ISA Transactions 50 (2011) 119–130

Contents lists available at ScienceDirect

ISA Transactions

journal homepage: www.elsevier.com/locate/isatrans

LAN attack detection using Discrete Event Systems

Neminath Hubballi, Santosh Biswas *, S. Roopa, Ritesh Ratti, Sukumar Nandi

Department of Computer Science and Engineering, Indian Institute of Technology, Guwahati 781039, India

ARTICLE INFO

Article history:
Received 28 February 2010
Received in revised form
7 August 2010
Accepted 8 August 2010
Available online 30 August 2010

Keywords:
Discrete Event Systems
Failure detection
Network security
Local Area Network (LAN) Attack
Address Resolution Protocol (ARP)

ABSTRACT

Address Resolution Protocol (ARP) is used for determining the link layer or Medium Access Control (MAC) address of a network host, given its Internet Layer (IP) or Network Layer address. ARP is a stateless protocol and any IP–MAC pairing sent by a host is accepted without verification. This weakness in the ARP may be exploited by malicious hosts in a Local Area Network (LAN) by spoofing IP–MAC pairs. Several schemes have been proposed in the literature to circumvent these attacks; however, these techniques either make IP–MAC pairing static, modify the existing ARP, patch operating systems of all the hosts etc. In this paper we propose a Discrete Event System (DES) approach for Intrusion Detection System (IDS) for LAN specific attacks which do not require any extra constraint like static IP–MAC, changing the ARP etc. A DES model is built for the LAN under both a normal and compromised (i.e., spoofed request/response) situation based on the sequences of ARP related packets. Sequences of ARP events in normal and spoofed scenarios are similar thereby rendering the same DES models for both the cases. To create different ARP events under normal and spoofed conditions the proposed technique uses active ARP probing. However, this probing adds extra ARP traffic in the LAN. Following that a DES detector is built to determine from observed ARP related events, whether the LAN is operating under a normal or compromised situation. The scheme also minimizes extra ARP traffic by probing the source IP–MAC pair of only those ARP packets which are yet to be determined as genuine/spoofed by the detector. Also, spoofed IP–MAC pairs determined by the detector are stored in tables to detect other LAN attacks triggered by spoofing namely, man-in-the-middle (MiTM), denial of service etc. The scheme is successfully validated in a test bed.

1. Introduction

The security and performance considerations in any organization with a sizeable number of computers lead to creation of LANs. A LAN is a high-speed communication system designed to link computers and other data processing devices together within a small geographic area, such as a department or building. A security threat to any computer, based on LAN specific attacks is always from a compromised or malicious host in the LAN. The basic step involved in most of these attacks comprises cache poisoning with falsified IP–MAC pairs, which may then lead to other attacks namely, MiTM, denial of service etc. [1].

Computers in the internet are identified by their IP addresses. IP addresses are used by the network layer for identifying the machine uniquely. At the data link layer, computers use another address known as a MAC address or hardware address. It is to be noted that IP addresses can be dynamic and change over time but the MAC address of a computer is constant unless the Network Interface Card (NIC) is replaced. To deliver a packet to the correct machine, the IP address has to be mapped to some MAC address. This dynamic binding (since IP is dynamic) between the IP and MAC address is done by the Address Resolution Protocol (ARP). ARP is responsible for finding the MAC address given the IP address. The data link layer uses the MAC address of the destination machine for sending the packets. If the host sending the packets does not know the MAC address of the destination host, it sends a broadcast request to know "What is the MAC address corresponding to the IP address". The host which has the IP address in the broadcast message sends a unicast reply message to the sender, mentioning its MAC address. In order to reduce the number of broadcast requests each machine maintains a table termed as the ARP cache, which holds the mapping between the IP and MAC. Entries in the ARP cache can be either static or dynamic. In the dynamic cache the entries are erased as they get older than a predefined duration. The problem with ARP is that, it is a stateless protocol. Any host after receiving any ARP response message will update its cache without verifying whether it has earlier sent a request corresponding to the response. This enables the malicious hosts to craft custom ARP packets and forge the IP–MAC pair.

There are number of solutions proposed in the literature to detect, mitigate and prevent ARP attacks. The schemes can be broadly classified as:

* Corresponding author. Tel.: +91 9957561026; fax: +91 361 2692787.
E-mail addresses: neminath@cse.iitg.ernet.in (N. Hubballi), santosh_biswas@cse.iitg.ernet.in, santoshbiswas402@yahoo.com (S. Biswas), roopa.s@cse.iitg.ernet.in (S. Roopa), r.ratti@cse.iitg.ernet.in (R. Ratti), sukumar@cse.iitg.ernet.in (S. Nandi).

0019-0578/$ – see front matter © 2010 ISA. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.isatra.2010.08.003

Static ARP entries [2]: The most foolproof way to prevent ARP attacks is to manually assign static IPs to all systems and maintain the static IP–MAC pairings at all the systems. However, this scheme is not suitable for a dynamic environment.

Security features [3]: One possible action to combat ARP attacks is enabling port security (CIS) on the switch. This is a feature available in high-end switches which tie a physical port to a MAC address. These port–address associations are stored in Content Addressable Memory (CAM) tables. A change in the transmitter's MAC address can result in port shutdown or ignoring the change. The problem with this approach is, if the first sent packet itself is having a spoofed MAC address then the whole system fails. Further, any genuine change in the IP–MAC pair will be discarded (e.g., when notified by Gratuitous request and reply).

