NRC·CNRC

NRC Publications Archive
Archives des publications du CNRC

Security System for Wireless Local Area Networks

Korba, Larry

NRC Publications Record / Notice d'Archives des publications de CNRC:
https://nrc-publications.canada.ca/eng/view/object/?id=7ac4cde7-8605-4098-817e-61457b5a2f4d
https://publications-cnrc.canada.ca/fra/voir/objet/?id=7ac4cde7-8605-4098-817e-61457b5a2f4d

Access and use of this website and the material on it are subject to the Terms and Conditions set forth at
https://nrc-publications.canada.ca/eng/copyright
READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THIS WEBSITE.

L'accès à ce site Web et l'utilisation de son contenu sont assujettis aux conditions présentées dans le site
https://publications-cnrc.canada.ca/fra/droits
LISEZ CES CONDITIONS ATTENTIVEMENT AVANT D'UTILISER CE SITE WEB.

Questions? Contact the NRC Publications Archive team at PublicationsArchive-ArchivesPublications@nrc-cnrc.gc.ca. If you wish to email the authors directly, please see the first page of the publication for their contact information.

Vous avez des questions? Nous pouvons vous aider. Pour communiquer directement avec un auteur, consultez la première page de la revue dans laquelle son article a été publié afin de trouver ses coordonnées. Si vous n'arrivez pas à les repérer, communiquez avec nous à PublicationsArchive-ArchivesPublications@nrc-cnrc.gc.ca.

National Research Council Canada | Conseil national de recherches Canada

Canada

Security System for Wireless Local Area Networks

Larry Korba

National Research Council of Canada, email: Larry.Korba@iit.nrc.ca

ABSTRACT

Security and privacy issues complicate wireless local area network deployment. For a wired network, certain levels of security are maintained since access to the physical medium is restricted to the devices physically connected to the network. Though wireless local area networks offer some built-in security features, security breaches are possible if appropriate precautions are not taken. This paper describes security issues related to wireless local area networks and presents a software approach for restricting and controlling wireless access. The system authenticates users on the basis of identity, privileges and access hardware by distributed software agents that implement security policy and restrict unauthorized access.

1. INTRODUCTION

There has been a dramatic growth in the availability of untethered network connections. Key reasons for the popularity of wireless networks are:

1. The potential for mobility. Wireless portable PCs and PDAs provide mobile workers within buildings access to network resources. These combinations open the doors to new business applications which combine communications and computers for nomadic network access [Pahlavan 95].

2. Lack of cabling and its concomitant problems. Wireless connections offer ad hoc network connection. They may be used to extend wired LANs, bridging two physically separated LAN segments.

3. Rapid network configuration.

This work concerns radio-based wireless LANs (WLANs) that use a bridge to the wired LAN. The techniques and system developed using Digital Equipment Corporation's Roamabout wireless modems and access points (APs) [Digital Equipment url1] are applicable to other wireless modem systems (e.g. Proxim, Breeze Wireless Communications).

Contact Information: National Research Council of Canada, Rm. 286b, Building M-50, Montreal Road, Ottawa Ontario K1A 0R6. (613) 998-3967, FAX (613) 952-7151, Larry.Korba@iit.nrc.ca. NRC Paper #41582.

The system described here provides secured WLAN access using network management techniques. Its distributed approach protects wired network resources from unauthorized wireless access. It offers the following security benefits:

- Authentication of wireless users by name, password, privilege level and WLAN modem ID for a timed access period,

- Controls over who is allowed to change operating parameters of the WLAN access points,

- Bolsters security for WLAN modems irrespective of IEEE 802.11 compliance and

- Provides automatic Security Policy management.

This paper is divided into three major sections. The rest of this section provides background information on the security exposure of WLANs and related work in the area. Section 2.0 provides a description of the system. The conclusions summarize the work.

A. RF Wireless LAN Security

It is difficult to completely control the coverage of a WLAN access node. There is always the possibility that someone within the operating range of a WLAN modem or APs may gain access to network resources or may tap into the wireless communications of others. Organizations now experience wireless networking solutions as a security tender spot [Wood 95].

Key to the successful deployment of WLAN technologies has been the development of the IEEE 802.11 WLAN standard. The standard specifies a single Media Access Control (MAC) sublayer and 3 Physical Layer Specifications: one for infrared (IR) and two for radio frequency-based communication. The two physical layers for RF (in the US ISM band) are Frequency Hopping Spread Spectrum and Direct Sequence Spread Spectrum. Both RF types have been commercially deployed in the 915 MHz band and 2.4 GHz ISM bands. RF systems have been more popular than IR systems within buildings because of their range and the ability of the RF signal to penetrate walls. Two computers, each equipped with a wireless LAN modem, may communicate in a point-to-

point fashion over a range of 100 m in an open area. Communication rates as high as 2 MBPS are commonplace with current market units. Others have analyzed the performance of different transmission techniques in a typical office environment [Falsafi 96].

