IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011
ISSN (Online): 1694-0814
www.IJCSI.org

ARP Storm Detection and Prevention Measures

S.Vidya[1] and R.Bhaskaran[2]

[1] Department of Computer Science, Fatima College
Madurai – 626 018, Tamil Nadu, India

[2] School of Mathematics, Madurai Kamaraj University
Madurai – 625 021, Tamil Nadu, India

Abstract

The Address Resolution Protocol (ARP) is used by computers to map network addresses (IP) to physical addresses (MAC). The protocol has proved to work well under regular circumstances, but it was not designed to cope with malicious hosts. By performing ARP storming attacks, an intruder can create Denial of Service (DoS) in another host and prevent it's functioning or just cause network slowdowns. Several methods to mitigate, detect and prevent these attacks do exist at the router level and through certain customized software tools. In this paper we propose an algorithm to detect the ARP storm at the local sub network level within the ARP boundary in real-time and in offline mode. In real-time, the software detects dynamically, the IPs from which the ARP storm emanates. The inexpensive and portable software developed can be implemented in SOHOs in each machine in the local network. The attempt was successful and also effective in terms of cost, portability and ease of use. The offline packet analysis software, detects all the possible malicious IPs that are responsible for the ARP storm from among the packets captured in real-time using Wireshark. The proposed method also suggests the means of preventing the ARP storm.

Keywords: *ARP storm, Denial of Service, Internet Protocol address, Media Access Control Address, algorithm.*

1. Introduction

In Local Area Networks (LAN), Media Access Control (MAC) addresses are used in data transfer. MAC address operates at the Data Link layer of the TCP/IP protocol stack. So it is important to convert IP address to MAC address in order to communicate in a LAN. Address Resolution Protocol (ARP) is used for this purpose. When a node in a LAN wants to send data, it refers the ARP cache to find out the MAC address corresponding to the IP address of the node [1].

In Ethernets, Ethernet addresses or MAC addresses are required for communication between network devices. Such devices must send or receive packets to Ethernet addresses. These addresses consists of 48 bits (6 octets), whereas IP addresses are of 32 bits (4 octets). ARP deals with the two kinds of packets – ARP request and ARP reply.

When a sender wants to know the MAC address of the destination IP node, it broadcasts the ARP request to every host in the network. The destination node sends a reply to the sender with MAC address through ARP reply in a unicast mode. Under ideal conditions where the LAN is safe with no attackers present, the intended target IP node replies to the sender. After receiving such response, the sender caches the MAC address of the target IP node locally to speed up future communication between these two nodes.

Fig.1 shows how a typical ARP protocol communication happens. The machine with IP address 192.168.0.1 sends a broadcast request, asking for the MAC address of the machine whose IP address is 192.168.0.3. Once the request is received by 192.168.0.3, it sends a reply to 192.168.0.1 that, 00:E0:FE:09:C2:11 is the MAC address [2].

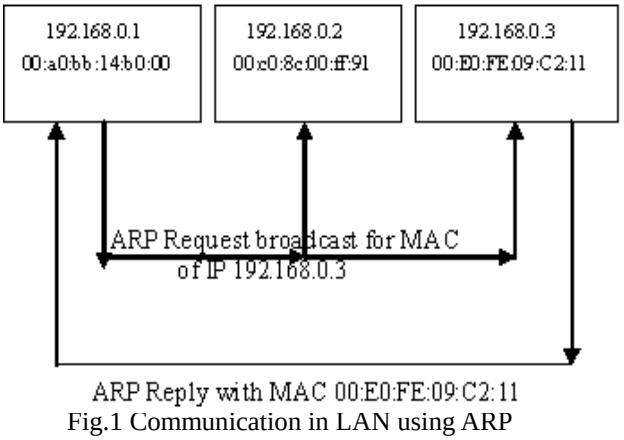

Fig.1 Communication in LAN using ARP

2. ARP Storm

It is common for computer networks to slowdown due to both internal and external factors. Internal factor generally is over extending of bandwidth and bottleneck situations when user needs exceeds resources in specific network sectors. These problems can be addressed by network management systems and system provided utilities such as traceroute [3], which allow administrators to identify problem spots and carry out load balancing to improve the situation. External factors are threats that exploit network vulnerabilities to carry out attacks like Denial of Service (DoS), Distributed Denial of Service (DDoS) and network data interception. DoS are intended to slow down or bring down the networks altogether or of a single specific machine. These attacks are among the most serious threats that computer networks face today [4].

ARP storm is an attack situation intentionally created by an attacker from within the local network. In ARP packet storm the attacker keeps generating broadcast packets, with IP addresses within a subnet range or even to IP addresses not present in the local subnet. The purpose of this attack might be that the attacker wants to create a DoS by reducing the bandwidth with unwanted traffic or collect the IP/MAC address details noisily, of all machines for later attacks. Even well known attacker tools like Ettercap [5] uses the noisy way as default to build the host list by performing an ARP storm, where the attacker machine sends out ARP requests or pings every IP address in the current net mask [6].

