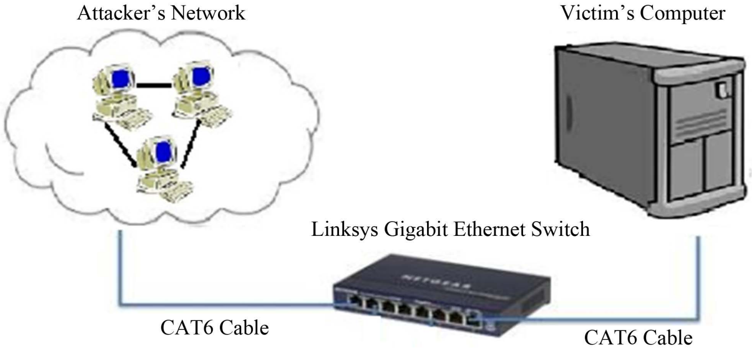


Figure 3. Experimental set-up.

The victim computer used in the lab experiment was an Apple iMac hardware platform, which came equipped with an Intel Core i5 2.5-GHz quad-core processor and 8 GBytes of RAM. The network interface card was a Broadcom NetXtreme Gigabit Ethernet adapter and both Apple's OS X 10.7.4 Lion and Microsoft Windows 7 were available for installation on it. The experimental set up and the test configurations used were similar to the ones used in [11]-[14], but with the newer operating system *i.e.* Apple's Lion compared with Microsoft's Windows 7.

4. Experimental Results

The two Operating Systems *i.e.* Apple's Lion and Microsoft's Windows 7 were subjected to Cyber warfare scenario where different ICMP attack loads were used—(a) Low attack loads were defined as attack traffic used in Kbps (not to exceed 100 Mbps), and load was incremented by 10 Kbps, (b) High attack loads were defined as attack traffic used in the range of 100 Mbps up to 1 Gbps (1000 Mbps), and the load was incremented by 100 Mbps.

In this paper, we consider two cases. Case-1 compared the resilience of both OS against the ICMP Ping Flood attacks. Case-2 compared the resilience of both OS against the ICMP based Land attacks.

Case 1: *Ping Flood Attacks—Comparing performance of the two operating systems against the ICMP Ping Flood attacks*

For Ping Flood attack, we first investigate how these two popular operating systems are able to handle ICMP flood attacks under conditions of the same hardware resources and same attack loads. We measure the number of Echo Requests that were received and Echo Reply messages that were sent out (as a response) by the two operating systems when faced with Ping Flood attack of varying loads. We also compared the respective processor exhaustion of the victim computer caused by the Ping Flood attack when running these two different operating systems. We evaluate performance of the two operating systems under varying attack loads and are given below.

1) Apple's lion operating system under low attack loads of ping flood attack

In our experiments, we first send ping flood attack of lower load (in Kbps) to Apple's Lion operating system.

For Apple's Lion, we observed that it would reply to every echo request message that was received up to the attack load of 180 Kbps (**Figure 4**). However, when the load exceeded 180 Kbps, it would not reply to all ICMP request messages, but only send out maximum of 250 echo reply messages per second. The load of 180 Kbps seemed to be the threshold exceeding which maximum number of echo reply messages that Apple's Lion would send is limited to 250 echo replies per second for the remainder of attack period.

This shows that the Apple's Lion operating system starts limiting the number of echo reply messages sent per second in order to ward off the adverse effect of Ping-flood attacks.

2) Apple's lion operating system under high attack loads (in the range of 100 Mbps to 1 Gbps) of Ping Flood attack

We observed the ICMP echo request and echo reply messages as recorded by the Apple's Lion operating system (**Table 1**). The maximum echo request messages that were received and recorded by Apple's Lion OS under high attack loads were limited to around 394,000/sec (**Table 1**). Response of Apple's Lion OS to the flood of Ping messages was also observed. We observed that the maximum number of echo reply messages that were sent out by the Apple's Lion OS in response to the incoming Ping flood were 250 echo reply messages per

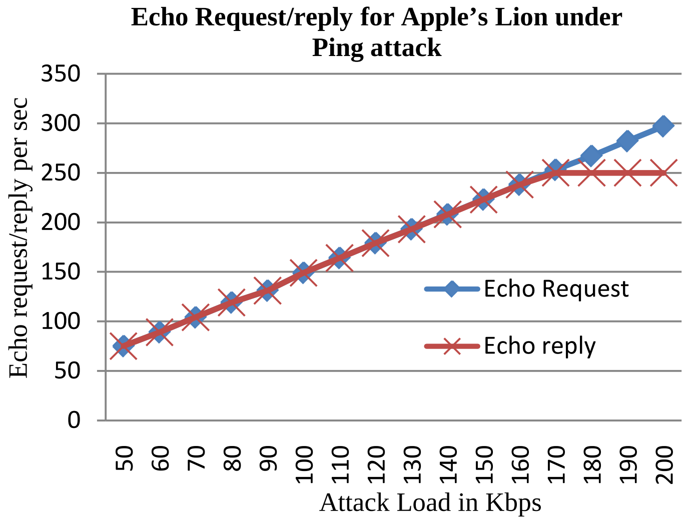


Figure 4. Same behavior observed for echo request/reply for Apples Lion OS under ICMP Ping Flood, and ICMP Land attacks.

