무선 네트워크망의 정보보호를 위한 시스템 설계

김정태[*] · 정승민

[*]목원대학교 · 용인송담대학

Security Design of Information Security for Wireless Local Area Network

Jung-Tae Kim[*] · Sung-Min Jung

Mokwon University, Yongin Songdam College

E-mail : jtkim3050@mokwon.ac.kr

요 약

무선 통신망의 데이터를 보호하기 위한 암호화의 방법 및 비밀 통신을 위한 인증 메카니즘에 대한 방법을 제안하였다. 무선 통신망의 경우 기존의 유선망에 비해, 설치, 이동성 등이 우수하여 많은 기술적인 발전을 보이고 있다. 따라서 이에 대한 데이터의 보호에 대한 관심이 고조되고 있다. 본 논문에서는 가정, 사무실, 건물과 같은 전형적인 외부 환경에 대해 정보를 보호할 수 있는 시스템의 구조를 설계하여 제안하였다.

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.

Key Words

WLAN, Security

I. Introduction

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

- The potential for mobility. Wireless portable PCs and PDAs provide mobile works within buildings access to network resources. These combinations open the doors to new business applications which combine communications and computers for nonmadic network access.
- 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.
- Rapid network configuration

This paper concerns rs아-based wireless LANs that use a bridge to the wired LAN. The techniques and system developed using Digital Equipment Corporations Roamabout wireless modems and access points are applicable to other wireless modern system. The system described 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. It provides automatic security policy management[1,2].

Ⅱ. Configuration of Architecture

This paper uses software process 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. In the approach described, 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.

2.1 Design Consideration

It was decided that this paper focus on protecting communications on the WLAN and that sniffing on the wired LAN was a smaller threat. The wired LAN is assumed to be secure. Thus the system has to provide some means of allowing communications between wireless hosts and hosts on the wired LAN. Wireless hosts should be required to use cryptographic protection, so each wireless host runs a protocol that refuses communication it the packets are not appropriately encrypted from an authenticated host. The wireless hosts not running this protocol may communicate directly without encryption or authentication, but this is impossible to prevent in any case as the user may always boot host in whatever system configuration is desired. Communication with hosts on the wired LAN is only possible through Raylink Access Points(APs), which act as bridges between the wired LAN and the WLAN. In order to prevent inadvertent broadcast of encrypted data over the WLAN, and to prevent wireless hosts from being able to communicate with wired hosts without encrypting their message, a gateway is placed between each AP and the rest of the wired LAN. The gateway enforces the requirement to encrypt messages over the WLAN, and so wireless hosts must obey the rules to gain access to the resources on the wired network. A major consideration in the design is the layer at which the information is cryptographically protected. With sufficiently fast encryption, this may be performed at the link level, the network level. The choice was made to provide the protection at the LSP layer, for the reasons given below. The link level is desirable from the standpoint of transparency and enforcement, but it presents problems in that the data would have to be intercepted and modified in the WLAN interface driver, since the interface card itself has not subject to modification[3,4].

2.2 Agent-based Secured Access for WLANS

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.

The system controls access to the wireless LAN by:

- Forcing authentication of wireless network users and security system operator,
- Detecting the MAC address of the network interface cards connected to the wireless side of any access point.
- Controlling which NIC may access the LAN
- Logging and displaying access events

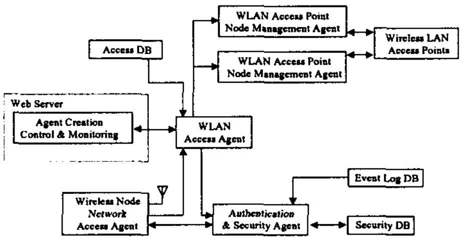
WLAN Access Point Node Management Agent
Wireless LAN Access Points
Access DB
WLAN Access Point Node Management Agent
Web Server
Agent Creation Control & Monitoring
WLAN Access Agent
Event Log DB
Wireless Node Network Access Agent
Authentication & Security Agent
Security DB

Fig. 1 Simplified block diagram of the secured WLAN access system

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 Node Management Agent

- Network Access Agent
- LAN Access Agent
- Authentication and Security Agent

The Agent System Creation, Control and Monitoring Block provides a WWW to the agent system.

2.3. WLAN AP Node Management Agent

The WLAN AP NMA communicate via Simple Network Management protocol(SNMP) with the SNMP agents of a WLAN access point. This element has two key roles. It restricts access to key write enabled objects of the WLAN. Many objects within its MIB control the operational characteristics of the WLAN access point. The poor security under SNMP, puts the WLANN 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 WLAN devices. Any changes are reported to the LAN Access agent where a decision is made whether or not to allies 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.

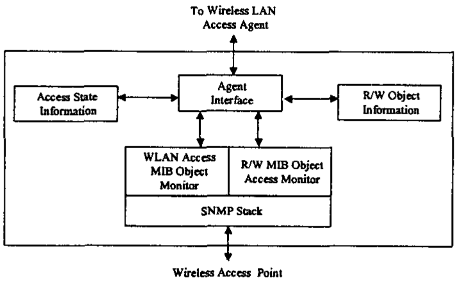

Fig. 2 WLAN Access Point Agent Functional Block Diagram

2.4. WLAN Access Agent

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

- Accesses a database of Ethernet addresses allowed to connect with the WLAN or from where management applets may be executed.
- Acts upon rules associated with the security policy of the organization for the WLAN. 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.
- 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 sub-network.

One LAN access network 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 minimized traffic across network hubs, bridges and routers.

2.5. Agents 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 provides by the agent daemon is a WWW access gateway. This provides a web-based interface to the agent environment acting as a communication gateway between:

- The WLAN security agent system
- The facilities of a web server
- 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.

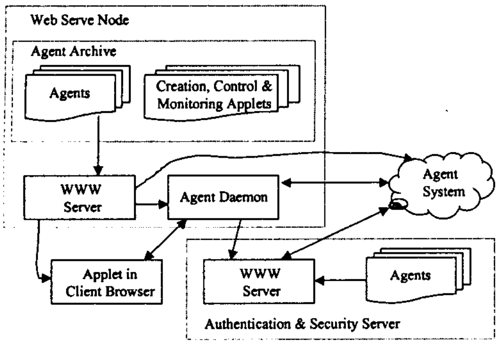

Fig. 3 Component Block diagram of the agent system creation, control and monitoring block. '

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

- Assembling prebuilt agents required for an agent system
- Interconnecting agents to from agent systems
- Dispatching agents to target Network Nodes

The prototype uses predefined agents and agent systems for different application. 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.

III. Conclusions

This paper have presented a distributed system designed to secure WLAN access. The multi-agent system provides a WWW interface to assemble, deploy, control and monitor agents operating on different network nodes. This approach offers the following benefits:

- Users are authenticated on the basis of identity and MAC address
- The system bolsters access security of WLAN modems, where or not they are IEEE 802.11 compliant
- Automatic security policy management

The system will detect and attempt to authenticate any user whose wireless modem negotiates communication through a WLAN access point.

References

[1] A.Aziz et at all, "Privacy and authentication for wireless local area networks", IEEE personal communications, V.1, NO.1, 1994, pp.25-31

[2] A. Falsafi, "Transmission Techniques for Wireless LANN", IEEE Journal on Selected Areas in Communication, Special issue on Wireless LANs, pp.477-491, April 1996

[3] B. Schneir, "Applied Cryptography", John Willey & Sons, 1996

[4] W. Stallings, Data and Computer Communication Prentice-Hall, 1997