Securing Wireless LAN Access : A Network Management Approach

Korba, Larry

Securing Wireless LAN Access: A Network Management Approach

Larry Korba, National Research Council of Canada

***Abstract*—Although the IEEE 802.11 specification has gone a long way towards providing some level of security for wireless LAN transactions, there are still some security holes. This paper describes several security issues with current Spread Spectrum wireless LANs and describes a system, based on a network management approach, for securing wireless LAN access.**

I. Introduction

Security issues complicate wireless local area network (WLAN) deployment. With a wireless medium, it is difficult to ensure that WLAN access is restricted to only authorized individuals. Even though the IEEE 802.11 WLAN standard has been helpful for successful deployment, radio frequency wireless modem implementations under this standard offer little impediment to WLAN access by anyone with either inside information or knowledge of the technologies. For instance, with appropriate equipment, the 40 bit RC4, MAC layer encryption may be broken in as little as a few seconds [1]. For some WLAN equipment, encryption keys are accessible to any user either via the network or via a control panel dialog box. Wireless LAN access points extend wireless vulnerability into the wired network. Anyone with a computer equipped with a properly configured WLAN modem may gain access to network services through a WLAN access point. Simple Network Management Protocol (SNMP) agents operating in the access points provide a flexible means for controlling and monitoring Wireless LAN operations. On the other hand, the poor security of currently deployed versions of SNMP [2] leave WLAN access points open to denial of service attacks and unauthorized service accesses.

II. Securing Wireless LAN Access

Authentication of and certificate distribution to users of network services has been an effective method for securing wired network access for some time [3]. The system described in this paper uses authentication in combination with network management techniques to secure WLAN access. It provides the following security benefits for WLAN networks with wired network bridges (WLAN access points):

1. Access to the SNMP agent for WLAN access points is restricted to only authorized administrators.
2. Wireless users are authenticated by name, password, privilege level, WLAN modem identification for a timed access period.
3. The system secures ISM (802.11 compliant) as well as 915 MHz spread spectrum radio modems.
4. Security Policy Management may be automated.

A network of intercommunicating software agents furnishes this functionality. Currently being implemented in the Java programming language, the system provides a web-based user interface. Each software agent has specific functions within a hierarchical, inter-agent relationship. A secure server authenticates: wireless LAN users, system managers and system agents for access to network resources. Node management agents (NMA) protect WLAN access points against unauthorized accesses. NMAs also monitor WLAN modem connections to the WLAN Access Points via the SNMP agent of the access points to challenge newly-connected users. The NMA restricts unauthorized access to the wired network by changing filter objects of the WLAN access point. Users may be certified on the basis of authentication and MAC identification of WLAN or network interface cards. Depending on organizational security policy, access may only be allowed to wireless modems which have been previously registered with the system. An alarm message notifies system administrators of any unauthorized access via the WLAN or to the security system.

III. References

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

[2] M.T. Rose. The Simple Book: An Introduction to Management of TCP/IP-based Internets. Prentice Hall, New Jersey, 1991.

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

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, email: korba@iit.nrc.ca. NRC Paper # 41580.