Table 1. Echo reply produced by Apple's Lion OS for high loads of Ping Flood attacks.

Echo Requests/Reply for Apple's Lion OS under Ping Flood Attack		
Attack load in Mbps	Echo request/sec	Echo reply/sec
0	0	0
100	148,809/sec	250/sec
200	297,619/sec	250/sec
300	393,412/sec	250/sec
400	393,367/sec	250/sec
500	393,879/sec	250/sec
600	393,117/sec	250/sec
700	393,536/sec	250/sec
800	393,600/sec	250/sec
900	393,606/sec	250/sec
1000	393,490/sec	250/sec

second, irrespective of the number of echo request messages that were received by it at high load. This shows that upon exceeding a threshold on the rate of received Ping requests, Apple's Lion OS was rate limiting the response to those ping request messages to mitigate the adverse effect of such attacks on its computing resources.

3) Microsoft's Windows 7 under low loads (below 100 Mbps) of Ping Flood attacks

To understand the behavior of Windows 7 operating system, we sent low loads of ping flood attacks comprising of ICMP echo request messages. It was observed (**Figure 5**) that up to the flood load of 10.7 Mbps, the Windows 7 replied (by sending out ping reply messages) to all 15,845 echo request messages that were received. When the ping flood load was increased to 10.8 Mbps then it received 16,018 echo request messages, and the Windows 7 didn't reply to all ping requests this time. It only sent out a fixed number *i.e.* 500 echo replies for the 1st second and didn't respond (*i.e.* no echo replies were sent out) for the remainder of the attack period. Hence exceeding a certain threshold for the incoming ping flood, the Windows 7 started rate limiting the echo replies produced in response to the ping flood attack, which helped contain the exhaustion of the CPU resources.

It was observed that the processor resource was consumed up to 14% as the load of the ping flood increased

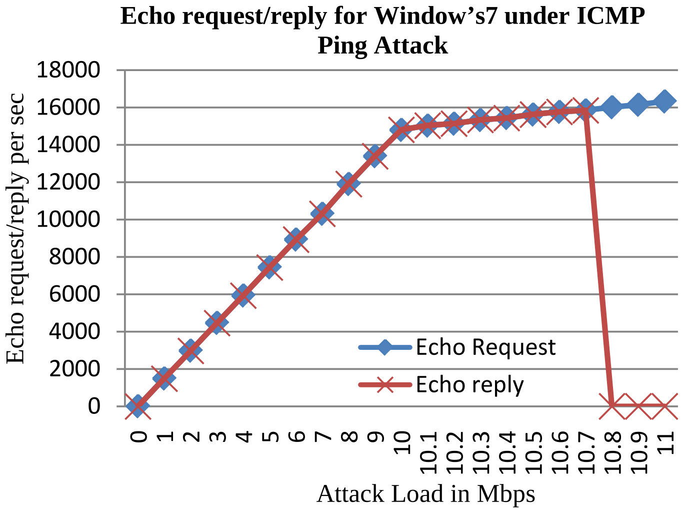


Figure 5. Echo request/reply for Microsoft's Windows 7 OS under low loads of ICMP Ping Flood attacks.

to 10.8 Mbps; however when we increased the load of ping flood beyond this threshold of 10.8 Mbps than the processor resource rather decreased to 6% (**Figure 6**). This is mainly because the Windows 7 started rate limiting the echo-replies and did not respond to all ICMP echo request messages when it crossed a threshold of 10.8 Mbps. This rate limiting helped contain the exhaustion of the processor resource and it can be seen to drop from 14% CPU consumption to 6% CPU consumption (**Figure 6**).

4) Microsoft Windows 7 under high attack loads of Ping flood (above 100 Mbps)

For Microsoft's Windows 7 operating system under high attack loads (in the range of 100 Mbps to 1 Gbps), we observed the echo request and echo reply messages as recorded by the Windows 7 operating system. The maximum number of echo request messages that were received by Windows 7 OS under high attack loads was around 697,000/sec (**Table 2**). In response to the high load of ping flood messages (after exceeding the threshold of 10.8 Mbps, as discussed in the previous section), it was observed that the Windows 7 OS sent out 500 echo reply messages only for the 1st second of the attack. Thereafter it didn't send out any more echo reply messages for the remainder of the attack period (as long the attack load exceeded the threshold). This was not the case for Apple's Lion OS where it was found to be sending 250 echo reply messages every second for the entire attack period even after exceeding the attack threshold.

