WEP Security Statement
Wireless Ethernet Compatibility Alliance

September 7, 2001

Summary
The recently published approach to compromising WEP is the most effective reported to date. However, Wi-Fi wireless LANs with appropriate security measures are a proven technology that brings significant tangible benefits to large and small businesses, schools, home consumers and many other settings. However, it is important that they be deployed in a manner which is consistent with the same sound security practices used to secure wired LANs and dial-up access connections. The following information should be considered when deploying this or any other network technology. Steps being taken to enhance WEP are also discussed in this document.

1) The acronym WEP stands for Wired Equivalent Privacy. WEP was part of the original IEEE 802.11 standard. From the outset, the goal for WEP has been to provide an equivalent level of privacy as is ordinarily present with a wired LAN. Traditional wired LANs such as IEEE 802.3 (Ethernet) are ordinarily protected by the physical security mechanisms within a facility (such as controlled entrances to a building) and, therefore, IEEE wired LAN standards did not incorporate encryption. Wireless LANs may not be protected by a physical boundary since their transmissions penetrate walls. As a result, WEP encryption was added to the IEEE 802.11 standard to provide an equivalent level of privacy similar to a physical boundary (like a wall).

2) By far, the biggest threat to the security of a wireless LAN is the failure to use any form of security. This is the most significant risk today. WEP should be used as the "first line of defense" to deter the casual intruder. If the value of the data justifies it, other more advanced security techniques should be deployed. For users in smaller organizations, at home, or where the value of the data does not justify extensive additional measures, the Wireless Ethernet Compatibility Alliance (WECA) recommends one or more of the following:

    a) Turn WEP on and manage your WEP key by changing the default key and, subsequently, changing the WEP key, daily to weekly.
    b) Password protect drives and folders.
    c) Change the default SSID (Wireless Network Name).
    d) Use session keys if available in your product.
    e) Use MAC address filtering if available in your product.
    f) Use a VPN system. Though it would require a VPN server, the VPN client is already included in many operating systems such as Windows 98 Second Edition, Windows 2000 and Windows XP.

3) For larger organizations, or those where the value of the data justifies strong protection, users should set up additional security methods. Some examples of these methods are RADIUS -or Kerberos- based access control, end-to-end encryption, password protection, user authentication, Virtual Private Networks (VPN), Secure Socket Layer (SSL), and firewalls. Wi-Fi technology integrates seamlessly with these and other security approaches.

4) IEEE 802.11 Task Group I (IEEE 802.11i) is currently working on extensions to WEP for incorporation within a future version of the standard. The enhancements currently proposed include an entirely different privacy algorithm and provisions for enhanced authentication. The work of Task Group I benefits from the recent papers about RC4 and WEP and will incorporate new mechanisms for dealing with the threats that these papers described.

5) Wi-Fi certification will include requirements for implementing IEEE 802.11i after it is an approved standard. WECA expects to include the new security enhancements from IEEE 802.11i in the next update to Wi-Fi certification testing in 2002.

6) IEEE Task Group I participants and WECA member companies have formed an additional committee whose goal is to develop an interim solution that will be secure against all the known attacks, run on existing Wi-Fi-certified hardware, and be available before the IEEE 802.11i standard is complete.