A clarification of the concerns in IEEE P802.11-93/21.

David Bagby

802.11 MAC group Chairman.
Sun Microsystems Computer Corporation
Office: (415) 336-1631
Email: david.bagby@Sun.COM

This paper hopes to provide clarification regarding the concerns (related to security aspects of wireless LANs) expressed by Jan Kruys in document IEEE P802.11-93/21.

During the January 1993, 802.11 meeting, I presented a paper which explored conceptual information flow within an 802.11 architecture. A portion of this paper touched on the need for support of two services - Privacy and Authentication.

I presented the talk from a set of slides I prepared for the meeting. The slides were handed out during the meeting. This approach works for me as an efficient way to prepare presentations for 802.11. Alas, it does have the drawback that for anyone who has only the slides at hand, it is more difficult to acquire an understanding of the material presented. This is particularly true for anyone who could not attend the presentation.

After I read paper 93/21, it seemed to me that a misunderstanding had occurred about the contents of my presentations. I hope to clear this up with this paper.

Many of the comments in 93/21 are actually in agreement with my own positions regarding security (though from the phrasing, I doubt that the author would have agreed at the time he wrote the document). It is gratifying to know that someone is reading the 802.11 papers, giving the contents consideration and going to the effort to write commentary papers in response.

I believe that I can fairly summarize the main thrusts of document 93/21 as:

1) An assertion that 802.11 features should be justified based on market needs.

2) An assumption that the MAC group has decided to require that the implementation of security services be contained within the 802.11 standard.

3) A recognition that 802.11 must provide services that compensate for the impacts of the media differences between wired and wireless LANs.

Justification based on market needs:

As members of 802.11, we must be aware of market requirements, which if left unfulfilled, might result in a standard with poor commercial success. Each of us does a pretty good job of bringing to light the features and functionality that we believe are required for success within our intended markets. With the diverse set of people and organizations represented within 802.11, this has resulted in some lively discussions.

One key point of my presentations was that we must enable the support of systems which span the range from "unsecured" to "highly secured". While accomplishing this, we must not attempt to impose any particular privacy or authentication scheme. This was stated

explicitly in my slides dealing with both the privacy and authentication service transactions.

My presentation gave examples of networks that were unsecured, based on common password schemes, and networks that made use of sophisticated (public key cryptographic) approaches to security. I asserted that for authentication, a three transaction sequence was sufficient to support this broad range of system types. I explicitly asked if there were any approaches known to the group that could not be supported via the approach presented; I heard of none.

My goal was to provide an approach that would support the range of differing security needs represented by 802.11 members.

While not everyone needs the same levels of security, we must not preclude the ability to provide appropriate security features (for the differing customer requirements) .

Since this portion of my presentation was motivated by the desire to satisfy a broad spectrum of market requirements, I was surprised that 93/21 claimed that "...proposals are being presented and discussed without justification on the basis of user needs".

I agree with the author that justification of features based on perceived market requirements is desirable. I disagree that this is not being done (In fact, Leon from NSA gave a presentation during the January meeting that talked about the security needs of the U.S. government as a customer for wireless LANs).

Assumptions about how and where security services get implemented:

I think that a misunderstanding is centered around how much complexity is perceived to be required within the MAC to support the adopted security services. Much of document 93/21 appears to be arguing that this complexity should not be contained within the MAC layer. Document 93/21 also refers to two other presentations given regarding security (93/8 and 93/2).

I think that this misunderstanding over intent comes about because of the level of complexity which was presented in 93/8. (As I was not involved in the writing of document 93/2 (from IBM) I can not comment on it.)

I realized that the level of sophistication regarding security approaches in the 802.11 audience varied greatly. Thus, I decided that it would be useful for the MAC group to be exposed to an introduction to the subject of security, in order to build an appreciation for how security issues and wireless LANs interact. To this end, I brought Whitfield Diffie to the meeting, who gave a talk based on the slides contained in 93/8.

During my presentations, during my introduction of Whit and his presentation, and after Whit's presentation, I went out of my way to explicitly state that the intent of the

presentations was not to try and place all the details of security as described by Whit into the MAC. I only wanted to raise the awareness level of the group, provide an appreciation of the different approaches to security, and provide background information helpful to understanding the assertion (in my own talk) that providing the three transaction sequence was sufficient to support the identified range of authentication needs.

