Light Weight Approach for IP-ARP Spoofing Detection and Prevention

Dr. S. G. Bhirud
Department of Computer Engineering
V.J.T.I., Mumbai, India
sgbhirud@yahoo.com

Vijay Katkar
Department of Computer Engineering
Bharti Vidyapith, Pune, India
katkarvijayd@gmail.com

Abstract —**Heavily used intra-domain protocols (like IP, ARP) do not have protection mechanism against malicious activities by network clients. As a result IP and ARP spoofing are used by attackers to launch Man In The Middle (MITM), Denial of Service (DoS) and other attacks. These attacks are severe threats to the organizations. Detecting and preventing IP-ARP spoofing will enhance the security to great extent. This paper presents a simple and light-weight mechanism for detection and prevention of IP-ARP spoofing attacks. Experimental results are also provided to support the proposal.**

Keywords— ARP Spoofing, IP Spoofing, Spoofing Detection and prevention

I. INTRODUCTION

Network Intrusion Detection System (NIDS) is most widely tool for network security. It can detect attacks against network, but cannot prevent network from attacks. Thus researchers are working on design of Network Intrusion Detection and Prevention System (NIDPS) which can prevent network from detected attacks.

Raw socket programming feature is supported by all programming languages which allows programmer to create and inject TCP/IP packets on network. This feature is widely used by attackers to create fake TCP/IP packets and intrude into the system. This process of creating and injecting fake TCP/IP packets on network is called as Spoofing.

Worms and viruses are used by attackers to create zombie machines in the Organization. This paper denotes such an organization as Zombie Organization. These zombie machines are then used by attackers to launch attack against Zombie Organization itself or other Organizations using IP and ARP spoofing. Thus there should be a mechanism which can detect and prevent these attacks at the zombie organization itself. If attack is detected and blocked at the Zombie organization, then it will reduce a huge amount of traffic between Attack Target and Zombie organization.

The rest of this paper is organized as follows. Section 2 gives brief introduction of IP Spoofing-based attacks. Section 3 gives brief introduction of ARP Spoofing-based attacks. Section 4 gives overview of research work done for detection and prevention of IP and ARP spoofing based attacks. Proposed mechanism is discussed in section 5 and section 6 presents the experimental results. Section 7 concludes the paper.

II. IP SPOOFING-BASED ATTACKS

IP Protocol: IP is basic and most widely used protocol in TCP/IP suit. It is used to uniquely represent a host on the network. Since it is connectionless protocol, upper layer protocols such as TCP are responsible for connections establishment and management.

IP Spoofing: IP spoofing is process of forging the Source IP addresses in TCP/IP packets. It is one of the widely used mechanisms by hackers to launch DDoS attacks. Two main reasons for using this:

- Hide true identity and location of attacker
- Making Source IP based packet filtering less effective.

Types of IP Spoofing-based attacks: Connectionless nature of IP protocol is exploited by attackers to launch following attacks.

978-1-4577-1088-9/11/$26.00 ©2011 IEEE

A. *Port Scanning*

Spoofed IP packets with SIN flag set are used to check which ports of a host are open. Then these open ports are used to intrude into host.

B. *OS Finger Printing*

Spoofed IP packets are used o check which OS is installed on the host machine. Then known vulnerabilities of that OS are used to intrude into host.

C. *DoS Attack*

Huge volume of Spoofed IP packets are sent to a target host or server. This high volume of traffic makes that machine unable to respond to a genuine traffic. Since attacker is not interested in response to these spoofed packets, IP spoofing is most suitable for such attacks.

D. *DDosS Attack*

DoS Attack: Huge volume of Spoofed IP packets are sent to a target host or server from many machines. This method is used to make DoS attack detection Security systems less effective.

III. ARP SPOOFING-BASED ATTACKS

A. *ARP Protocol*

The Address Resolution Protocol (ARP) [3] is used to map Network Addresses of a machine (IP address) to Physical Addresses (MAC address). This protocol plays an important role in LAN environment, as each frame transmitted by host must contain a destination MAC address. If IP address of a destination host is known, then ARP is used to determine the host's MAC address. This MAC address is then used to deliver frames to destination host on the network. The working of ARP protocol is as follows.