5) Comparing processor exhaustion due to high loads of ping flood attacks under the two operating systems

It is observed (**Figure 7**) that the iMac platform with Apple's Lion operating system experienced a higher CPU exhaustion (max 31%), when compared with CPU exhaustion of the same iMac computing platform with Microsoft's Windows 7 operating system (max 18%) for a given attack load.

As was previously mentioned, Apple's Lion was sending out 250 echo reply messages every second even after exceeding the threshold of incoming echo request messages, whereas the Microsoft's Windows 7 operating system sent out 500 echo reply messages only in the 1st second and none in the following seconds when the threshold of incoming echo request messages was exceeded. This gave us an understanding as to why the exhaustion of the processors was higher with Apple's Lion operating system when compared to that under Windows 7 operating system (**Figure 7**) for high loads of Ping attacks. We also observed that the exhaustion of the iMac processors when running it native Lion OS was at its maximum (30%) under the relatively low attack load of 200 Mbps. This was not the case when the iMac desktop was running Microsoft's Windows 7. Windows 7 was only using 9% of the CPU to process the attack load of 200 Mbps. It was not until the attack load of 500 Mbps that Windows 7 reached its maximum exhaustion of the processor (~18%). However, as the speed of the attack increased, the exhaustion of the processor under Windows 7 was decreasing. We believe this was because Windows 7 seemed to register lower number of echo request messages after 500 Mbps of attack loads. Even though it seemed that Apple's Lion was limiting the incoming echo request messages more efficiently (**Table 1**), the exhaustion of the processors was still higher than that under Windows 7. This was mainly because it was

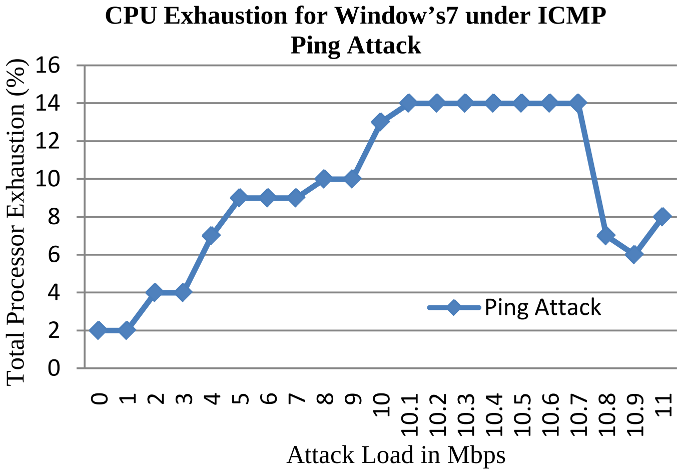


Figure 6. CPU exhaustion for Microsoft's Windows 7 OS under low loads of ICMP Ping Flood attacks.

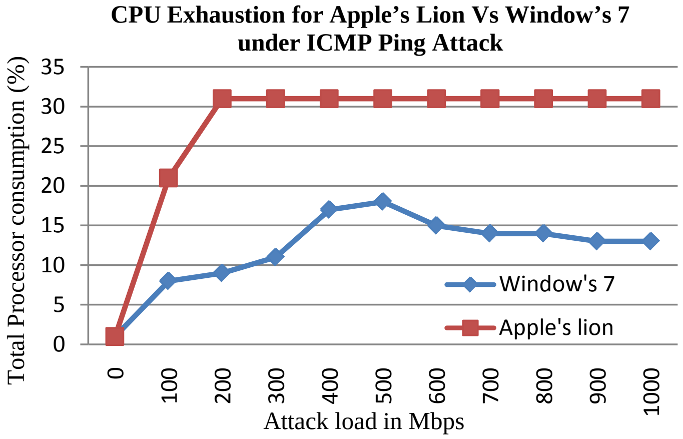


Figure 7. CPU exhaustion of Apple's Lion vs. Windows 7 under ICMP Ping Flood attack.

Table 2. Echo request/reply produced by Windows 7 OS.

Echo Request/Reply for Windows 7 under Ping Flood Attack		
Attack load in Mbps	Echo request/sec	Echo reply
0	0	0
100	148,807/sec	Max: 500
200	297,616/sec	Max: 500
300	446,422/sec	Max: 500
400	578,630/sec	Max: 500
500	697,032/sec	Max: 500
600	583,926/sec	Max: 500
700	579,121/sec	Max: 500
800	579,679/sec	Max: 500
900	593,956/sec	Max : 500
1000	582,908/sec	Max: 500

responding to ping requests even after crossing the attack threshold.

