2003

Agent Based Intrusion Detection and Response System for Wireless LANs

Mohan K Chirumamilla
University of Nebraska-Lincoln, mohankc@cse.unl.edu

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

ICC '03. IEEE International Conference on Communications, 2003.
Volume: 1 Digital Object Identifier: 10.1109/ICC.2003.1204225
Publication Year: 2003 , Page(s): 492 - 496 vol.1

Agent Based Intrusion Detection and Response System for Wireless LANs

Mohan K Chirumamilla
Department of Computer Science and Engineering
University of Nebraska-Lincoln
Lincoln, NE, 68588-0115 U.S.A.
mohankc@cse.unl.edu

Byrav Ramamurthy
Department of Computer Science and Engineering
University of Nebraska-Lincoln
Lincoln, NE, 68588-0115 U.S.A.
byrav@cse.unl.edu

Abstract— **Wireless LAN technology, despite the numerous advantages it has over competing technologies, has not seen widespread deployment. A primary reason for markets not adopting this technology is its failure to provide adequate security. Data that is sent over wireless links can be compromised with utmost ease. In this project, we propose a distributed agent based intrusion detection and response system for wireless LANs that can detect unauthorized wireless elements like access points, wireless clients that are in promiscuous mode etc. The system reacts to intrusions by either notifying the concerned personnel, in case of rogue access points and promiscuous nodes, or by blocking unauthorized users from accessing the network resources.**

Keywords— ***Wireless LANs, Intrusion Detection, Security, Rogue Access Point, promiscuous nodes.***

I. INTRODUCTION

Security has always been a concern in communication networks as it is in many other areas. The important typical security issues that one should consider are, threats to the physical network, unauthorized access to network resources, internal and external attacks. In the context of wired LANs, the solutions to the above issues are well defined and are fairly reliable. The same approaches, however, cannot be directly adapted to wireless LANs.

A. Security in the Wireless Networks

WEP (Wired Equivalent Privacy) is the security protocol provided in the IEEE 802.11 [8] wireless standard to bring the security in wireless networks comparable to the security in wired networks. Its main objective is to protect the data that is transmitted over wireless links from malicious eavesdroppers. WEP tries to accomplish its goal by encrypting the data that is being transmitted at the MAC layer.

The main scheme that is being employed in WEP is Shared key authentication. Shared key cryptography is used to authenticate and also to communicate with a mobile node. However, studies [1, 2, 4] have proved WEP to be a complete failure. In [1] it has been shown that WEP can be compromised by successfully modifying the data, injecting fake data and decrypting the data. As a result it has been proved that Authentication, Authorization and Accounting (AAA) are all not achieved with WEP. A recent study [4] has shown how packets can be forged in a wireless environment, despite the protection offered by WEP2 (an improved version of WEP which is not yet standardized). Last but not the least, inventors of RC4 encryption algorithm have exposed a weakness in their algorithm, which indirectly has a significant impact on the credibility of its use in wireless environments.

Taking advantage of all the above weaknesses, one could easily break into a wireless network with a minimal setup, a laptop and a wireless card (which allows RF monitoring). To make things worse, this kind of eavesdropping can be carried in a completely passive undetectable mode.

B. Intrusion into WirelessLANs

Intrusion, in the field of networks, is defined as the act of wrongfully accessing the network resources without having appropriate privileges. Intrusion into wireless networks is relatively easier when compared to wired networks. Wireless networks are highly susceptible to intrusion because of the radio technology that is being used. An intrusion into wireless networks can be carried in two ways, either by passively sniffing the wireless network or by physically installing access points on the wired network in unnoticed places.

Passively sniffing the network is the easiest intrusion that one can attempt with just a wireless card and a laptop. The wireless card can be slipped into RFMODE (promiscuous mode) and all the data in the air can be sniffed. Intrusion of this kind is possible if and only if the network has wireless access points installed on the wired network. In the case where the network has inaccessible access points, one can intrude into a corporate network by gaining physical access to the wired network and installing a rogue access point. In either case, the attacks can either be *internal* – attack carried by people within the organization – or *external* – attack carried by people outside the organization. In the latter type of intrusion, it is as simple as passively sniffing the network once the access point is installed.