1) The host broadcasts an ARP request message on the network to determine MAC address of another host.
2) All the hosts connected to LAN receive the request.
3) The host, whose IP address matches with the destination IP of ARP request message, sends back a unicast ARP reply containing its own MAC address.
4) After receiving ARP reply, the host caches the (IP, MAC) pairing in a local ARP cache to avoid the same ARP request in future.

B. *ARP Spoofing*

ARP spoofing is a process of creating and injecting fake ARP request and ARP reply messages on the network. It is used by attackers to control the flow of packets over a network according to their requirement.

C. *ARP Cache Poisoning*

ARP is a stateless protocol. Even though ARP request is not issued by host and it receives an ARP reply message, it will update its own ARP cache using ARP reply message. Attacker takes advantage of this by using ARP Spoofing to manipulate the ARP cache of target host(s). This manipulated ARP cache is then used to launch Man-In-The-Middle (MITM) and DoS attacks. This process of manipulating the ARP cache for malicious activities is called as ARP cache poisoning

D. *Types of ARP Spoofing-based Attacks*

Following attacks are launched by attackers using ARP spoofing

1) DoS attacks: ARP spoofing is used to change the ARP cache table of host so that every packet sent by host is directed to the attacker. In this way communicating originating from host is blocked by the attacker.
2) Host impersonation attack: ARP spoofing is used to change the ARP cache table of host communicating with each other so that every packet sent by host is directed to the attacker. After receiving the packet from host attacker responds to it and creates impression that host is communicating with desired destination.
3) Man-In-The-Middle (MITM) attack: By poisoning ARP cache of two hosts which are communicating with each, the attacker can monitor all the traffic between two hosts.. This attack is used to access sensitive information like passwords and modify the data being communicated to compromising the data integrity.

IV. RELATED WORK

Use of static ARP entries is the simplest mechanism to protect against ARP spoofing. But this solution is not suitable for large organization. Neminath H. el at [1] has proposed a light weight mechanism using state transition tables for detection of ARP response spoofing, but it does not provide prevention mechanism against the attack. Wenjian Xing el at [2] has proposed a simple and light weight mechanism for defense against ARP attacks based on Inspection of ARP packets. This method is vulnerable to ARP packet spoofing using RAW socket programming. Somnuk Puangpronpitag and Narongrit Masusai [4] have proposed a light weight mechanism for ARP spoofing detection and prevention using static IP-MAC pair entries of every host on the network. Maintaining these entries is a responsibility of the System Administrator. But it is not feasible for Administrator to maintain such a huge table in large scale organizations. D. Bruschi et al [5] have proposed Secure ARP (S-ARP) protocol which uses, Key Distributor, Public-Private keys for signing every ARP message. Separate Server is used for resolving ARP requests based on secrete sharing concept. Craig A. Shue et al [6] have proposed a mechanism for ARP Spoofing detection and prevention using Secure DHCP. According to them while sending ARP reply host must include certificate issued by Secure DHCP in a reply message. This certificate is then used to check the authenticity of the ARP reply. This scheme requires changes in the implementation of ARP protocol which is not feasible. There are many proposed mechanisms [7, 8, 9, 10, 11, and 12] to detect and prevent IP spoofing based attacks. But none of them can detect and prevent IP spoofing at the Zombie Organization itself.

V. PROPOSED MECHANISM

NIDPS monitors the traffic of entire network. In large scale organizations load on NIDPS is very high and as the number of high-speed machines in the organization are increased, it increases a burden on NIDS to a great extent. Due to this analysis of every packet of the network is almost impossible for NIDS.

Every large scale Organization is divided into departments and each department has its own Local Area Network. So we can use separate NIDPS for every department (as shown in figure 1) to reduce a load on NIDPS.

A small agent program called Information Agent [IA] is installed on every machine of the organization. NIDPS communicates with these agents to detect spoofing activities.