Unfortunately, while this was done orally three times at the meeting, it was not part of the written slides that were provided as handouts. I apologize for this oversight which I think is the source of some consternation.

My presentations were designed to simply point out that we need to have hooks to appropriate security services within the 802.11 MAC. Since my paper was addressing only the hooks and transactional information flow within an 802.11 architecture required for security services support, I tried to avoid statements about layers or other implementation artifacts.

A large portion of document 92/21 is concerned with making arguments to convince the reader that security and in particular key management (assuming the use of a key based security approach) should not be a part of the MAC. With much of this sentiment I agree; e.g. key management is not something the MAC need be concerned with.

From reading document 93/21, I must have implied that this was the case. I did not intend to do so. I believe that those who participated in the discussions, also do not believe this to be the case, as we spent a significant amount of time talking about what mechanisms were available which we could take advantage of. One resulting action item was to ask 802.10 to provide a tutorial on their work during the March meeting.

Because of this misunderstanding of the intent of the 93/8 and 93/9 presentations, the author of 93/21 went to the trouble to express what he believes to be a dissenting opinion.

Actually, I think the author is mostly in agreement with the sentiment from the last meeting.

Compensating for differences between wired and wireless media:

Within 93/21 it is pointed out that the physical differences between wired and wireless media necessitate that some unique abilities be incorporated into the 802.11 standard.

Document 92/21 states: "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."

From this premise, the author reaches the conclusion that there is a need for support of a privacy service in 802.11 (since the wireless medium does not provide the physical security features inherent to a wired medium).

I believe most of 802.11 agrees with this conclusion. This is shown by the extended discussion held during the January meeting re "should 802.11 adopt a minimal required privacy service which is perceived to be equivalent to wired LANs?". This issue is still under discussion within the group. (Sidebar: Curiously enough, while most recognized the need for a minimal privacy level, very few were willing to commit to it. A fact which I take as support for the position that we must support the entire range from "unsecured" to "highly secured".)

Yet from the same logical starting point, the author of 93/21 concludes that there is no need for an authentication service.

With that conclusion I must disagree.

One of the aspects of wired LAN physical security (which is different in wireless LANs) is the ability to simply establish a physical connection to the network. In wired LANs this is usually reasonably difficult (must first penetrate building security), and can be made very difficult, and reasonably easy to detect (by monitoring the physical medium). In a wireless medium the situation is different - there is no physical impediment to the equivalent of making the wired LAN connection and the connection can be very difficult to detect.

This difference significantly compromises the security of not only the wireless segment, but of any wired segment that is integrated with the wireless segment. Just two of the possible resulting security threats (which are not addressed by a privacy service) are impostor stations and traffic analysis.

On a wired LAN, assertion of the device identity is usually accepted as "good enough". This is an artifact of the assumption that if the network owner cares, he can make it very difficult to establish a network connection without first passing security checks that are not an inherent part of the network operation (ever tried to take a camera or laptop into a secured facility?). With a wireless LAN this assumption is no longer valid; anyone can "connect" without ever entering the facility where the wireless LAN is installed.

Device authentication is the service required to begin to deal with these types of security threats. Without authentication a wireless LAN (and any integrated wired LAN) is required to accept any and all stations - opening the door to impostor station problems (and impostor LANs, which is rather hard to do using a wired medium). While this may be acceptable for some market segments, I can assure you that it is not an acceptable situation for many market segments. I believe that this was recognized by many at the meeting when we adopted authentication as a functional service 802.11 would support.

I strongly disagree with the assertion made in 93/21 that device authentication is totally unnecessary and should not be supported at all.

In recognition of the fact not all wireless LANs will decide to be concerned over these problems (and hence may choose to run unsecured in this respect), I went to some effort to describe an approach that would let each segment use whatever amount of authentication it needed. I was describing an approach which would meet the requirements without requiring all networks to operate in a secured manner.

To ignore device authentication issues would prevent us from satisfying the requirements of significant markets. Perhaps the author took his position because of a misunderstanding of the complexities of authentication between the various permutations of users, networks and devices (while user to user authentication is clearly not within the realm of 802.11, device to device authentication is).

I hope that this paper has helped to clear up the intention of those portions of 93/8 and 93/9 discussed in 93/21 as well as clarifying the discussions held in January re the security aspects of Wireless LANs.