II. OUR CONTRIBUTION

In our work, we designed and implemented a fully secured agent-based intrusion detection system that detects the presence of unauthorized wireless elements, namely, rogue access points, wireless promiscuous nodes and unauthorized clients. Depending on the kind of wireless element detected, the system would respond accordingly. In the case of the wireless element being a rogue access point or a wireless promiscuous node, the response would be sending the relevant information such as the geographical information, the time when the element was detected, etc. to the concerned personnel. If the wireless element turns out to

This work was supported in part by the U. S. National Science Foundation grant (ANI-0074121) and the UNL MoCoRePro project.

be an unauthorized client, the response would be blocking that client from getting onto the network, thus preventing unauthorized access.

Our solution to protect the wireless network mainly focuses on detecting intrusions as soon as possible and preventing them up to a certain level. Another important aspect of this project is its vendor independence. This solution can be deployed in a fully heterogeneous environment unlike other vendor specific solutions. Other advantages it has over similar tools like Netstumbler [5], Kismet [6] is its ability to gather information about the whole wireless network and communicate back with the central location. One tool that is similar but not the same, is Airtraf [7]. AirTraf is a database-aware software that mainly detects rogue access points across the organization and communicates back to a central server. Our solution is different from AirTraf, by providing extra features like, detecting promiscuous nodes, blocking unauthorized users from accessing the network resources, and providing x.509 certificates to the users of the wireless networks. The x.509 certificates can be used by the wireless network users to protect their wireless data by using a virtual private network (VPN).

So our solution accomplishes all the threes A's (Authentication, Authorization and Accounting) that WEP was supposed to offer, in a completely heterogeneous environment. The rest of the paper is organized as follows. In the section III we will discuss the design issues. In section IV we will discuss the implementation and test bed details. In section V we will discuss the advantages and disadvantages (limitations) and possible future extensions that can be made to the present system. In section VI we conclude our work.

III. DESIGN

One of the main characteristic features of radio is attenuation of the signal with distance. Due to this inherent property of wireless technology, we need to have multiple access points located at various locations to have a reasonable amount of wireless coverage. So given an area where a wireless network has to be deployed, it can be logically divided into cells as shown in Fig 1. Agents are deployed in all the cells and are connected to the wireless back bone as shown in Fig 2.

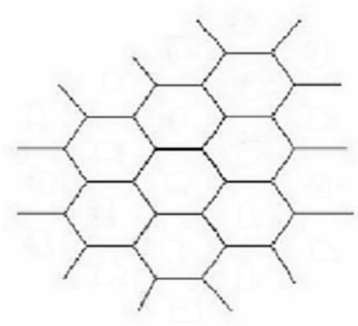

Figure 1 An area divided into logical cells.

In order to provide wireless connectivity in a particular cell, the access point should be connected to the agent (as shown in Fig 2) that also acts as a firewall. The agents, in the absence of access points, act as sniffers, looking for rogue access points and promiscuous nodes in their respective cells. In the case of an access point being present,

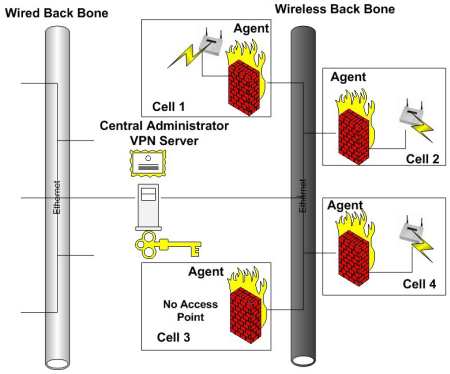

Figure 2 Overview of the architecture.

the agents act as both sniffers and firewalls, to stop unauthorized users from accessing the network resources and to detect unauthorized wireless elements. In the following sections we explore the details of the system by closely examining at the roles played by the agents and the central administrator.