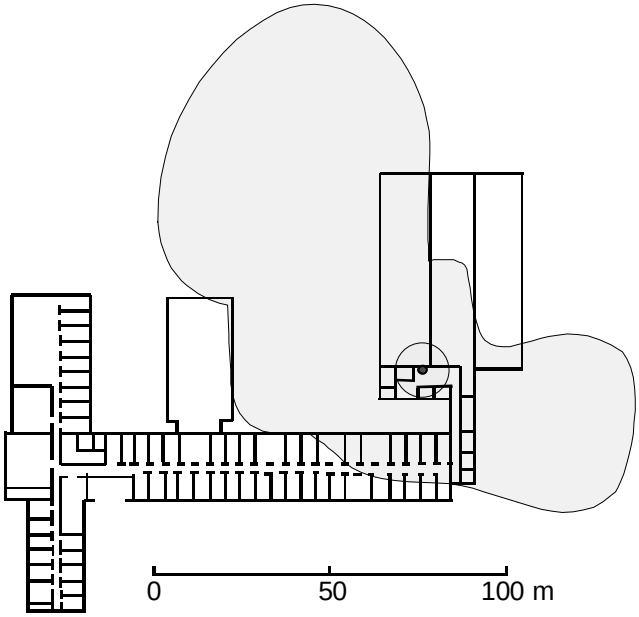

Figure 1. Coverage for a DEC Roamabout ISM band modem used in our experiments. Located on the second floor, the Access Point connected to the LAN is located at the center of the circle.

Figure 1 illustrates the coverage for the DEC Roamabout ISM band modem equipped with a standard antenna. One WLAN Access Point is located at the center of the circle. Although extending coverage to the outdoors benefits the nomadic user, it also exposes the network to intruders. Here the AP provides up to 2 MBPS access to the wired LAN within the shaded coverage area.

Lanthrop noted that it is difficult to capture and interpret spread spectrum transmissions without specialized equipment [Lanthrop 92]. The reality is that the only specialized equipment required is a single wireless modem of the correct make with a typical cost of a few hundred dollars. Two hardware provisions offer some protection from unsolicited access to a WLAN. One of them is a parameter that allows the operation of several wireless subnetworks in the same area. For the Roamabout system the register is called Domain Identification (ID). An intruder would have to select the correct Domain ID to connect to the network. The length of the Domain ID registers is only 16 bits. A straight forward search technique may be used to determine the correct setting for connection. As well, the Domain ID setting is available as Management Information Base MIB [Rose 91a] objects accessed via the Simple Network Management Protocol (SNMP) Agent within the WLAN access point. Security provisions in SNMP version 2 for access to MIB objects are very poor [Rose 91b].

The second privacy provision is encryption. The license-free wireless LAN working group responsible for the IEEE 802.11 specification has been sensitive to the issue of security. As part of the specification, there is provision for RC4 encryption at the Media Access Control (MAC) layer. Although this provides some level of data security, brute force methods can break the 40 bit RC4 symmetric encryption key in as little as a few seconds [Schneier 96]. Furthermore, the encryption layer becomes a small encumbrance for anyone with inside knowledge [Sharp 94]. In the DEC system, all that is required to learn the encryption key is to inspect the key setting available in the dialog box for the modem driver. As well, the encryption key may be accessed as an SNMP object in the WLAN AP.

B. Other Approaches for Securing Wireless Access

Authentication of wireless users offers a method for ensuring that only those individuals who use the correct user name and password and level of authority may access the requested services. It has been suggested that MIT's Kerberos [Steiner 88] would offer password encryption and authentication while not requiring computationally intensive session encryption [Woods 95]. Bharghavan describes a technique for authentication and encrypting communication with a shared key between communicating parties [Bharghavan 94]. Communicating parties authenticate each other, and communications are encrypted. This scheme ignores media access control (MAC) device addresses (a unique address assigned to each network interface card, or in this case, modem) since their cellular communication system dynamically assigns them.

Aziz and Diffie described another authentication technique for wireless LANs. Their approach employs public-key and shared-key cryptographic techniques to produce privacy and authenticity [Aziz 94]. One benefit of this approach is that the computers operating within this system need not have synchronized clocks. Synchronized clocks for all networked computers is a requirement in MIT's Kerberos and some other authentication systems [Bharghavan 95]. None of these techniques use MAC device addresses or simple network management protocol (SNMP) in securing wireless access.