Software based solutions: The basic notion of port security involving observation of changes in IP–MAC pairs in switches has also been utilized in software solutions namely, ARPWATCH [4], COLASOFT-CAPSA [5]. These software solutions are cheaper than switches with port security but have a slower response time compared to switches. Obviously, these tools suffer from the same drawbacks as that of port security in switches.

Signature and anomaly based IDS: Signature based IDSs like Snort [6] can be used to detect ARP attacks and inform the administrator with an alarm. The main problem with IDSs is that they tend to generate a high number of false positives. Furthermore, the ability of IDSs to detect all forms of ARP related attacks is limited [7]. Recently, Hsiao et al. [8], have proposed an anomaly IDS to detect ARP attacks based on SNMP statistics. A set of features are extracted from SNMP data and data mining algorithms such as decision tree, support vector machines and Bayes classifier have been applied to classify attack data from normal data. Reported results show that false negative rates are as high as 40%.

Modifying ARP using cryptographic techniques: Several cryptography based techniques have been proposed to prevent ARP attacks namely S-ARP [9], TARP [10]. Addition of cryptographic features in ARP lead to a performance penalty [7] and change the basic ARP.

Active techniques for detecting ARP attacks: An IDS using active detection for ARP attacks sends probe packets to systems in the LAN in addition to observations in changes of IP–MAC pairs.

In [11], a database of known IP–MAC pairs is maintained and on detection of a change the new pair is actively verified by sending a probe with a TCP SYN packet to the IP under question. The genuine system will respond with a SYN/ACK or RST depending on whether the corresponding port is open or closed. While this scheme can validate the genuineness of IP–MAC pairs, it violates the network layering architecture. Moreover it is able to detect only ARP spoofing attacks.

An active scheme for detecting man-in-the-middle (MiTM) attacks is proposed in [12]. The scheme assumes that any attacker involved in MiTM must have IP forwarding enabled. First, all systems with IP forwarding are detected (actively). Then the IDS attacks all such systems one at a time and poisons their caches. The poisoning is done in a way such that all traffic being forwarded by the attacker reaches the IDS (instead of the system the attacker with IP forwarding wants to send). In this way the IDS can differentiate real MiTM attackers from all systems with IP forwarding. There are several drawbacks in this approach, namely huge traffic in the case of a large network with all machines having IP forwarding, assumption of successful cache poisoning of the machine involved in an MiTM attack, cache poisoning (of the machine involved in an MiTM attack by IDS) exactly when the attack is going on etc.

From the review, it may be stated that an ARP attack prevention/detection scheme needs to have the following features

- Should not modify the standard ARP.
- Should generate minimal extra traffic in the network.
- Should not require patching, installation of extra software in all systems.
- Should detect a large set of LAN based attacks.
- Hardware cost of the scheme should not be high.

In this paper, a Discrete Event System (DES) based network IDS for detecting ARP related attacks has been proposed. A DES is characterized by a discrete state space and some event driven dynamics. DES have widely been used for failure detection and diagnosis of large systems like chemical reaction chambers, nuclear reactors etc. [13]. The basic idea is to develop a DES model for the system under normal conditions and also under each of the failure conditions. Following that, a state estimator called a diagnoser (or detector, if only detection of failure is required) is designed which observes sequences of events generated by the system to decide whether the states through which the system traverses correspond to the normal or faulty DES model. This idea has been used to develop host based IDS [14,15], where a sequence of system calls under normal conditions comprises the normal model and the sequence under compromised conditions comprises the failure (attack) model. So, the DES detector acts as the host IDS. A preliminary attempt has been made for network level IDS using the same idea in [16]. The work illustrated theoretically how DES may be applied to detect one type of ARP attack i.e., response spoofing.

The objective of the present paper is to design and implement a DES based network IDS that meets all the desired characteristics of an ARP attack detector (as listed above). Design of such an IDS requires certain extensions over the (classical) theory [13] and techniques which have been used in [14–16]. The basic motivations and the extensions are enumerated below:

(1) In the case of ARP, the DES framework needs to model not only sequences of events but also their time of occurrences. So the DES model used in the proposed technique extends the untimed model [14,15] with time information.
(2) Unlike host based IDS, in the case of spoofing (in LAN attacks) there is no difference in the sequence of ARP events compared to normal situations. To handle this situation, an active probing mechanism is used so that sequences of ARP packets are different under spoofing and normal conditions. It may be noted that the probing technique maintains the standard ARP.
(3) Active ARP probes generate extra traffic in the network. To minimize additional traffic, IP–MAC pairs corresponding to normal and spoofed conditions (decided by the detector) are recorded in tables. Following that, ARP probes are sent only to IP–MAC pairs which are absent in the tables. Interfacing results of the detector with the ARP probe sending module requires extension of the concept given in [16].
(4) Entries in the table are used to verify if spoofing leads to other attacks like man-in-the-middle and denial of service etc. Detecting attacks other than spoofing requires enhancement of [16].

The proposed network IDS based on failure detection theory of DES [13] has the following salient features

(1) Follows standard ARP and does not violate the principles of network layering structure.
(2) Generates minimal extra traffic in the network, as probes are sent only for unverified IP–MAC pairs.
(3) It involves installation of the DES detector (based network IDS) in just one host in the network.
(4) Detects a large set of LAN attacks namely, malformed packets, response spoofing, request spoofing, man-in-the-middle and denial of service.