A. *Central Administrator*

The central administrator is the main central server that acts as the centralized-entity to monitor all the wireless cells in the network. It maintains the information of all the access points and agents present on the network. It also maintains the list of all clients which can use the wireless network. Should a new access point or wireless client be installed on the network, it has to be registered with the central administrator; otherwise, it would be considered as an unauthorized element. The central administrator maintains a record for each access point which consists of information about the geographical location it is serving, its MAC address, the name and IP address of the agent present in that cell, status of WEP etc. This information can help network administrators in taking strategic decisions in strengthening the security of the network. In addition to this information it also maintains critical information about the client card like its MAC address and the public key. The following are the functions offered by the central administrator

- Registering and deregistering access points (AP), client cards, and agents;
- Scanning the network;
- Generating x.509 certificates for client cards; and
- Acting as a VPN server for the whole wireless network.

When a wireless element like an access point or a wireless client card, is registered, the central administrator will send the element's information to all the agents. The agents upon receiving this information act accordingly which is discussed in section B. But, registering a client card involves an extra action other than just sending the information to the agents. When a client card is registrered, an x.509 certificate is generated using the information like the MAC address, user name, email address, department etc. This certificate can be used by the wireless client to build a secured tunnel (using IPSec [10]) between the central administrator and the wireless node as shown in Fig 3.

When an agent is registered, the central administrator will add the agent's information, name, IP address and geographical location to its list of other agents' records. This information is used for communicating with the agents. The central administrator can deregister an agent by removing the agent's record from its list of agents.

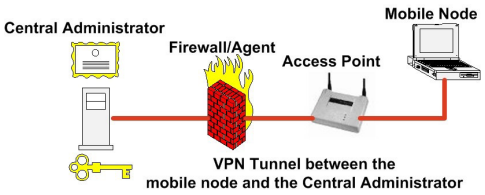

Figure 3 A VPN tunnel between the mobile node and the Central Administrator.

B. *Agents*

Agents are the main building blocks on which the whole system relies. It is the job of the agents to detect unauthorized wireless elements like rogue access points and promiscuous wireless nodes. These agents also act as the first line of defense to protect the network from unauthorized use of the network resources.

Each agent will be equipped with three network interface cards one of which is a wireless interface. This interface is necessary in order to sniff and detect rogue access points. The other two are normal ethernet cards which are used to connect the access point to the backbone (Fig 1). The following are the functions of agents

- Accept registration and deregistration messages for APs and client cards from the central administrator;
- Keep scanning the cell for rogue access points (Those access points that are not registered with the central administrator) and notify the concerned personnel if found;
- Detect promiscuous wireless nodes; and
- Block unauthorized users (those who did not get their card registered with the central administrator).

Each agent maintains a list of registered APs. When a new AP is registered with the central administrator, the central administrator will send the MAC address of the AP to all the agents. The agents, upon receiving the registration, will update their list of authorized APs by adding the new MAC address to their list. Similarly when a deregistration message is received from the central administrator, the corresponding MAC address would be removed from the list of trusted access points. In case of a client card, upon receiving a registration or deregistration message from the central administrator, the agents update their firewall policy to allow or block the user depending on the MAC address of the client card. Some might argue that vendors directly incorporate MAC filtering into their APs. But the main challenge lies in maintaining the list of such allowable MAC addresses in all the APs present on the backbone. There is no centralized solution that can update the list efficiently on all the APs. Using our solution, we register the client card once at the central administrator thus making it easy to maintain the list.

The other two important activities of the agents are, scanning their respective cells for rogue APs and for wireless promiscuous nodes. The agents scan for rogue APs by sniffing for beacon frames emitted by the APs. Each time a beacon is sniffed, the agent compares the source MAC address of the frame with the list of registered access points. If not found in the list of registered users, the agent considers the AP to be a rogue one and sends a message such as an email notification to the concerned personnel. The agents also maintain the list of unregistered APs they find in order to make sure that, they do not start a Denial of Service (DoS) attack by continuously sending out messages for each beacon found.