In ARP attack, the DDoS agents constantly send a barrage of ARP requests to the gateway, or to a victim computer within the same sub network, and tie up the resource of attacked gateway or host.

When we diagnosed the network traffic using a network analyzer, we could detect a large series of Address Resolution Protocols. This might cause temporary disruption in network access and in bi-directional traffic throughout the network. Even if the attack is aimed at a single specific machine, Sanjeev Kumar et al [7] in their work have observed that an ARP attack not only exhausts resource of the victim computer but also significantly exhausts processing resource of other non-victim computers. The non-victim computers do have the impact in terms of the network traffic slowdown and time wasted in processing of unwanted broadcast packets only to be discarded.

2.1 Causes for the Storm

The reason for the storm need not always be the malicious intent of an attacker, but can be vulnerability due to some network hardware misconfiguration or presence of malicious software somewhere in the network. Incorrect network design and improper plan in the hubs might easily lead to broadcast storm, NIC or switching equipment damage, Network loop. Our research has been carried with the assumption that most of the hardware in the LAN will be in working condition and are configured properly with zero or minimal vulnerability due to mis-configuration and there are no malicious software that uses MAC vulnerability, are present in the network.

The computer program that implemented our algorithm identifies the attacker machine in the local sub network within the ARP boundary, from which the storm is intentionally created by an attacker.

3. Proposed Method

The existing common solution being suggested, implemented and practiced to prevent ARP storm is to configure the routers and manageable switches in such a way to prevent ARP flooding. In large internetworks, many of these concerns are addressed through protocol filtering within routers and switches in the network layer 3 routing design. When a problem occurs because of an anomaly or possible misconfiguration of an internetwork, then software tools could be used to capture the information. By applying specific technique with a protocol analyzer, an analyst can very quickly capture a broadcast storm and identify the cause of the broadcast storm and develop a method to resolve the storm. Almost all management systems for internetwork hubs, routers and switches facilitate broadcast storm identification. The threshold that determines what is an actual broadcast occurrence versus an actual broadcast storm is usually set by the network manager or the configuring analyst of the network management platform [8].

At the software front, very few of the commercial soft wares available for IDS, detect and prevent an ARP storm.

Attacks against layer two, the data link layer, range from various ARP attacks like the cache poisoning for wired clients to de-authentication of wireless clients. Fairly simple to implement, these attacks can often go unnoticed by intrusion analysts since intrusion detection systems typically look at the network layer and above to detect attacks. Whatever method of attack an attacker uses to attack the data link layer, in all cases, an adversary attempts to compromise confidentiality, authentication or availability of information. The attacks succeed for the most part because of the lack of fine-grain controls for the data link layer. While layer 2 is considered a less novel platform for attacks, layer 2 attacks continue to trouble the networked systems. The implementation of each attack is unique [9]. This being the current scenario, gave us the

motivation to develop new algorithm and software tools to examine network traffic for data link layer attack and proactively respond to attacks. The tool we have developed supports both online and offline detection.

3.1 Online Detection Method

Identifying weak points of network systems and protecting them before attackers or hackers detect and exploits are regarded as essential security methods, especially on the LAN system which uses ARP, a protocol with known security loopholes enabling hackers to conduct various ARP attacks on the LAN systems [10]. The online detection method proposed here, is our algorithm implemented into a software tool written in JAVA using the Jpcap wrapper class for winpcap/libpcap [11]. Jpcap is a Java library for capturing and sending network packets. It has been tested in Microsoft Windows (98/2000/XP/Vista) and Linux (Fedora, Mandriva, Ubuntu), MacOS X (Darwin), FreeBSD, and Solaris. It is open source and is licensed under GNU LGPL. Jpcap does not block, filter or manipulate the traffic generated by other programs on the same machine. Therefore, it does not provide the appropriate support for applications like traffic shapers, QoS schedulers and personal firewalls.

This tool is designed to capture the online network traffic, filter the ARP packets, analyze for the ARP storm based on time and look out for the various source IPs which create the storm. The tool is also enabled to display the details of the IPs that are sources of the storm and need to be blocked.

The Algorithm for the Detection scheme:

1. Fix the threshold for the storm detection in terms of number of packets per second.
2. Capture network traffic online using Jpcap wrapper class.
3. Filter ARP packets.
4. Identify malicious IPs by comparing against the threshold and are categorized based on the criticality.

The critical nature of the situation is categorized into three as, possibility of a storm – Low, a storm has occurred – Critical, Denial of Service – Highly Critical.

