2004

Distributed Hybrid Agent Based Intrusion Detection and Real Time Response System

Vaidehi Kasarekar
University of Nebraska - Lincoln

Byrav Ramamurthy
University of Nebraska - Lincoln, bramamurthy2@unl.edu

Digital Object Identifier: 10.1109/BROADNETS.2004.33

Distributed Hybrid Agent Based Intrusion Detection and Real Time Response System

Vaidehi Kasarekar and Byrav Ramamurthy
University of Nebraska Lincoln
Email: {vaidehi, byrav}@cse.unl.edu

Abstract

Wireless LANs are growing rapidly and security has always been a concern. We have implemented a hybrid system, which will not only detect active attacks like identity theft causing denial of service attacks, but will also detect the usage of accesspoint discovery tools. The system responds in real time by sending out an alert to the network administrator.

1. Introduction

WIRELESS LANs using the IEEE 802.11 protocols are being deployed widely. With this increasing popularity in Wi-Fi, security has become a major concern. Until now WLANs have encountered threats such as unauthorized access to network resources, installation of rogue access points and illegal sniffing [1]. We refer to these as classical security threats. Today in addition, active and advanced attacks like MAC spoofing or Denial of Service attacks are more prevalent. Wardriving also pose a major security risk. [2].

1.1. Our Contribution

We have designed and implemented (DH-ABIDERS), which is a combination of Signature and Anomaly based Intrusion Detection System (following the classification in [3] for wired networks). DH-ABIDERS stands for Distributed Hybrid Agent Based Intrusion DEtection and Real time Response System. To summarize, we have designed and implemented a system, which uses

1. Anomaly Based Model to detect identity theft
2. Signature Based Model to detect wardriving.
3. *LanScan* - monitor wireless LAN and to detect installation of Rogue Access Points.

2. Related Work

AirTraf (Now Elixar) [4], AirDefense [5] are examples of software solutions for 802.11 security threats. AirTraf is used to discover problems in the WLAN. AirDefense provides solutions for intrusion prevention by using an anomaly detection system. These tools are not comprehensive enough to detect wardriving, identity theft and installation of network misconfigurations. There is a similar ongoing work being carried out by researchers at the University of Minnesota, Twin Cities [6]. Like DH-ABIDERS, Ajanta uses the "Sequence Number Analysis" technique to detect MAC layer spoofing attacks. We unlike Ajanta, extend this technique to ICMP augmentation to Sequence Number Analysis, for decreasing the number of false positives.

3. Design and Implementation

3.1. Architecture

Consider a cell, which can be thought as an area where one WLAN is deployed. Each cell also has a centralized agent. This agent is responsible for:

1. Data collection - Scanning of the cell activity.
2. First level data analysis.
3. Updating information with central administrator.

All these cells come under a central administrator. It is responsible for:

1. Interpreting data passed by cell agents.
2. Second level data analysis
3. A response system if intrusion is detected.

Figure 1 shows agents and the central administrator.

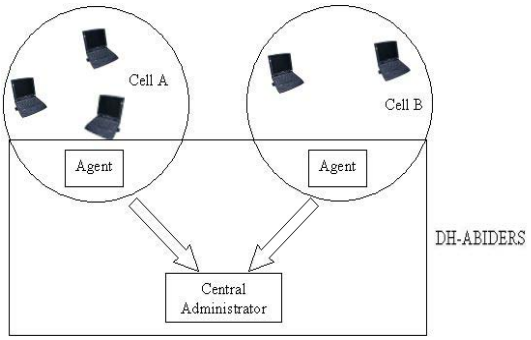

Figure 1. Cells, Agents, Central Administrator.

3.2. 802.11 Attacks

As shown in Figure 2, we have broadly classified wireless attacks as Active and Passive attacks. Installation of network misconfigurations like rogue access points cannot be classified into passive or active attacks. Identity theft (impersonification) attacks are further classified according to the techniques used: Packet insertion technique and application layer techniques. Passive attacks can be classified into illegal sniffing and wardriving. Wardriving is discussed in section 3.6.