Case 2: *ICMP based Land Attack—Comparing performance of the two operating systems against the ICMP Land attacks*

In the case of the ICMP Land attack, the ICMP request and reply messages both are sent to the victim computer, we expected that both operating systems would use up most of the computer's memory in processing the echo request and echo reply messages, as was the case with Apple's Leopard and Windows Vista [13]. However, our results were a bit different.

1) Apple's lion operating system under low attack loads of ICMP Land attack

Our experiments showed that the Apple's Lion did not treat the ICMP Land attack any different than the ICMP Ping attack messages. This is why identical results (as in **Figure 4** and **Table 1**) were obtained for the performance of Apple's Lion when under ICMP Land attacks.

2) Apple's lion operating system under high attack loads (in the range of 100 Mbps to 1 Gbps) of ICMP Land attack

Since the Ping attack and ICMP based Land attacks are both based on ICMP ping request messages sent to the victim computer, the Apple's operating system seemed to treat the ICMP based Land attack similar to the Ping attack.

Table 3 shows the reaction of the Apple's Lion OS when encountering a wave of ICMP Land attack traffic, and the measurement is same as that in the earlier **Table 1**. From **Table 3**, it can be seen that the Apple's Lion OS sends out 250 echo replies each second even though the threshold is crossed and replies are sent out to itself.

The CPU exhaustion was found to be the same for ICMP Land and Ping Flood attacks (**Figure 8**). Apple's Lion OS could not distinguish one from the other. We can say this due to the fact that Apple's Lion OS had exactly the same performance characteristics under both attacks. The echo request and echo reply messages handled by the Apple's Lion OS can be viewed in **Table 3**, whereas the CPU exhaustion can be seen in **Figure 8**.

3) Microsoft's Windows 7 under low loads (below 100 Mbps) of ICMP based Land attacks

We investigate the handling of low loads of ICMP based Land attacks by Windows 7 operating system. ICMP based Land attack messages were ICMP echo request messages with source and destination addresses being the same as that of the victim's computer. It was observed that the Windows 7 reacted a bit differently to the ICMP based Land attack packets compared to that of Ping flood attack. In the case of the Land attack, the Windows 7 sent out (to itself) echo reply messages for up to the attack load of 10.7 Mbps of echo request messages (**Figure 9**). Once the ICMP Land attack speed reached 10.8 Mbps (threshold), Windows 7 stopped replying to any of the echo request messages that it would receive.

Table 3. Echo request/reply recorded by Apple's Lion OS under ICMP Land attack.

Echo Requests/Reply for Apple's Lion OS under ICMP Land Attack		
Attack load in Mbps	Echo request/sec	Echo reply/sec
0	0	0
100	148,809/sec	250/sec
200	297,619/sec	250/sec
300	393,412/sec	250/sec
400	393,367/sec	250/sec
500	393,879/sec	250/sec
600	393,117/sec	250/sec
700	393,536/sec	250/sec
800	393,600/sec	250/sec
900	393,606/sec	250/sec
1000	393,490/sec	250/sec

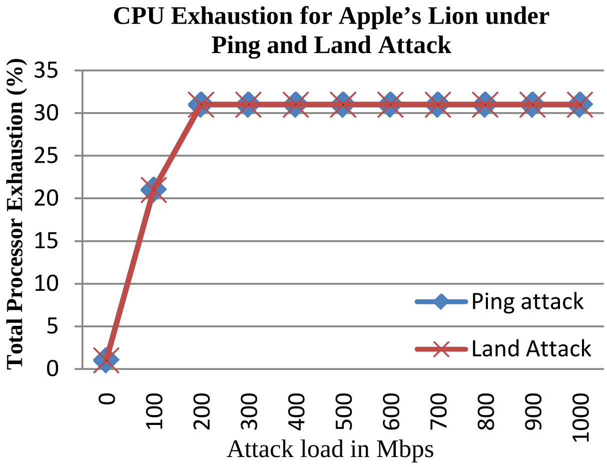


Figure 8. CPU exhaustion is measured to be same for Apple's Lion under ICMP Ping and Land attacks.