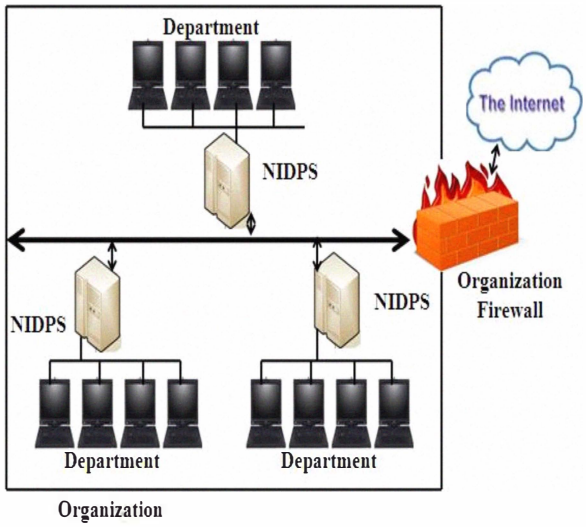

Figure 1: Network Organization

Responsibilities of IA are:

i. Every time a machine is booted, IA sends the IP-MAC address pair to NIDPS
ii. When machine sends an ARP Request message, IA informs this event to NIDPS
iii. When machine sends an ARP Reply message, IA informs this event to NIDPS.
iv. It maintains a table of IP Address-Identification pair present in every IP packets sent by the host.
v. It counts number of packets sent by machine A in a time interval 'T' (i.e. IP_Pavket_Count_A) and sends it to NIDPS.

IP Address and Identification is used to uniquely identify every packet sent by a host. So this field is used in this mechanism to detect spoofed packets sent by zombie machines.

NIDPS uses IP-MAC address pairs sent by IAs to create and manage table of IP-MAC address pairs of all machines in LAN. Working of NIDPS for Detection and Prevention of ARP Spoofing is as described below.

I. If ARP reply message is sent from machine A to a machine B in a LAN Then
   a. Note the IP-MAC address pair present in the ARP Reply message
   b. If (IA of B has informed ARP Request message AND IA of A has informed ARP Reply message) then
      i. No Problem
   c. Else If(IA of B has not informed ARP Request message or IA of A has not informed ARP Reply message) Then
      i. Report ARP spoofing
      ii. Retrieve IP-MAC pair from table maintained by NIDPS using IP address present in spoofed packet.
      iii. Create ARP reply message using IP-MAC pair retrieved from NIDPS table
      iv. Send newly created ARP Reply message to B

II. If (No of packets received with source IP Address of Machine A within a time interval 'T' >IP_Packet_Count_A)
   a. Report IP spoofing activity
   b. Add every packet with source IP address of Machine A to buffer
   c. Use IP Address and Identification pair present in IP buffered packet to ask IA of machine A whether this packet is sent by Machine A
      i. If(Reply is 'YES')
         1. Sent buffered packet over a network
         2. Instruct IA of machine A to delete that entry from machine A
      ii. Else
         1. Discard the buffered packet

Mechanism used by NIDPS to detect and prevent IP-ARP spoofing based activities is briefly described above. Existence of ARP Reply message from machine A to machine B even though machine B has not ask for ARP request or machine A has not sent ARP Reply message, indicates ARP Spoofing Activity. If this activity has happed, it means machine B has wrong ARP cache entry due to spoofed ARP Reply message. So to correct this ARP cache entry, NIDPS creates a new ARP Reply packet with correct entries from its own IP-MAC pair table and sends it to the machine B. Now after receiving this ARP Reply packet machine B will again modify its own ARP cache and its ARP cache will be correct now. Here we have used ARP spoofing to prevent ARP cache poisoning.

If machine A has sent only 'N' number of IP packets and number of IP packets received by machine NIDPS with IP address of machine A is greater than 'N', indicates IP spoofing activity on the network. If this activity is detected on network, NIDPS buffers every packet with source IP of machine 'A' instead of discarding or allowing it to pass. Then it asks IA of machine A using IP Address-Identification pair of buffered packet, whether machine A has sent this packet or not. If IA of A sends positive reply, NIDPS firewall allows that packet to pass otherwise it simply discards the buffered packet as spoofed one.

VI. EXPERIMENTAL RESULTS

NIDPS Firewall is implemented using a machine with two network cards. One network card is used to receive packets from the LAN and second network card is used to pass the packets from LAN to outside network. We have implement ARP spoofing, IP spoofing, NIDPS using JAVA Raw Socket programming. NIDPS programs read packets from one network card and decide whether to place the packet on second network card or not.

