Wireless Ethernet Compatibility Alliance

802.11b Wired Equivalent Privacy (WEP) Security

February 19, 2001

The Standard for Wireless Fidelity.

A team of researchers at University of California at Berkeley correctly reported ("Intercepting Mobile Communications: The Insecurity of 802.11") a sophisticated methodology that could be potentially used to compromise security of the Wired Equivalent Privacy (WEP) mechanism of Wi-Fi (IEEE 802.11b standard) wireless LAN products. While we welcome this report's contribution to raising the level of awareness related to the importance of wireless LANs security, it has also been the source for misconceptions in the media. WECA would like to clarify these misconceptions and describe the current state of Wi-Fi-based WEP security.

1. Given the goals for Wired Equivalent Privacy, WEP has been, and continues to be, a very effective deterrent against the vast majority of attackers who might attempt to compromise the privacy of a wireless LAN.

2. The goal of WEP is to provide an equivalent level of privacy as is ordinarily present with an unsecured wired LAN. Wired LANs such as IEEE 802.3 (Ethernet) do not incorporate encryption at the Physical or Media Access layer, since they are ordinarily protected by physical security mechanisms such as controlled entrances to a building. Wireless LANs are not necessarily protected by this physical security because the radio waves may penetrate the exterior walls of a building. IEEE 802.11 decided to incorporate WEP into the standard to provide an equivalent level of privacy as the wired LAN by encrypting the transmitted data. If this goal were achieved, then higher layer security mechanisms that were developed for wired LANs would work with no modification on IEEE 802.11 wireless LANs. It is important to emphasize that WEP was never intended to be a complete end-to-end security solution. It protects the wireless link between the client machines and access points. Whenever the value of the data justifies such concern, both wired and wireless LANs should be supplemented with additional higher-level security mechanisms such as access control, end-to-end encryption, password protection, authentication, virtual private networks, or firewalls.

3. The potential attacks on WEP that have been reported in the media are not simple to mount. They are attacks that could be mounted given a high level of sophistication and enough time and money. It is also important to point out the reported attacks appear to require considerable development resources and computer power. It is not clear whether the payoff to the attacker would be adequate enough to spend the time and money required to mount such an attack - particularly given the presence of cheaper and simpler alternative attacks on the physical security of a facility.

4. IEEE 802.11 is currently working on extensions to WEP for incorporation in a future version of the standard. This work was initiated in July 1999 as Task Group E, with the specific goal of strengthening the security mechanisms so as to provide a level of security beyond the initial requirements for Wired Equivalent Privacy. The WEP weaknesses that were described in the UC Berkeley report were identified in Task Group E in October 2000 and solutions that eliminate those potential attacks have already been proposed and adopted as part of the IEEE 802.11e draft. There are additional enhancements currently proposed that are intended to counter extremely sophisticated attacks, including standardizing on a higher layer authentication protocol.

5. We believe that all Wi-Fi certified products will be able to implement the low level IEEE Task Group E enhancements (known as WEP2) through firmware upgrades. It is our belief that this will eliminate most of the weaknesses described. There are other features being proposed by Task Group E such as additional encryption algorithms that may require other changes that are not possible to implement as firmware upgrades. This will vary from vendor to vendor. The schedule for IEEE 802.11e completion or vendor implementation of these upgrades is not clear. Estimates range from 6 to 12 months.

6. Several wireless LAN vendors already have solutions to all of the issues described in the media. WECA and IEEE 802.11 will try to move the entire industry forward so that we have interoperable, standardized solutions to these issues.

7. Contrary to certain reports by the media, the development of WEP, as an integral part of the IEEE 802.11 standard, was accomplished through a completely open process. Like all IEEE 802 standard activities, participation is open to all interested parties, and the 802.11 committee has had a large and active membership from its inception.

8. It has been reported that frequency hopping wireless LAN systems are less vulnerable to security attacks than other wireless LANs. It is WECA's belief that this is not accurate. Current frequency hopping systems transmit the hopping sequence and timing for their network in the clear several times per second. We believe that is it is possible for any compatible off the shelf frequency hopping product to hop along with a system that it is trying to observe. In our opinion, neither frequency hopping nor direct sequence as employed in today's wireless LAN systems has any substantial benefit as a security mechanism.

9. In a home environment, we believe that the likelihood of such an attack being mounted is probably very small, given the difficulty and cost of the attack versus the typical value of the stolen data. Nevertheless, there are other security measures such as personal firewalls that one can use in addition to WEP to enhance the security.

10. By far the biggest threat to the security of any wireless LAN is the failure to use the protection mechanisms that are available, including WEP. Any 802.11 installation where data privacy is a concern should use WEP.