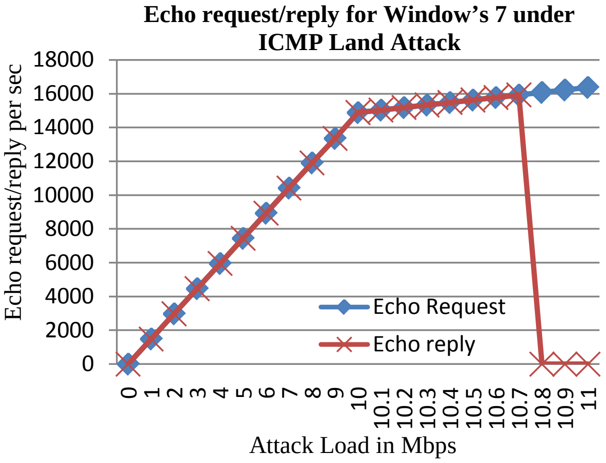


Figure 9. Echo request/reply for Windows 7 under low loads of ICMP Land attack. Windows stopped replying to ICMP Land attack packets after crossing the threshold of 10.8 Mbps.

After crossing the attack threshold of 10.8 Mbps for the received ICMP request messages of the Land attack, Windows 7 completely stopped replying to those ICMP request messages. This was a different approach taken by the Windows 7 operating system for handling the Land attack packets when compared to an ICMP based Ping flood attack. Since it completely stopped responding to ICMP echo request messages, we could see that the exhaustion of the processor decreased approximately by half (**Figure 10**) after crossing the threshold (10.8 Mbps) for the Land attack. This was not the case for Apple's Lion, which would still send 250 echo reply messages per second (**Table 3**) for the duration of the attack.

Unlike the Ping flood attack, the ICMP based Land attack involved sending the echo reply messages to itself and as a result the victim computer (iMac platform) had to process additional echo reply messages when under Land attack. This process had the effect of increasing the exhaustion of the processor under ICMP Land attacks when compared to that under Ping Flood attack especially at lower speeds (**Figure 11**).

4) Microsoft Windows 7 under high attack loads of Ping flood (above 100 Mbps)

As discussed, the Windows 7 was found to handle the ICMP based Land attack packets differently than those of Ping flood attack packets. In the case of ICMP Land attacks, the Windows 7 was found to completely stop replying to the ICMP echo request messages after the attack load of ICMP request messages had crossed the threshold of 10.8 Mbps (**Table 4**, **Figure 9**, **Figure 12**).

We also compare the Windows 7 performance under high attack loads of ICMP based Land attack against that

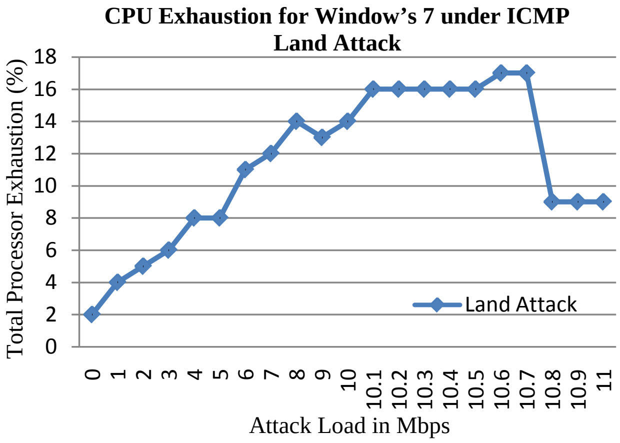


Figure 10. CPU exhaustion for Microsoft's Windows 7 OS under ICMP Land attack.

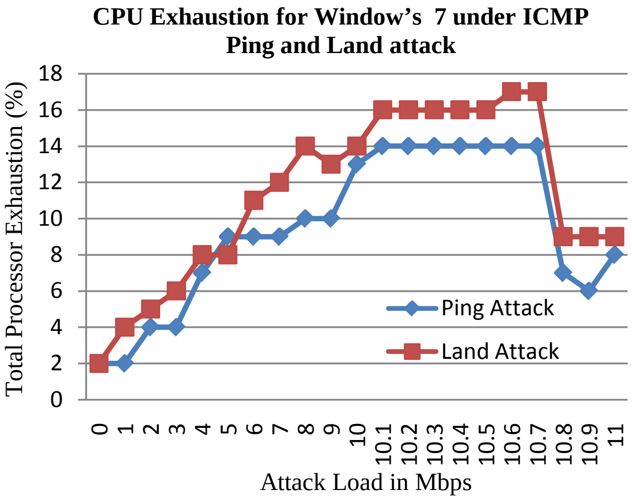


Figure 11. CPU exhaustion for Microsoft's Windows 7 under low loads of ICMP based Land and Ping attacks.