For detecting promiscuous wireless nodes, the agents use ARP Spoofing [9] to fool the promiscuous nodes. The Agents broadcast fake ARP messages, for all the IP addresses in the subnet that the agent operates in, with fake broadcast address (address that is not a true broadcast address but will be considered as broadcast address [9]). Should a promiscuous node be present in their respective cells, it will respond back with an ARP response (refer to [9] for details). Once the node is detected by its ARP response, the information, like the geographical location, the IP address, and time when the node was seen, will be passed on to the administrator.

IV. IMPLEMENTATION

In this section we discuss the implementation details of how exactly the registration and deregistration of access points, client cards and agents are done. We will also discuss the test bed on which the system has been successfully implemented and tested.

A. *Registration and Deregistration*

Figure 4(a) shows the GUI into which the user has to enter the required information. A copy of the information entered will be stored in a local flat file and another copy will be passed on to all the agents as shown in Figure 4(b).

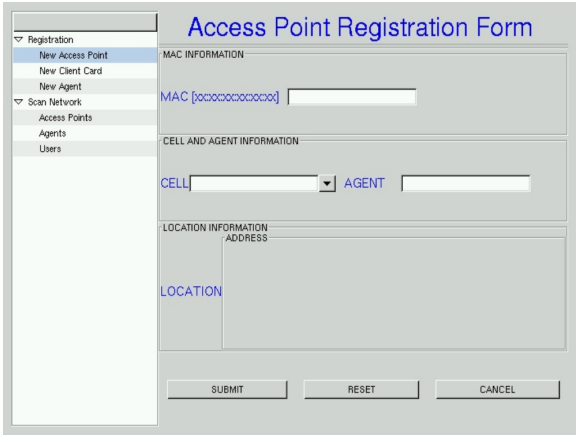

Figure 4(a) Access Point registration GUI.

Once the agents receive this information they will store the MAC address of the AP sent by the central administrator in their lists of registered access points as shown in Figure 4(b). Likewise, when an access point is deregistered, the

central administrator will instruct all the agents to the delete the corresponding information from their lists.

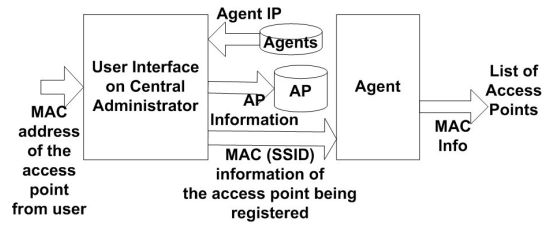

Figure 4(b) access point registration process

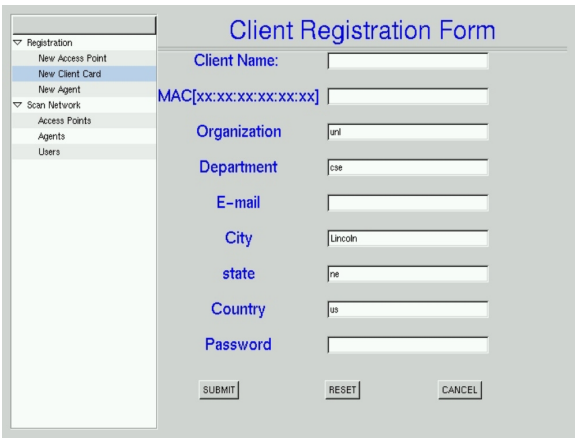

Figure 5(a) Client card registration GUI.

