# Security for wireless systems

*Modern hackers are choosing the newest and most vulnerable information system to exploit—the Wireless Local Area Network. Fortunately, it's relatively easy to secure even robust WLANs from those that would cause the most harm. The following steps are fairly generic in terms to wireless networking and will apply to almost all WLANs.*

**Activate the built-in wireless encryption.** Wired Equivalent Privacy was the first attempt at providing some measure of security in wireless networks. Because several free-ware hacking tools are available to "crack" WEP keys, WEP should not be used alone to protect WLANs. Future standards for wireless encryption include Wi-Fi Protected Access (WPA - an enhanced version of WEP) that uses key caching and AES encryption. Currently, DOD and Air Force WLAN security policies provide guidance on using encryption to secure WLANs.

**Update the WLAN interface card and access point software.** Security-conscious manufacturers provide patches to software that fix security issues. Hardware often sits on shelves for weeks and months, and one or more patches may have been created during that time.

**Change the access point default password and WLAN network name, or Service Set Identifier-SSID.** A common step when setting up a WLAN is to change the default passwords/SSIDs on access points. System administrators spend so much time in the setup that they often forget to go back and change these critical settings once the network is running. Some will move back to factory defaults (no security at all) when they are reset.

**Install all WLAN access points in securable areas.** Don't leave APs unsecured where they can be easily accessed, or even switched by a hacker with their own AP so it will accept access from anyone. If the AP is not used during specific times of the day, disable it by unplugging it. If there are several APs in the WLAN, installing "Power-over-Ethernet" equipment from a central location will make this administrative task easier to manage.

For users accessing the WLAN, **installing Virtual Private Network technology** on their clients will secure their access to sensitive information and applications. IP Security Protocol VPN software will provide the necessary levels of encryption and access control required by DOD and AF security policy, and give the user peace of mind when they are transferring information across the WLAN. If the wireless internet service provider allows a VPN connection, this is a good idea for home wireless networking as well.

— **Master Sgt. Dave Hammack** AF Network Security Program Manager

# System certification process

*The computer system you're using most likely went through four independent reviews before it was allowed to operate on the Air Force enterprise network. This certification team consists of program managers, system engineers, user representatives, Designated Approving Authority representatives, information system security officers, and others as needed, to develop and document in a system security authorization agreement the system's security architecture and policies. By understanding the process, you will be more careful in how you operate and take care of your system.*

— **Lt. Col. Bruce Harmon** AETC Cyber Security Branch

### CERTIFICATION TEAM

The certification team performs comprehensive testing and evaluations to ensure agreed upon security measures are used. After rigorous review and testing, the Certifier certifies to the DAA that the system meets network security requirements, and if a particular requirement cannot be fully met, recommends risk mitigation procedures.

### AIR FORCE COMMUNICATIONS AGENCY

AFCA validates the certification team's findings and recommendations through an independent assessment of the system's security features and architecture. This assessment is documented in the issuance of a "Certificate of Networthiness."

### MAJCOM REVIEW

Although the primary emphasis is on sustainment issues such as fielding schedules, network bandwidth usage, and allied support, the system's security is again reviewed to ensure the system meets MAJCOM-unique needs. The MAJCOM review is documented in a "Certificate to Operate."

### BASE-LEVEL ASSESSMENT

The base Information Systems Security Manager, in conjunction with the program management office and the base network control center ensure the system is installed and operated from the agreement developed by the certification team.