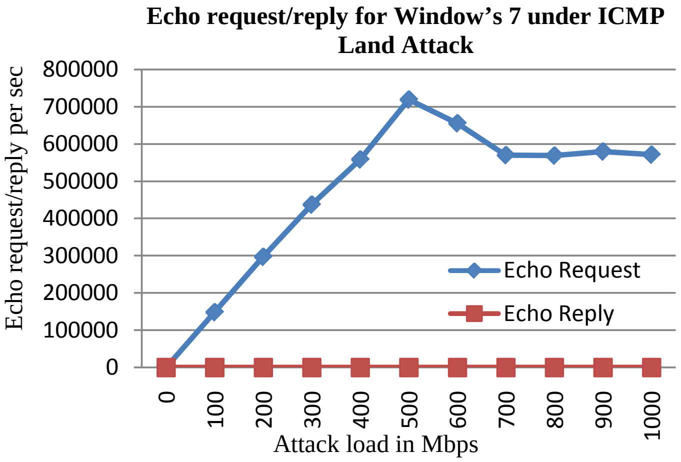


Figure 12. Echo request/reply for Windows 7 under high loads of ICMP Land attack. No echo reply is sent after threshold of 10.8 Mbps is exceeded for the attack load.

Table 4. Echo request/reply recorded by Windows7 under high loads of ICMP Land attack.

Echo Request/Reply for Windows 7 under Land Attack		
Attack load in Mbps	Echo request/sec	Echo reply/sec
0	0	0
100	148,758/sec	0
200	297,355/sec	0
300	437,468/sec	0
400	558,640/sec	0
500	719,453/sec	0
600	655,777/sec	0
700	570,246/sec	0
800	569,050/sec	0
900	579,927/sec	0
1000	571,538/sec	0

under Ping flood attack. We find that the handling of ICMP Land attack packets are such that at higher attack loads, the Windows 7 helps relieve processor exhaustion once the attack load exceeds 10.8 Mbps. In fact, the processor exhaustion was found to be lower than that under the Ping flood attack. This was mainly because in the case of Ping flood attack of higher loads, the Windows 7 was still sending 500 ping replies in the 1st second of the attack, whereas in the case of the ICMP Land attacks, the Windows 7 was sending no replies resulting in less CPU utilization, and hence lower processor exhaustion under Land attack when compared with the Ping flood attack (**Figure 13**).

5) Comparing processor exhaustion due to high loads of ICMP land attacks for the two operating systems

Now we compare the CPU exhaustion under two operating systems namely the Apple's Lion and Windows 7 when exposed to the high attack loads of ICMP based Land attacks.

We found that the Apple's Lion OS was replying to ICMP echo request messages even after crossing the threshold, however, it was rate limiting the response to ICMP request messages by sending out only 500 echo replies/sec. In the case of the Windows 7 operating system, no echo replies were produced when it crossed the threshold and hence it lowered the exhaustion of the CPU at higher attack loads when running the Windows 7 operating system (**Figure 14**) when compared with that under Apple's Lion operating system.

5. Conclusions

Now days, operating systems are increasingly designed with embedded features to protect against DDoS attacks on their own *i.e.* without the help of external security systems. In this paper, we evaluated the built-in security features for the two most popular operating systems namely Apple's Lion and Microsoft's Windows 7 and investigated their performance in protecting a computer system against ICMP based DDoS attacks. We considered two common ICMP based DDoS attacks for our evaluation namely the Ping flood attack and the ICMP based Land attack. We investigated how the two operating systems for the same hardware platform handled the ICMP attack packets and how they rate limited the attack traffic to minimize the adverse effect on the computer's processor exhaustion. It was observed that both operating systems were able to survive these attacks by introducing some useful techniques. One of these techniques was that both operating systems were able to rate limit the number of echo request and echo reply messages that were generated by the processor after crossing a certain threshold for a given attack traffic.

Even with rate limiting, both operating systems didn't produce the same result as they took a bit different approach in rate limiting the ICMP based attack traffic. When under the ICMP Ping and Land attack, it was observed that the processor was less exhausted when the computing platform used Window's 7 as the operating

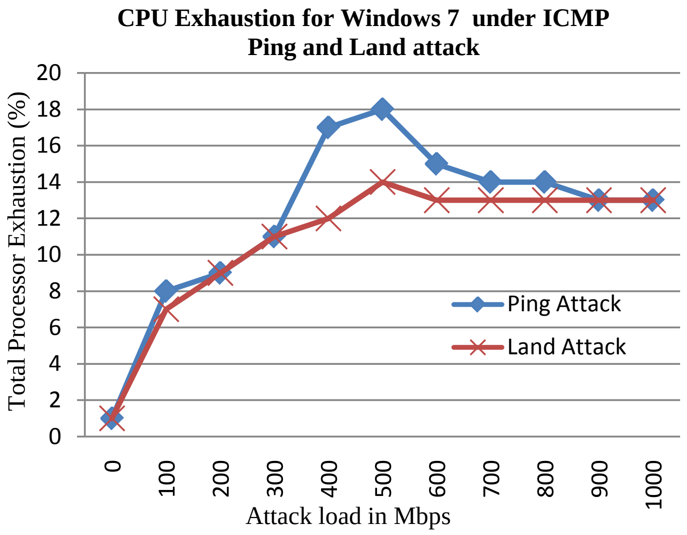


Figure 13. CPU exhaustion for Microsoft's Windows 7 under ICMP Ping and Land attack.