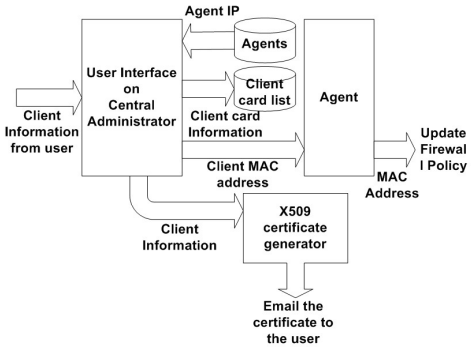

Figure 5(b) Client card registration process.

Figures 5(a) and 5(b) illustrate how the client cards are registered. The user has to enter the required information such as user name, the user's department, etc. into the form shown in Figure 5(a). Once the information is submitted, an x.509 certificate will be emailed to the user of the card. This certificate can be used in implementing a secured tunnel between the user's mobile node and the central administrator. A copy of the user information is stored in a local flat file before sending it to the agent. The agents upon receiving this information update their firewall policies, thus allowing the user to use the network resources. For deregistering a card, the central administrator instructs the agents to update their firewall policies to block the user, based on his/her MAC address, from using the network resources

Figures 6(a) and 6(b) show the GUI and the process for registering agents. Once the information corresponding to a particular agent is submitted, it will be stored in a local flat file and used when registering access points and client cards.

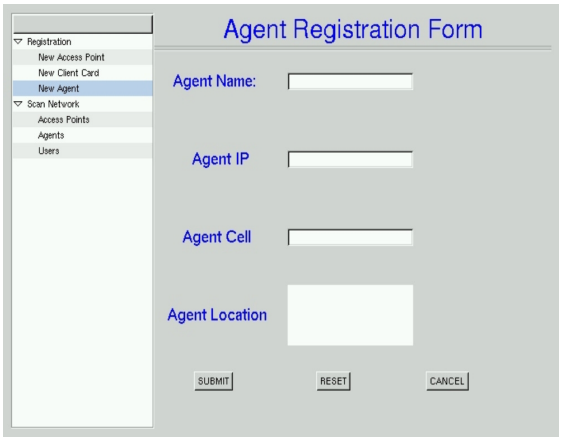

Figure 6(a) Agent registration GUI.

Similarly when an agent is deregistered, the corresponding entry will be deleted from the list of agents.

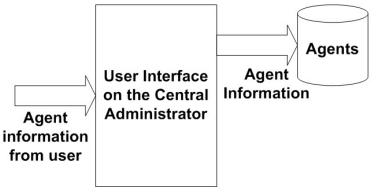

Figure 6(b) Agent registration process.

B. *Detection rogue access points and promiscuous nodes*

The following two figures (Figures 7 and 8) show the pseudo code for detecting the rogue access points and the promiscuous nodes respectively.

```
Begin
sniff for 802.11b beacon frames
if beacon found then
  extract MAC
  if MAC exists in Registered access points list
    Iterate again
  else
    if SSID exists in rogue access points list
      next
    else
      send warning message
      add SSID to rogue access points list
    End If
  End if
Else
  Iterate again
End if
End
```

Figure 7 Procedure for rogue access point detection.

```
Begin
    For each IP in the subnet
      send a fake ARP and wait for reponse
      if response seen
        check log if entry exists;
        if entry exits then
          Iterate again
        else
          send a warning message and log the entry
          Iterate again
        End if
      else
        Iterate again
      End if
End
```

Figure 8 Procedure for promiscuous node detection.

C. *Test-bed*

The system has been implemented on a test bed, which consists of an Orinoco AP 1000 access point, a mobile node (a laptop) and a desktop, as shown in Figure 9. Both the agent and the central administrator are run on the single Linux box. FreeSWAN 1.96 with x.509 patch has been used as a VPN server to provide a secured connection to the mobile clients. For additional details and results refer to [11].

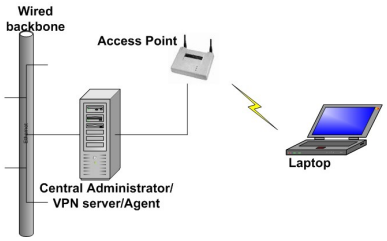

Figure 9 Test-Bed.

