The 802.11w standard will increase the security of 802.11 networks by protecting types of frames that currently leave 802.11 networks vulnerable to attack. Although the 802.11i standard protects data frames from most vulnerabilities, it leaves management and control frames unprotected. Attacks that exploit management and control frames can currently totally disable an 802.11 network, and the forthcoming 802.11k and 802.11v standards will increase the functionality of management frames, potentially creating new vectors of attack. The 802.11w standard extends 802.11i's protections to management frames, further increasing the security of 802.11 networks and negating attacks based on unprotected management frames.

The 802.11w standard will provide protection for management frames by extending the encryption and authentication methods defined in 802.11i to cover these frames, in addition to the data frames that were originally covered by 802.11i. Work on 802.11w started in early 2005, and an official draft is expected to be ratified in the first half of 2008. It is expected to require only firmware and/or driver updates in access points and client devices, not hardware updates. Since 802.11w is still in development, it is difficult to say much about it with certainty, but as of mid-2006, here is what we know.

802.11w provides protection in three categories. The first is for unicast management frames. To protect these frames, 802.11w simply extends the existing encryption algorithms defined in 802.11i—TKIP/RC4 and CCMP/AES—to encrypt management frames as well as data frames. This protects against forged management frames, since an attacker will presumably not have the information required to properly encrypt the frames, and the frames will be rejected by the decryption engine in the station. This also provides confidentiality since the attacker won't be able to decrypt the frames.

The second category is for broadcast management frames. Since these frames typically do not carry as sensitive information as unicast frames, and since encryption of broadcast frames is more complex than encryption of unicast frames, 802.11w protects only against forgeries, not against eavesdropping. The AP distributes a key to the clients via an encrypted connection, and stations can verify whether a management frame was sent from a station that had the key or not, even though the management frame itself is not encrypted. One weakness of this method is that authenticated stations can forge packets to look as though they came from the AP, so an "attack from the inside" is still possible.

Finally, 802.11w has a third category for deauthentication and disassociation frames. For these frames, a pair of one-time keys is used to validate a single deauthentication or disassociation exchange. This method might prevent the previously-mentioned mechanism of allowing a wireless intrusion detection system (WIDS) to use deauthentication frames to kick unauthorized devices off the network. If the unauthorized device supports 802.11w, it might reject the deauthentication frames from the WIDS.

802.11w promises to enhance 802.11's security and protect against more forms of attacks than previous 802.11 security mechanisms. Nevertheless, some holes still remain. 802.11w does not currently seem address the issue of DoS attacks based on control frames, although it may be extended to do so by the time the standard is completed, and few methods exist to prevent attacks based on RF jamming. Even as new technological methods of securing 802.11 networks are developed, it will remain critical to design a wireless network so that it provides the services that it requires and responds robustly to attacks and failures.

A white paper containing more information on DoS attacks in 802.11, the kinds of attacks that 802.11w will prevent, can be found at this URL (not affiliated with Connect802):

http://www-cse.ucsd.edu/~savage/papers/UsenixSec03.pdf