This tool could be run as a background task infinitely until the user chooses to stop.

3.2 Sample Screen Shots of result generated by Online Detection

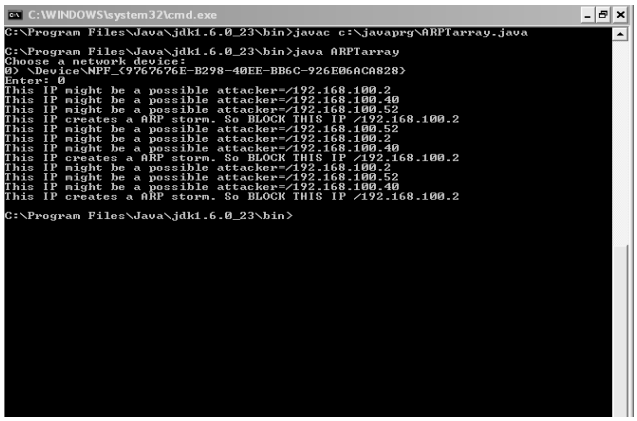

Fig.2 Screen Shot listing Malicious IPs detected

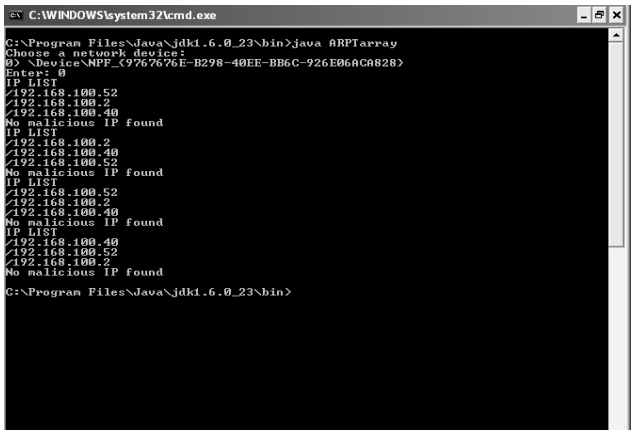

Fig.3 Screen Shot listing No malicious IP detected

3.3 Offline Detection Method

The offline detection method is implemented on the packets captured online using Wireshark V1.4.1 [12]. The software tool that is developed analyses these captured packets in offline and detects whether there had been an ARP storm from any of the IPs. The result is a list of malicious IPs, if found, based on the category of criticality of the situation. As in the case of online detection method the three categories of Low, Critical and Highly Critical are classified based on the count of the packets arrived within a second or less than a second.

The offline detection algorithm is as follows,

1. Fix the threshold for detection of malicious IP in terms of packets captured per second.
2. Open the database of captured packets. This database is created by exporting the Wireshark captured file to csv format file.
3. Filter ARP packets.
4. Count the number of ARP packets captured within a second or less based on relative time of capture.
5. Generate output, listing the IPs under the category of criticality.