2.0 APPROACH

This work uses software processes or agents distributed throughout the network and SNMP to secure wireless LAN access. The system may be configured to automate a security policy. For instance, it may automatically prompt users to change passwords when a security breach has been detected or after a period of system use. Another issue addressed by this approach is the lack of security within SNMP v2 [O'Mahony 94]. In the approach described here, elements called node management agents restricts access to key MIB

objects to ensure they are not altered, except through authenticated interaction with the agent system.

A. Agent-based Secured Access for Wireless LANs

Figure 2 illustrates the system. Agents intercommunicate with each other. For the sake of clarity, the lines connecting the agents only partially illustrate the message or information interchange between agents or objects.

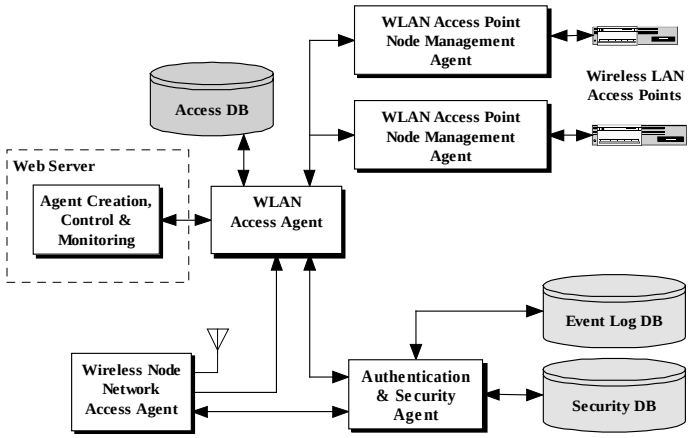

Figure 2. Simplified block diagram of the secured wireless LAN access system.

The system controls access to the wireless LAN by:

1. Forcing authentication of wireless network users and security system operators,

2. Detecting the MAC address of the network interface cards (NICs) connected to the wireless side of any access point,

3. Controlling which NIC may access the LAN, and

4. Logging and displaying access events.

The system uses a web-based interface and Java applets to deploy agents, and to control and to display the system in operation.

The prototype system is comprised of the following agents:

· Wireless LAN Access Point (WLAN AP) Node Management Agent

· Network Access Agent

· LAN Access Agent

· Authentication and Security Agent

The Agent System Creation, Control and Monitoring Block provides a World Wide Web interface to the agent system. It is described in a separate section. Each agent is discussed in turn below.

B. WLAN AP Node Management Agent

The WLAN AP NMA communicates via Simple Network Management Protocol (SNMP) with the SNMP Agent of a wireless LAN access point (Figure 3). This element has two key roles.

· It restricts access to key write-enabled objects of the WLAN MIB. Many objects within its MIB control the operational characteristics of the WLAN access point. The poor security under SNMP version 2, puts the WLAN at risk of an attack. The NMA ensures that only authenticated Network Managers can change important MIB Objects.

· The WLAN AP NMA monitors MIB objects of the WLAN AP which indicate the MAC addresses of wireless LAN devices. Any changes are reported to the LAN Access Agent where a decision is made whether or not to allow a modem to remain connected to the access point. The WLAN AP NMA prevents wireless access by modems with MAC addresses that are not listed in the access database or in cases where a user cannot provide a valid user name and password. Setting filtering objects for the bridge portion of the access point's MIB disables access to a user [Decker 93].

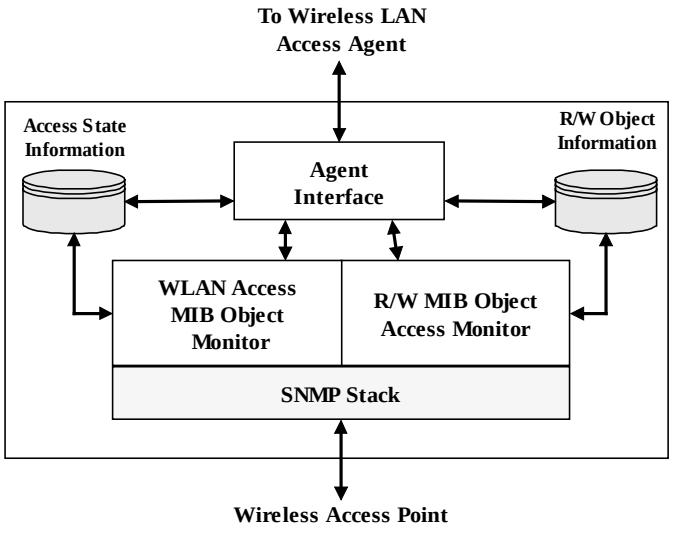

Figure 3. WLAN Access Point Agent Functional Block Diagram.