A. *Test Scenario 1*

We sent spoofed ARP Packets from three machines of the network. This event was detected by NIDPS. After detecting this event NIDPS sent spoofed ARP reply packets to correct the ARP cache. We checked the ARP cache entries of OS after this test and it was correct.

B. *Test Scenario 2*

Went sent 20,000 spoofed IP packets containing source IP address of another two machines of the LAN and destination IP address of "Google.com". NIDPS identify the IP spoofing event and out of these 20,000 packets 18,628 packets were discarded by NIDPS.

C. *Test Scenario 3*

Went sent 20,000 spoofed IP packets containing source and destination IP address of another two machines of the LAN. This event was detected by NIDPS but none of these packets were discarded by NIDPS.

VII. CONCLUSION

The proposed mechanism for IP and ARP spoofing detection has following plus points:

i. Can block attack at the source of attack itself.
ii. It can detect as well as prevent IP and ARP spoofing based attacks.
iii. Even though it maintains tables of IP-MAC pairs, it does not require manual entries, which makes it is suitable for large organizations.
iv. Proposed mechanism does not require change in ARP protocol.
v. It is a light weight mechanism.

The limitation of this mechanism is that, it cannot detect IP spoofing attacks launched from the LAN against the LAN itself. Research should be done to avoid such attacks.

REFERENCES

[1] Neminath H, S Biswas, S Roopa, R Ratti, R Nandi, F.A. Barbhuiya, A Sur, V Ramachandran, "A DES Approach to Intrusion Detection System foe ARP Spoofing Attacks", 18th Mediterranean Conference on Control & Automation (MED), ISBN: 978-1-4244-8091-3, IEEE 2010

[2] Wenjian Xing, Yunlan Zhao, Tonglei Li, "Research on the defense against ARP Spoofing Attacks based on Winpcap", 2010 Second International Workshop on Education Technology and Computer Science, Digital Object Identifier: 10.1109/ETCS.2010.75, 2010 IEEE

[3] David C. Plummer, "An Ethernet Address Resolution Protocol", Request For Comments: 826

[4] Somnuk Puangpronpitag, Narongrit Masusai, "An Efficient and Feasible Solution to ARP Spoof Problem", 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 2009. ECTI-CON 2009. ISBN: 978-1-4244-3387-2

[5] D. Bruschi, A. Ornaghi, E. Rosti, "S-ARP: a secure address resolution protocol, "Annual Computer Security Applications Conference (ACSAC), 2003.

[6] Craig A. Shue, Andrew J. Kalafut, Minaxi Gupta, "A Unified Approach to Intra-Domain Security", International Conference on Computational Science and Engineering, IEEE 2009,ISBN: 978-1-4244-5334-4

[7] Yunji Ma, "An Effective Method for Defense against IP Spoofing Attack", 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), EEE2010, ISBN: 978-1-4244-3708-5

[8] Haining Wang, Cheng Jin, Kang G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL.15,NO.1, FEBRUARY 2007

[9] Lei Wang, Tianbing Xia, Jennifer Seberry, "Inter-Domain Routing Validator Based Spoofing Defence System", International Conference on Intelligence and Security Informatics (ISI), IEEE 2010, ISBN: 978-1-4244-6444-9

[10] Dalia Nashat, Xiaohong Jiangand, Susumu Horiguchi, "Detecting SYN Flooding Agents Under Any Type of IP Spoofing", IEEE International Conference on e-Business Engineering, IEEE 2008,ISBN: 978-0-7695-3395-7

[11] Wei Chen, Dit-Yan Yeung, "Defending Against TCP SYN Flooding Attacks Under Different Types of IP Spoofing", International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, IEEE 2006. ICN/ICONS/MCL 2006, ISBN: 0-7695-2552-0

[12] Zhenhai Duan, Xin Yuan, Jaideep Chandrashekar, "Controlling IP Spoofing through Inter domain Packet Filters" IEEE Transactions on Dependable and Secure Computing, Issue: Jan.-March 2008 ISSN : 1545-5971