IEEE P802.11
Wireless Access Method and Physical Layer Specifications

Title: Security aspects of Wireless LAN standards

Date: February 16, 1993

Author:
Jan P. Kruys
NCR WCND
Zadelstede 1-10
NL 3431 JZ Nieuwegein
the Netherlands
phone +31 3402 76529
fax +31 3402 39125
e-mail jan.kruys@utrecht.ncr.com

I have seen the contributions to the last 802.11 meeting on this subject and I am concerned with the direction being taken in them: technical proposals are being presented and discussed without justification on the basis of user needs. For example, it is considered necessary to perform device authentication but this is not justified in the contributions I have seen so far. Having participated in a number of security standards groups (ANSI X9, ISO SC21 and 27 and ECMA TC32/TG9) I see a need for such justification before we decide what security features to put into 802.11 standards.

This message to the 802.11 members is intended to get the discussion going.

1 Some general notes

The primary objective of making a standard is to define the minimum necessary to meet market needs, not to incorporate what is possible. The specification of security functions in Wireless LANs should be done with this objective in mind.

Like all other systems functions, security should be approached from the user requirements point of view. Another consideration is that "Security" is a broad subject that should be treated from a systems point of view; not just from a subsystem point of view. When discussing wireless LAN security, the whole system, including its network operating system and applications, should be taken into account.

Document 93/2 (IBM) proposes a high level scenario "in the context of the medium access control protocol for wireless LANs..." I have no quibble with the scenario, only with its context: the scenario is a systems scenario and not a MAC level scenario. Similarly, 93/9 (Sun) gives an interesting view on security but fails to indicate what happens at what level in the stack. My contention is that we should avoid going beyond the minimum need AT MAC LEVEL. Systems

integrators should worry about putting complete systems together with the appropriate security features for a given set of customers. Systems integration is not the job of IEEE 802.11.

2. User requirements

User requirements for security in wireless LANs do not differ significantly from such requirements for wired LANs. In both cases, users expect the network to be reliable and not to leak information to third parties and users expect that third parties do not get access to the network. In case of the cable LAN, medium access is controlled to a large extent by the use of cables. Cables tend to keep third parties out and data in. Over and above that, users are authenticated by the network operating system: Novell, LAN Manager and most other NOS do this and users make use of these functions. There are classes of users who require a higher level of security than so provided but they have the choice of adding such capabilities as 802.10 SDE or OSI Network Layer or Transport Layer security functions.

The main difference between wireless LANs and wired LANs is the use of the air medium in the former and any difference in security capabilities needed should compensate for the openness of the wireless medium. All other security required in a system that incorporates wireless LAN technology can be provided by system functions available elsewhere and do not have to be provided by the wireless LANs functions (MAC or PHY). The openness of the air medium requires a confidentiality capability to achieve measure of protection that is equivalent to that of a wired installation.

One might add that in larger organizations there may be a need to logically separate wireless LANs operated under the same "roof". This is a secondary requirement that should be taken into consideration in the design of the key distribution method.

3 Meeting user requirements

One could argue that all security requirements in a wireless LAN based system can be provide by means outside the scope of the MAC and PHY. However, the cost of doing so may well be prohibitive for the majority of [commercial] users. By putting a simple confidentiality service in the MAC or PHY of a wireless LAN, we save the majority of users the cost of adding such a service in the higher layers of their systems. In combination with the user authentication function of the network operating system, an adequate level of protection (for the majority of users) is achieved.

Encryption is the appropriate mechanism for implementing a confidentiality service. Its use implies the provision of key management functions. However, such functions need not and should not be part of a wireless MAC or PHY standard. Instead, key management is an application function that belongs outside the MAC or PHY. See the work of IEEE 802.10 on this subject. What is proper in the MAC or PHY is methods or mechanisms for the selection of keys and the synchronization of their use.

4 Device Authentication

Known user requirements do not point to authentication needs that cannot be solved above the level of the wireless LAN subsystem. Hence there is no need to specify authentication as part of the wireless LAN subsystem standard.

It should be noted that the above is limited in scope to wireless LANs. Other wireless systems such a cellular networks that offer voice services have different requirements because the ability of the systems to function properly and the ability of the system operator to collect revenue depend on the correct operation of the handsets. In such systems, device authentications has a logical place. Wireless LANs are different in that they are privately owned and operated: possibly incorrect device operation has implications for the data transfer function not for revenue collection.

It could be argued that authentication is necessary in order to perform the key management for the confidentiality service. In general this is true but it is not true that real-time device authentication is always needed, nor is it true that this has to be implemented at the same level in the communications stack where the confidentiality is implemented.

In general, one does not distribute keys to users one does not know: the latter must be authenticated first and there are many ways to do this. The authentication can be done off-line, e.g. when the user personalizes his portable he can go to a security administrator and ask for WLAN keys. Another possibility is to use smart cards: users stick their card in their system before going "on-line" at that is all that is needed.

Authentication can also be done on-line, e.g. when a user logs on to the network operating system and gives his password. If that is okay he can be issued with WLAN keys. There are protocols that make this possible without the need to permanently store keys in a device (see Kerberos).

A final note on device authentication: if a station implements an encryption based confidentiality service and it has the appropriate key(s) to talk to other stations, then this is implicit proof of authentication of the user and/or his device having taken place prior to actual communication. This removes the need for explicit transactions to implement (re-)authentication).

5 Placement of a confidentiality service

Conceptually a confidentiality service can be placed in either the PHY or the MAC. The choice between these two options depends on the scope of the keys used in this service.

The PHY does not know about logical partitions of a network. Its knowledge is limited to the characteristics of the radio channel(s) it serves. Therefore, placing the confidentiality service in the PHY effectively links cryptographic keys to radio channels. Since there is no reason why radio channels should map one to one on logical network partitions, placement in the PHY does not support the user requirements outlined above. Another drawback of PHY level confidentiality is that all MAC data would be encrypted; this would deny the option to exchange

clear text data between stations e.g. for the purposes of frame level acknowledgement or key synchronization.

Placement of the confidentiality service in the MAC allows a more flexible approach in which the MAC frame building function can decide which key to use and which data or frames to encrypt.

Finally, it should noted that it will be necessary to device a mechanism to synchronize the use of a given key on a given wireless network or segment thereof.