For this application there is one WLAN AP NMA assigned to each WLAN access point node. WLAN AP NMAs operate on a network element other than the AP since the AP node is a limited function, embedded environment. The WLAN AP NMA is subordinate to the LAN Access Agent. It simply reports events to and responds to commands from the WLAN Access Agent.

C. Network Node Access Agent

This agent resides on every node of the wireless network. It handles user authentication when a mobile workstation connects to the network. A Network Node Access Agent (NNAA) also resides in the Agent System Creation and Control gateways where it authenticates users of the wireless security system. The NNAA is designed and installed on the wireless node in such a way that it cannot be defeated, i.e. without its correct installation and operation, the computer will not connect to the WLAN. A user name and password combination identifies users. All users must first be registered with the authentication server along with their privileges.

Whenever a Network Access Agent successfully connects to the wireless service, the WLAN Access Agent is notified and, depending on settings in the system security policy, its access database may be updated with any changes in MAC addresses associated with the connection. This information offers the provision for the WLAN access system to allow access on a name basis rather than on a MAC Address basis. If authentication fails, the event is logged and the WLAN Access Agent is notified to prevent LAN access for the node.

D. WLAN Access Agent

This agent coordinates activities of the WLAN AP NMAs and communicates with the monitoring and control station. Key functions performed by this agent include:

1. Accesses a database of Ethernet (MAC) addresses allowed to connect with the WLAN or from where management applets may be executed.

2. Acts upon rules associated with the security policy of the organization for the wireless LAN. For instance, MAC addresses may be ignored and only user authentication may be used for network access. If a user does not authenticate properly after three tries, the MAC address associated with the user is disabled for a period of time.

3. Acts as an information concentrator between the WLAN AP NMAs and the Agent Control and monitoring function. As a user moves between access points within a subnetwork,

One LAN Access Agent is assigned per sub-network of a network. The situation is illustrated in Figure 4. Besides the benefit of application and resource partitioning, this arrangement minimizes traffic across network hubs, bridges and routers.

E. Authentication and Security Server

The Authentication and Security Server is a trusted server which authenticates participants and provides contract certificates at the initiation of the following services:

· When wireless network users log into the network,

· When a user attempts to operate the network management interfaces.

Authentication is based on user name and password and MAC address access privileges. It is accomplished using a conventional interchanges for authentication involving password encryption and a 64 bit key [Schneier 96]. Future implementations will use Photuris Session Key Management Protocol [Karn 97]. Authenticated services have a contract, which expires after a period of time, depending on user privileges. Message interchanges with the WLAN Access Agent determine whether or not a particular user and MAC address is allowed connection. All authentication attempts and all contract expirations are logged in the Event Log database.

F. Agent System Creation, Control and Monitoring

The block diagram in Figure 4 shows the component parts of this block. An Agent Daemon provides an operating environment and services for the agents at target nodes throughout a network. One of the services provided by the Agent Daemon is a World Wide Web (WWW) Access gateway. This provides a web-based interface to the agent environment acting as a communication gateway between:

1. The WLAN security agent system,

2. The facilities of a web server, and

3. The Agent Creation, and Control and Monitoring functions supported by Java applets served out by the web server.

This block mediates secure distribution and operation of the agents. Key technologies in this process include: single hop agents, secure agent storage, digital signing of agents, agent authentication based upon agent role within the agent system, agent access restrictions based upon role, secure sockets for inter-agent communication. A detailed description of these technologies is beyond the scope of this paper.

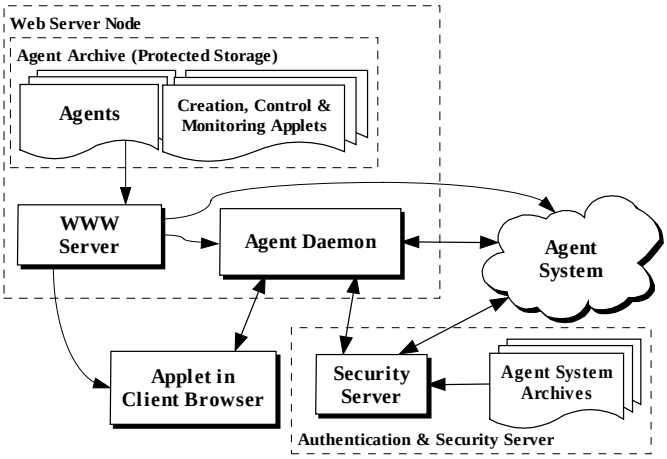

Figure 4. Component Block diagram of the Agent System Creation, Control and Monitoring block. The dashed arrows indicate paths for distribution of agents and applets.