V. DISCUSSION

The main goals of the project are, to make the wireless network as secured as possible – using VPN, and to detect intrusions as early as possible. The system has been fully tested for its accuracy and promptness in identifying the intrusions. One of the greatest advantages with our approach is that, the wireless cell to be monitored has no geographical restrictions. As long as the agent is connected to the Internet, the wireless cell can be at any distance from the central administrator. However, there are a few complications and restrictions involved. Every wireless element should be registered with the central administrator in order to be labeled as legitimate. Another limitation on the functionality of agents is its inability to detect a promiscuous node, which is not IP based. Since we use the technique of ARP spoofing, the agent can detect a promiscuous node if and only if that node is associated with a TCP/IP stack. Lastly, the system is meant for IEEE 802.11b networks. Should there be an access point, which does not comply with the IEEE standard, the system will fail in detecting it.

The architecture employed in this project can be used to solve some of the existing problems in IEEE 802.11 networks. One of the most important problems besides security is interoperability between different vendor products. For issues like the handoff mechanism, which does not have any standard defined, different vendors have their own proprietary solutions making it impossible to achieve interoperability. With our proposed architecture, agents can be allowed to transfer the clients between the cells instead of the access points performing the handoff. With this approach we can have access points from different vendors cooperating with one other.

Another interesting improvement that can be made to the existing system is to allow restricted access to unregistered users instead of simply blocking them. Traffic can be analyzed at a corresponding agent each time an unregistered user accesses the wireless network. The results of the analysis can be communicated back to the central administrator, which decides the legitimacy of the user cumulatively using similar information from other agents. Using such a solution, even unregistered users can enjoy the convenience of wireless connectivity with, of course, limited access.

VI. CONCLUSION

Our agent-based intrusion detection and response system has been developed to provide a secured wireless LAN solution. Our main focus is on detecting unauthorized elements as soon as possible. By incorporating the feature to generate x.509 certificates, a VPN solution can be easily deployed to overcome the shortcomings of WEP. The architecture proposed here can serve as a building block for finding efficient solutions for various other problems discussed earlier. Since the whole project involves open source tools, the cost for deploying such a system is very minimal.

References

[1] I.N. Borisov, I. Goldberg, D. Wagner. Intercepting Mobile Communications, In Mobicom 2001, Rome, Italy, Jul. 2001.

[2] A. Stubblefield, J. Ioannidis, A.D. Rubin. Using the Fluhrer, Mantin, and Shamir Attack to break WEP, In Network and Distributed System Security Symposium. San Diego, California, Feb. 2002.

[3] S. Fluhrer, I. Mantin, and A. Shamir. Weakness in the key scheduling algorithm of RC4. In Eigth Annual Workshop on selected Areas in Cryptography, Toronto, Canada, Aug. 2001.

[4] A. Mishra, W.A. Arbaugh. An Initial Security Analysis of the IEEE 802.1X Standard CS-TR-4328, University of Maryland, http://www.cs.umd.edu/~waa/wireless.html Accessed in Aug. 2002.

[5] Netstumbler. A windows tool to scan for available wireless networks. www.netstumbler.org Accessed in Aug. 2002.

[6] Kismet. A linux tool used for scanning wireless networks. www.kismetwireless.net Accessed in Aug. 2002.

[7] AirTraf. A linux tool for gathering information about the available wireless networks. http://airtraf.sourceforge.net/ Accessed in Aug. 2002.

[8] 802.11 Standard http://grouper.ieee.org/groups/802/11.

[9] D. Sanai. Detection of promiscuous Nodes Using ARP packets. A white paper from http://www.securityfriday.com Accessed in Aug. 2002.

[10] IPsec Security Architecture for the Internet Protocol http://www.ietf.org/html.charters/ipsec-charter.html.

[11] Mohan K Chirumamilla. M.S Project report, Dept. of Comp. Sci. & Engg., University of Nebraska-Lincoln, 2003. http://csce.unl.edu/~mohankc