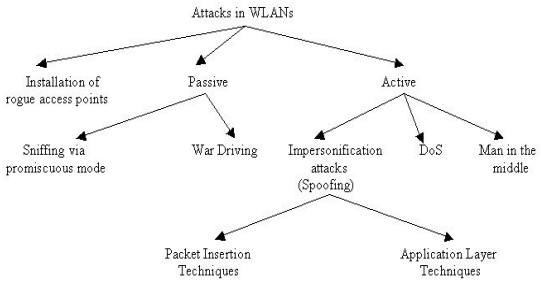

Figure 2. Classification of attacks dealt with.

3.3. Intrusion Approaches

Many WLANs today rely on MAC address as an authentication entity. While this provides a low level of security, there are many security breaches.

Our first approach is based on impersonification of MAC address. An attacker can modify the manufacturer assigned MAC address of the wireless card on the fly and thus the identity of any user.

A second approach is based on the fact that 802.11 management frames are neither encrypted nor authenticated. Using open source libraries like AirJack or Radiate, attackers can inject malicious 802.11 frames in the network.

Libnet [7] is widely used as a packet insertion library for wired networks. However it does not provide an interface to inject 802.11 frames. Radiate provides 802.11-frame creation and injection APIs. They are based on HostAP [8] drivers. HostAP is driver for Intersil's Prism2/2.5/3[9] chipset wireless LAN cards.

We used Radiate library for injecting malicious frames in the network. After installing and configuring the wireless card with HostAP, we wrote a program to impersonify the identity of the access point of the network and then continuously inject disassociation frames. As an effect of this attack, all the other clients connected to the access point got continuously kicked off from the network.

3.4. Detection Approach

We use MAC Layer Sequence Number Analysis Technique [10] to detect the above-described active attacks. We also improve on this to minimize number of false positives generated by this technique as described in Section 3.5. The 802.11 standard has set aside 2 bytes for sequence control. 802.11 frames have a 12-bit sequence number and a 4-bit fragment number in the sequence control field. We can use this sequence number to detect such attacks. The frame structure of 802.11 is as shown in Figure 3. The sequence number is a 12- bit number and is generated by the firmware of the NIC card. The sender NIC, increments the sequence number, with every frame it places on the physical layer.

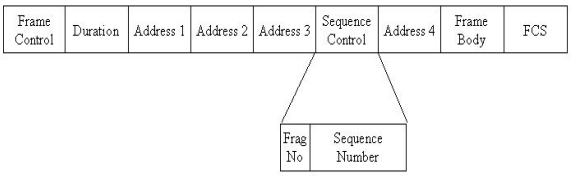

Figure 3. IEEE 802.11 frame structure.

Consider an attacker spoof his wireless NIC card using the techniques described in section 3.3. During this time, the legitimate user is unaware of the attackers intentions. Thus at any given point during the attack, the DH-ABIDERS agent will discover 802.11 frames which seem to have same MAC address and IP address; the addresses of the attacker and the legitimate user; however the order of sequence numbers would be notably different.

Moreover attacker does not have facility to change any sequence numbers on the fly because no NIC driver can handle sequence number functionality. Reason why NIC driver cannot handle this functionality is that, the fragmentation of frames is carried out by the NIC firmware. Fragments of the same frame need their sequence numbers to remain the same. Thus the NIC firmware will allocate sequence numbers according to the MTU of the physical link and the frame length.

3.5. ICMP Augmentation to Sequence Number Analysis

Intrusion Detection systems should minimize the number of false positives. To reduce these false positives generated, we propose an interesting extension called "ICMP Augmentation." It is based on the principle that, when an attacker tries to steal the identity of a legitimate user, by spoofing his/her MAC address, the attacker will certainly obtain the IP address of the legitimate user. Thus for a single IP address, there would be two NICs responding and thus can conclude malicious spoofing.

3.6. Detection of AP Discovery Tools

Wireless LAN discovery tools such as NetStumbler are designed to identify network characteristics. Wardriving takes advantage of 802.11 standards being open. The 802.11 framework has described active probing method, which uses probe request frames to detect wireless activity.

Our system detects the usage of AP Discovery tools like NetStumbler. Upon detecting the use of such a tool, the system sends an email to the system administrator and saves the packet log as evidence. A unique signature pattern of NetStumbler frame as described in [11] is used to detect this.

3.7. Summing up

As shown in Figure 4, agent has two modules-The sniffing module and the Parsing and Detection module. The sniffing module spawns as many agent threads as the number of clients, each representing a sniffer for every client of the WLAN.