There are two main types of applets used by the system: agent system creation applets and agent system monitoring applets. Agent system creation involves the following steps:

· Assembling pre-built agents required for an agent system.

· Interconnecting agents to form agent systems and,

· Dispatching agents to target Network Nodes.

The prototype uses predefined agents and agent systems for different applications. The agents are distributed to target nodes on an agent-by-agent basis. Agent systems are presented as text-based lists, associations with target nodes are made using tables.

3.0 CONCLUSIONS

This paper presents a distributed system designed to secure wireless LAN access. The multi-agent system provides a World Wide Web interface to assemble, deploy, control and monitor agents operating on different network nodes. This approach offers the following benefits:

1. Users (wireless users and network managers) are authenticated on the basis of identity and MAC address,

2. The system bolsters access security of WLAN modems, whether or not they are IEEE 802.11 compliant,

3. It provides improved SNMP security by way of preventing any unauthorized changes to sensitive write-enabled objects for Access Point MIBs.,

4. Automatic Security Policy Management,

5. Multiple agents distributed across subnetworks to reduce network traffic.

The system will detect and attempt to authenticate any user whose wireless modem negotiates communication through a wireless LAN access point. Unauthorized peer-to-peer communication between wireless modems is not prevented. The objective is to protect the wired network resources from rogue wireless users.

4.0 ACKNOWLEDGMENTS

The author wishes to thank Mansour Toloo Shams for his initial assistance with the literature search, and Sieu Phan for his most appreciated comments during the development of this work.

REFERENCES

[Aziz 94] A. Aziz, W. Diffie, Privacy and Authentication for Wireless Local Area Networks. IEEE Personal Communications, Vol. 1, No. 1, 1994, pp. 25-31.

[Bharghavan 94] V. Bharghavan, Secure Wireless LANs. Proceedings of the 2nd ACM Conf. on Computer Communications Security, 2-4 Nov., 1994, Fairfax, VA, pp.10-17.

[Decker 93] E. Decker, P. Langille, A. Rijsinghani, K. McCloghrie, Definitions of Managed Objects for Bridges, RFC 1493. July, 1993.

[Digital Equipment url1]
http://www.networks.digital.com:80/dr/wireless/

[Falsafi 96] A. Falsafi, K. Pahlavan, G. Yang, "Transmission Techniques for Wireless LANs', IEEE Journal on Selected Areas in Communication, Special issue on Wireless LANs, pp 477-491, April 1996.

[Karn 97] P. Karn, W.A. Simpson, Photuris: Session Key Management Protocol. Network Working Group Internet Draft, July, 1997.

[Lanthrop 92] D.L. Lanthrop, Security Aspects of Wireless Local Area Networks. Computers and Security, 11, 1992, pp. 421-426.

[O'Mahony 94] D. Mahony, Security Considerations in a Network Management Environment. IEEE Network, Vol.8, No. 3, May-June 1994, pp. 12-17.

[Pahlavan 95] K. Pahlavan, T. Probert, M. Chase, "Trends in Local Wireless Networks", IEEE Communications Magazine, Vol. 33, pp. 88-95, March 1995.

[Rose 91a] M. Rose, K. McCloghrie, Concise MIB Definitions, RFC 1212. March, 1991.

[Rose 91b] M. Rose, "The Simple Book, An Introduction to Management of TCP/IP-Based Internets." Prentice-Hall, New Jersey, 1991.

[Schneier 96] B. Schneier, "Applied Cryptography." John Wiley & Sons, 1996.

[Sharp 94] R.L. Sharp, S.R. Eisen, W.E. Kleppinger, M.E. Smith, Network Security in a Heterogeneous Environment. AT&T Technical Journal, Vol. 73, No. 5, 1994, pp. 52-60.

[Steiner 88] J. Steiner, C. Neuman, J.I. Schiller, Kerberos: An Authentication Service for Open Network Systems. Proceedings of the Winter USENIX Conference, Dallas, 1988.

[Wood 95] C.C. Wood, Wireless Network Security. Proceedings of COMPSEC International 95, 25-27 Oct., 1995 London, UK, pp.303-8.