WNN Wi-Fi Net News DAILY REPORTING ON WIRELESS DATA NETWORKING

March 7, 2007

Secure a Wi-Fi Network with a Fingerprint

By Glenn Fleishman

Shimon Systems extends biometric access to Wi-Fi networks: The firm, named after the Japanese word for fingerprint, started shipping its Bio-NetGuard a few months ago, and started talking more broadly about it recently. The device, starting at $500 for 10 users, allows a user's fingerprint to work as an authentication mechanism for a Wi-Fi network.

Shimon has built an 802.1X supplicant for Windows that connects a fingerprint scanner with the Bio-NetGuard, which acts as an authentication server using standard RADIUS and EAP (Encapsulated Authentication Protocol).

802.1X is port-based authentication in which a Wi-Fi access point or Ethernet switch prevents a device from accessing the rest of the network, but can pass authentication messages from a client-based connection program, called a supplicant, to an internal or external server that confirms credentials. In this case, the Bio-NetGuard acts as that server. With Wi-Fi networks, each attached client is assigned a unique network encryption key, preventing eavesdropping among connected devices.

Baldev Krishan, one of the company's four founders, said that using a fingerprint bypasses the weakness of user/password-based authentication. "Once the password is compromised, the whole network security goes by the wayside," he said. "Wouldn't it be nice to authenticate the user by who they are?" Krishan noted the advantage is that "you don't have to remember passwords. It can never be stolen, never be compromised," and it provides a log of access, too, in case of network troubles.

The Bio-NetGuard acts as a bit of a black box and a Roach Motel: "The fingerprint never leaves our box," Krishan said. The fingerprint templates can't be reverse engineered, either, as the supplicant sends just the reduced information, not the full scanned image or feature extraction; nor is that information stored in the server.

Bio-NetGuard is designed to be set up in a few minutes without information technology personnel. "You don't need any IT guy to install the RADIUS server. It's all out of the box. There are three or four settings needed," Krishan said.

One of the supported access points—a list of which is at Shimon's Web site, and is increasing all the time—needs to be configured with the RADIUS server information for the Bio-NetGuard,

which is an IP address, a shared secret (passed between the access point and the authentication server), and a TCP port. I've configured these setups many times, and it's not completely trivial, but neither is it very difficult.

The administrative tool allows enrollment, or adding a fingerprint, as well as removal of users and other tasks. The product can handle up to 250 users. The company is considering the market for larger use rbases, but has not yet announced a product for enterprises.

This first device clearly targets the small-to-medium-sized business market that uses IT consultants or limited in-house IT staff, but has a strong requirement for secure network access and logs of use. Medical, government, and legal industries are full of smaller shops with high regulatory burdens, such as the HIPAA rules governing medical patient privacy.

Krishan said that the three-year-old firm licensed its biometric technology for fingerprint characterization from **NEC, the world's leading firm in that space**. Krishan said that fingerprint scanners are becoming a common option in high-end laptops, with tens of millions of laptops expected to be sold with that biometric feature in the near future. External readers can be plugged in, as well.

Shimon's system uses a built-in or external fingerprint scanner to obtain an image, from which features—called minutiae points—are extracted, and then that data is compressed into a template. The template is transmitted by the built-in software to the server using 802.1X.

Shimon does an interesting end-run around the secure tranmission of that data over EAP, which, by default, has no encryption. Most supplicants found in operating system or releaesed by firms like Meetinghouse (now owned by Cisco) or Funk (purchased by Juniper) use PEAP (Protected EAP) or EAP-TTLS (Tunneled Transport Layer Security). Both methods wrap EAP messages in a secure layer using certificate exchange similar to that used on the Web for a secure SSL/TLS site.

Instead, Shimon uses the oldest secured EAP method: EAP-TLS. With EAP-TLS, you typically need to install a unique digital certificate on each computer. The certificate defines the uniqueness of the user for tracking purposes and to revoke former employees' access. However, because Shimon relies on the fingerprint for authentication, they can install a common certificate across all the computers on a network, providing verification in both directions (from client to server and server to client) of the validity of the public-key transaction before transmitting the fingerprint data.

For businesses that need this form of security coupled with the kind of simplicity that a fingerprint scanner offers, Shimon might have the right price and right product.

Posted by Glenn Fleishman at 11:50 AM | Categories: Security