Broadband Wireless Exchange Magazine

“The World's Largest Source of Municipal Wi-Fi Mesh Networking, WiMAX, and Wireless ISP Information”

Bio-NetGuard Wi-Fi Security Solution Shifts Verification Paradigm With Cost-Effective Biometric Technology

2/22/07 - Shimon Systems, Inc. has re-defined security for enterprise WiFi networks via its Bio-NetGuard™ WiFi Security Solution. A featured product at the prestigious DEMO emerging technology product showcase and winner of an INNY award from The Tech Museum in Silicon Valley, the Bio-NetGuard uses biometric fingerprint verification technology to authenticate the user. Incumbent technologies authenticate the equipment accessing the WiFi network and do not verify user identity like Bio-NetGuard.

"One of the fundamental weaknesses of most wireless networks at small-to-medium businesses and home offices is that any equipment within range can gain access to company WiFi resources," said Dr. Baldev Krishan, president and CEO of Shimon Systems. "Small, medium and large companies can now prevent unauthorized use of their WiFi networks' resources, save bandwidth, and filter out rogue access points."

Bio-NetGuard leverages the fingerprint readers that are increasingly built into laptop computers, as well as a wide range of USB and PCMCIA card sensors. Fingerprint matching is very fast and accomplished with virtually no performance penalty. Bio-NetGuard also prevents client association with WiFi access points that are not WPA/WPA 2.0 configured or authorized by the administrator.

The plug-and-play Bio-NetGuard unit can connect either to the WiFi access point or LAN router and requires about five minutes to install and set up. Most common 802.11a, 802.11b, or 802.11g wireless networks can be protected by Bio-NetGuard; the product is also fully compliant with 802.11i, the next-generation WiFi security standard also known as WPA/WPA2.0. Supported WiFi access point devices include NetGear, Linksys, Cisco, D-Link, and Bountiful, with more equipment in queue for interoperability certification.

Each Bio-NetGuard unit is capable of securing multiple WiFi access points connected to the same router, allowing authenticated users to freely and seamlessly roam between access points -- even access points from different vendors -- without having to re-authenticate! This ability not only minimizes equipment cost, but also lowers administrative overhead.

Management of Bio-NetGuard, regardless of the number of units within the enterprise LAN, is accomplished via a single, easy-to-use administrative interface. The device is available in a fingerprint-only version, as well as a two-factor fingerprint and password authentication version for maximum network security. Both versions can be purchased in user configurations supporting from five users for small application all the way to 250 users for a large deployments. More than 250 users can be accommodated as well.

Bio-NetGuard requires the Windows (2000/XP/Vista) operating system in either home or professional versions. The device is powered by algorithms from NEC, a world leader in biometric technology, and Texas Instruments' DSP chip running custom Shimon firmware.

By Robert Hoskins