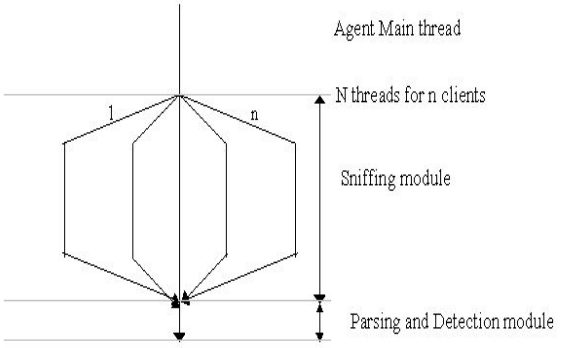

Figure 4. Process model of agent in DH-ABIDERS.

Parsing and Detection module:

1. Parses the verbose output of the sniffing module
2. Implements Anomaly based analysis model to detect identity theft and DOS attacks.
3. Implements Signature analysis model to detect wardriving.
4. Submits the anomaly-based analysis results to the central administrator to perform a second level analysis – ICMP Augmentation.

We have thus developed a Hybrid Real Time Agent Based Intrusion Detection and Response System to increase the security in wireless networks. The system is implemented and tested successfully. The system utilizes open source solutions, thus minimizing deployment and maintenance costs to a large extent

Figure 5 shows how the two models are used to detect the attacks, classified in Figure 2.

An interesting extension can be the integration of honeypots [12] with DH-ABIDERS. A significant improvement, is to integrate the current system with a more robust anomaly detection engine, which can analyze the captured data for signs of intrusions, using techniques such as data mining and statistical approaches for Intrusion Detection. Work has been done in [13] related to this.

Detailed information about this work is available in [14].

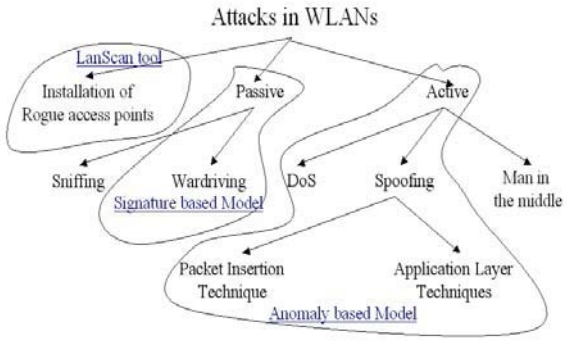

Figure 5. Models in DH-ABIDERS.

4. References

[1] W. Arbaugh, W. Shankar, Y. Wan. "Your wireless network has no clothes". Proceedings of International Conference on Wireless LANS and Home Networks. March 2001.

[2] Wardriving http://www.wardriving.com. August 2003.

[3] B. Mukherjee, T. Herberlein and K. Levitt. Network Intrusion Detection. IEEE Network. Pages 26-41. May-June 1994.

[4] AirTraf. http://www.elixar.com/. August 2003.

[5] Wireless LANs: Risks and Defenses. A whitepaper. AirDefense http://airdefense.net/ August 2003.

[6] S. Karanth and A. Tripathi. Wireless Network Monitoring. University of Minnesota Twin Cities. May 2003.

[7] Libnet. http://libnet.sourceforge.net/. August 2003.

[8] HostAP driver for 802.11 for Intersil Prism chipset http://hostap.epitest.fi/. August 2003.

[9] Intersil Prism www.intersil.com Accessed in August 2003.

[10] J. Wright. Detecting Wireless LAN MAC Address Spoofing. Johnson and Wales University. GCIH. CCNA. January 2003.

[11] Mailing List. August 2003. http://www.kismetwireless.net/archive.php?mss:2714

[12] Honeypots. http://www.honeypots.net/. August 2003.

[13] W. Lee and S. Stolfo. "A Framework for Constructing Features and Models for Intrusion Detection Systems". ACM Transactions on Information and System Security.November 2000.

[14] Vaidehi Kasarekar, MS project report, Dept. of Computer Science and Engineering, University of Nebraska-Lincoln, 2003. http://csce.unl.edu/~bhavanal/web/alumnidocs/vaidehi.MS.pdf