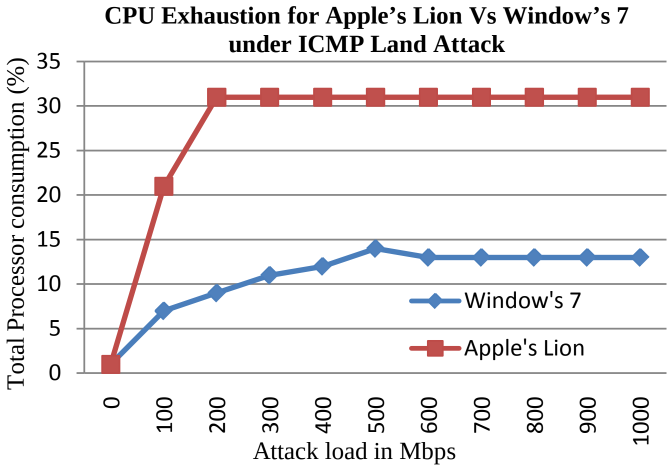


Figure 14. CPU exhaustion with Apple's Lion vs. Window's 7 under high loads of ICMP Land attack.

system compared to when it used Apple's Lion operating system. For example, in our measurements, Apple's Lion operating system incurred a maximum processor exhaustion of 31% whereas under the same ICMP Land attack and for the same hardware platform, the Windows 7 incurred a maximum processor exhaustion of 17%. Similar was the case with Ping flood attack where Windows 7 operating system was observed to incur lower processor exhaustion compared with the situation when Apple's Lion operating system was used. This paper conveys the fact that the rate limiting schemes when embedded in the operating systems can play an important role in DDoS attack mitigation. This paper also conveys the fact that different approaches to rate limiting can have varying impact on minimizing the exhaustion of computing resources of a computer system when faced with DDoS attacks.

Acknowledgements

This paper is based upon work supported in part by US National Science Foundation under Grant No. 0421585.

References

[1] Mirkovic, J., Dietrich, S., Dittrich, D. and Reiher, P. (2013) Understanding a Denial of Service Attack.

http://www.informit.com/articles/article.aspx?p=386163&seqNum=5

[2] Arbor Networks (2014) Worldwide Infrastructure Security Report. http://www.arbornetworks.com/research/infrastructure-security-report

[3] (2013) DDoS Attacks Against Government and Entertainment Websites Escalate.

[4] (2014) OS X Lion—The World's Most Advanced Desktop Operating System. http://web.archive.org/web/20110806091718/http://www.apple.com/macosx/

[5] (2014) Apple's Lion Roars onto Computers with 1 Million Downloads in a Day. The Independent (UK). http://www.independent.co.uk/life-style/gadgets-and-tech/apples-lion-roars-onto-computers-with-1-million-downloads-in-a-day-2318755.html

[6] (2013) Why You'll Love a MAC.

[7] Nash, M. (2014) Why 7? The Windows Blog. Microsoft. http://blogs.windows.com/windows/archive/b/windowsvista/archive/2008/10/14/why-7.aspx

[8] Wikipedia (2014) Windows 7. http://en.wikipedia.org/wiki/Windows_7

[9] Postal, J. (1981) Report for Comments for ICMP, RFC 792. http://www.ietf.org/rfc/rfc792.txt

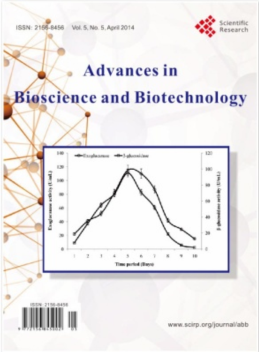
[10] (1989) RFC 1122—Requirements for Internet Hosts—Communication Layers. http://tools.ietf.org/html/rfc1122#page-42

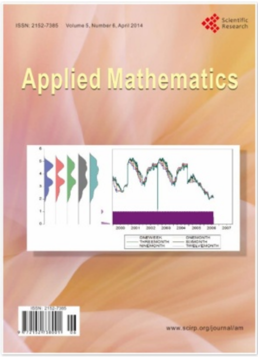
[11] Surisetty, S. and Kumar, S. (2010) Is Apple's iMac Leopard Operating System Secure under ARP-Based Flooding Attacks? *IEEE Proceedings of the* 5*th International Conference on Internet Monitoring and Protection*, Barcelona, 9-15 May 2010, 60-64.

