Simple Secrets/Simple Security

by Robert Moskowitz
Senior Technical Director
ICSA Labs, a division of TruSecure Corporation

Simple Secrets/Simple Security

The new Wi-Fi security component, WPA (Wireless Protected Access), is built from three security building blocks: datagram encryption and integrity, session key establishment, and user authentication. There is a feature in the user authentication that can compromise a WPA deployment. For deployers that do not want to implement IEEE 802.1X, Pre-Shared Keys (PSK) can be used in lieu of user authentication. PSKs are a potential Achilles Heel that can result in a weaker security position than if WEP were used.

The designers of WPA (derived from an early draft version of IEEE 802.11i) were very careful in analyzing the attack scenarios against their design, and in general built a very good security component for wireless networks. They did make a concession to vendors that considered an 802.1X deployment as too much for typical small wireless networks. PSKs were included to make deployment easier, but simple secrets cannot make for strong security. PSKs can be 8 to 63 characters long or 256 bits (represented as a 64 hex character string). Thus PSKs tend to be passphrases that users can remember and attackers can guess.

Elsewhere I have detailed the nature of the attacks against wireless networks that base their security on PSKs rather than 802.1X. There are two aspects of the attack. An outsider can deduce the PSK by performing an offline dictionary attack against session key establishment exchange (called the 4-Way Handshake). An insider can directly derive any user's session key by applying his knowledge of the PSK against another user's 4-Way Handshake (to date I have not found any AP supporting per-station PSKs that would block this attack).

The problem with PSKs is that users rarely can create good, shared secrets. This is a long observed phenomenon. For example the PGP community has had an FAQ for years on the challenges of creating a good passphrase. The 802.11i specification clearly states that a passphrase less than 20 characters will unlikely stop an attack, and few users can work with passphrases this long. Since AP vendors did not take the high road to securing user authentication (for example embedding a RADIUS server in the AP supporting PEAP/MSChap), it is up to them to provide the tools to make it possible for users to deploy PSKs and still get the class of security that WPA can provide.

People have a hard time creating real secrets, but computers do not have such difficulties. A random number even 96 bits long would successfully stop any offline attacks against the PSK with today's computing resources.

The 802.11i standard's recommendation of a 256 bit random value is for cryptographic 'correctness' against any foreseeable attack. This 96-bit number can be represented in Hex, 24 characters long, or a combination of all letters and numbers, 14 characters long.

Any wireless product vendor can easily include a program that generates these random values and writes them to disk. From there they can be copied and pasted into the various PSK User Interfaces. This would create a permanent recording of the PSK outside of the wireless APs and clients, but the risk of theft is small compared to risk of a successful offline dictionary attack against a memorable PSK.

Solving the insider attack against PSKs is a little harder, but only need to be implemented on the APs. WPA supports per-station PSKs, but these would have to be implemented on a station (i.e. MAC address) basis, not per-user. Practically every AP now supports MAC address filters. Adding a PSK field to the MAC filter list can provide the per-station PSK. 802.11i, through a feature called PMK caching and PMKIDs, can actually support per-user PSKs.

WPA (and 802.11i) is a well-designed security system. But as with any security system, one open window will allow an attacker to breach the whole system. PSKs are potentially this open window. It is up to the AP vendor community to either make them safer to use, or obviate them with easy to deploy 802.1X.

Robert Moskowitz
Senior Technical Director
ICSA Labs, a division of TruSecure Corporation
Phone: (248) 968-9809
Fax: (248) 968-2824
rgm@icsalabs.com