3.4 Sample Screen Shot of the result of Offline Detection

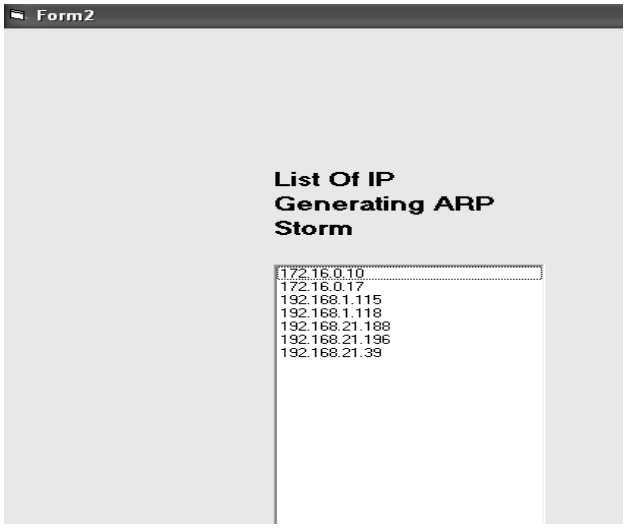

Fig. 4(a) Sample screen shot – offline detection

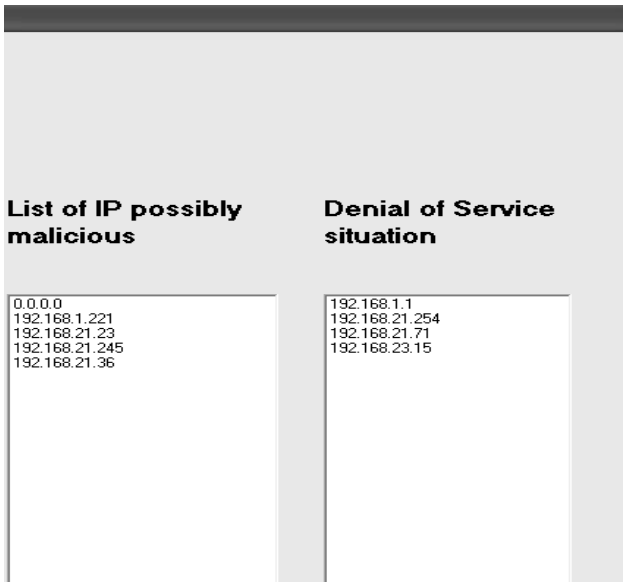

Fig. 4(b) Sample screen shot – offline detection

3.5 Using the developed tool

This tool detects malicious IP addresses. Not only the system administrator but also any network user could use this tool to analyze the network and possibly block the malicious IPs using firewall. The main objective of this tool is that any lay user using the network should be able to install in individual machine and be able to detect ARP anomaly and also block troublesome IPs.

Once the tool detects the IP to be blocked, preventing the storm is by blocking the traffic from the particular IP for a short span of time and releasing. For that, any personal firewall could be used. In Windows environment, wipfw was found to be effective for the purpose.

4 Conclusion

It is always better to find solutions in the local context to the problems arising in the network, to the extent possible. With the current trend being that of free wares, Open Source and platform independent software, it is good to design tools that could be tailored to detect and prevent, if not to mitigate the pricks and intrusions that arise. The tool explained here could be tailor made to suit the individual network environment needs. For instance, setting of the threshold value is localized to each network based on factors like the network bandwidth, usual nature of the broadcast traffic etc. In this work, the threshold was finalized by performing a passive analysis of real-time network traffic captured over a period of time [2]. The average number of packets per second in normal traffic was and the threshold finalized to suit our network environment.

References

[1] Behrouz A. Forouzan, "TCP/IP Protocol Suite", Fourth Edition, Tata McGraw Hill, pp. 220-223, 2010.

[2] S.Vidya, N.Gowri, R.Bhaskaran, "ARP traffic and Network Vulnerability", in proceedings of INDIACOM-2011, conducted by BVICAM, New Delhi, India, page – 619 and in CD.

[3] Wikipedia, The Free Encyclopedia, "Traceroute", http://en.wikipedia.org/wiki/Traceroute, 2011.

[4] "Network Vulnerabilities", http://javvin.com//etraffic/network-vulnerabilities.html. Javvin Network Management and security, Javvin Technologies Inc.

[5] Blaise Carrera, "Ettercap", http://openmaniak.com/ettercap.php, 2008.

[6] Patrick Kelly, "ARP Poisoning – ETTERCAPng", http://web.mac.com/opticrealm/iWeb/asurobot/MyCyberAttackPapers/MyCyberAttackPapers-files/ettercap_Nov_6_2005-1.pdf, 2005.

[7] Sanjeev Kumar, Orifiel Gomez, "Denial of Service due to direct and Indirect ARP storm attacks in LAN environment", Journal of Information Security, 2010, 1, pp. 88-94, doi:10.4236/jis.2010.12010 Published online October 2010 (http://www.SciRP.org/journal/jis)

[8] Daniel J. Nassar, "Network Analysis and Optimization Techniques", Chapter 5 from Network Performance Base lining, New Riders Publishing, http://technet.microsoft.com/en-us/library/bb726961.aspx#EJAA, 2011.

[9] TJ O'Connor, "Detecting and Responding to Data Link Layer Attacks", SANS Institute InfoSec Reading Room, Oct 13, 2010, http://www.sans.org/reading_room/whitepapers/detection/detecting-responding-data-link-layer-attacks_33513, 2010.

[10] Thawatchai Chomsiri, "Sniffing Packets on LAN without ARP spoofing", Third 2008 International Conference on Convergence and Hybrid Information Technology, 2008 IEEE, doi 10.1109/ICCIT.2008.318.

[11] Keita Fujii, "Jpcap – a Java library for capturing and sending network packets", http://netresearch.ics.uci.edu/kfujii/Jpcap/doc/, 2007.
[12] Gerald Combs, "Wireshark", http://www.wireshark.org/about.html, 2011.

S.Vidya M.Sc., M.Phil. Working as Associate Professor in Computer Science in the Department of Computer Science, Fatima College, and Madurai since 1990. Areas of interest are Data Structures and Algorithms. Currently, pursuing research in Network Security. Life member of Computer Society of India and member of ACM.

Dr.R.Bhaskaran M.Sc., Ph.D., Joined the School of Mathematics, Madurai Kamaraj University, Madurai in 1980. Currently, he is the Chairperson of School of Mathematics. His area of interest includes Linden Mayer System, Computer Applications, and developing software for learning mathematics. He has guided students in both Mathematics and Computer Applications. He is a Life Member of the Indian Mathematical Society.