[12] Surisetty, S. and Kumar, S. (2010) Is McAfee Security Center/Firewall Software Providing Complete Security for Your Computer? 4*th International Conference on Digital Society*, St. Maarten, 10-16 February 2010, 178-181.

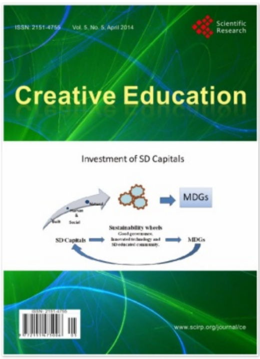
[13] Surisetty, S. and Kumar, S. (2012) Microsoft vs. Apple: Resilience against Distributed Denial-of-Service Attacks. *IEEE Security & Privacy*, 60-64.

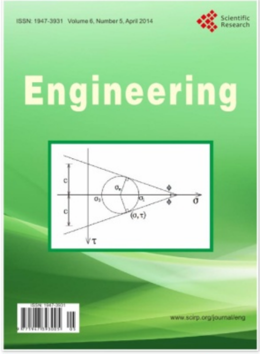
[14] Gade, R.S.R., Vellalacheruvu, H. and Kumar, S. (2010) Performance of Windows XP, Windows Vista and Apple's, Leopard Computers under a Denial of Service Attack. 4*th International Conference on Digital Society*, St. Maarten, 10-16 February 2010, 188-191.


Scientific Research
Advances in
Bioscience and Biotechnology
www.scirp.org/journal/abb

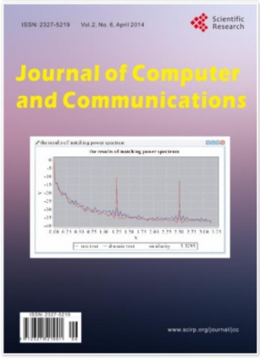

Scientific Research
Applied Mathematics
www.scirp.org/journal/am

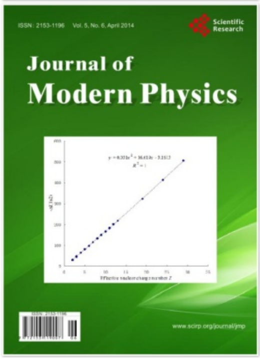
Scientific Research
American Journal of
Plant Sciences
www.scirp.org/journal/ajps


Scientific Research
Creative Education
Investment of SD Capitals
MDGs
www.scirp.org/journal/ce

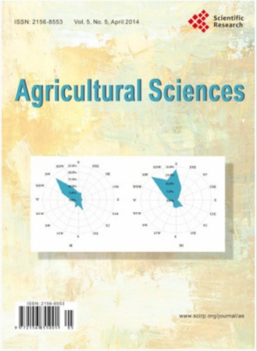

Scientific Research
Engineering
www.scirp.org/journal/eng

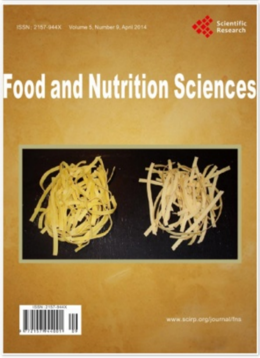
Scientific Research
HEALTH
Editor-in-Chief
Prof. James J. Chou
www.scirp.org/journal/health

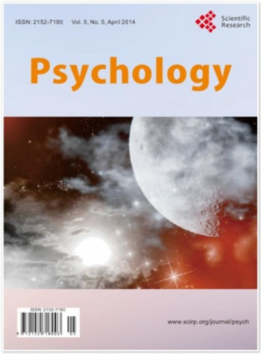

Scientific Research
Journal of Computer
and Communications
www.scirp.org/journal/jcc


Scientific Research
Journal of
Modern Physics
www.scirp.org/journal/jmp

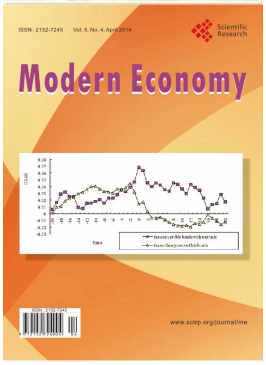
Scientific Research
Journal of
Environmental Protection
http://www.scirp.org/journal/jep


Scientific Research
Agricultural Sciences
www.scirp.org/journal/as


Scientific Research
Food and Nutrition Sciences
www.scirp.org/journal/fns


Scientific Research
Psychology
www.scirp.org/journal/psych

Scientific Research
Natural
Science
Editor-in-Chief
Kuo-Chen Chou
www.scirp.org/journal/ns


Scientific Research
Modern Economy
www.scirp.org/journal/me

Scientific Research
Journal of Cancer Therapy
www.scirp.org/journal/jct

Scientific Research
American Journal of
Analytical Chemistry
www.scirp.org/journal/ajac