WLAN Testing Reports

"PSK as the Key Establishment Method"

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

WLAN Testing Reports

Use of PSK as the Key Establishment Method

WPA and IEEE 802.11i provide for a Pre-Shared Key (PSK) as an alternative to 802.1X based key establishment. A PSK is a 256 bit number or a passphrase 8 to 63 bytes long. Each station MAY have its own PSK, tied to its MAC address. To date, vendors are only providing for one PSK for an ESS, just as they do for WEP keying.

When a PSK is used instead of IEEE 802.1X, the PSK is the Pairwise Master Key (PMK) that is used to drive the 4-Way Handshake and the whole Pairwise Transient Key (PTK) keying hierarchy. There is a straightforward formula for converting a passphrase PSK to the 256-bit value needed for the PMK.

This paper will look into the risks of using a PSK and particularly the risk associated with a passphrase-based PSK.

How the PSK is used in WPA and 802.11i

The PSK provides an easily implemented alternative for the PMK as compared to using 802.1X to generate a PMK. A 256bit PSK is used directly as the PMK. When the PSK is a passphrase, the PMK is derived from the passphrase as follows:

> PMK = PBKDF2 (passphrase, ssid, ssidLength, 4096, 256)
>
> Where the PBKDF2 method is from PKCS #5 v2.0: Password-based Cryptography Standard. This means that the concatenated string of the passphrase, SSID, and the SSIDlength is hashed 4096 times to generate a value of 256 bits. The lengths of the passphrase and the SSID have little impact on the speed of this operation.

The PTK is a keyed-HMAC function using the PMK on the two MAC addresses and the two nonces from the first two packets of the 4-Way Handshake. This is why the whole keying hierarchy falls into the hands of anyone possessing the PSK, as all the other information is knowable.

The Intra-PSK Attack

The normal practice is to have a single PSK within an ESS. To generate any PTK, a device only needs to learn the two MAC addresses and nonces (and the selected ciphersuite).

All of this is available in the initial exchange, from the ASSOCIATE through the 4-Way Handshake. Any device can passively listen for these frames and then generate the PTK.

If the device missed these frames, it can send a DISASSOCIATE against the STA and force the STA to perform the ASSOCIATE through the 4-Way Handshake again.
Thus even though each unicast pairing in the ESS has unique keys (PTK) there is nothing private about these keys to any other device in the ESS.

The Offline PSK Dictionary Attack

A station that does not know a passphrase based PSK can attack it with an offline attack. This is effective for an outsider where there is a single PSK in the ESS, or an insider where there are unique PSKs.

The 802.11i standard points out that:

> A passphrase typically has about 2.5 bits of security per character, so the passphrase of n bytes equates to a key with about 2.5n + 12 bits of security. Hence, it provides a relatively low level of security, with keys generated from short passwords subject to dictionary attack. Use of the key hash is recommended only where it is impractical to make use of a stronger form of user authentication. A key generated from a passphrase of less than about 20 characters is unlikely to deter attacks.

The PTK is used in the 4-Way Handshake to produce a hash of the frames. There is a long history of offline dictionary attacks against hashes. Any of these programs can be altered to use the information in the 4-Way Handshake as input to perform the offline attack. Just about any 8 character string a user may select will be in the dictionary. As the standard states, passphrases longer than 20 characters are needed to start deterring attacks. This is considerably longer than most people will be willing to use.

This offline attack should be easier to execute than the WEP attacks.

Using Random Values for the PSK

The PSK MAY be a 256bit (64 hexadecimal) random number. This is a large number for human entry; 20 character passphrases are considered too long for entry. Given the nature of the attack against the 4-Way Handshake, a PSK with only 128 bits of security is really sufficient, and in fact against current brute-strength attacks, 96 bits SHOULD be adequate. This is still larger than a large passphrase, but is unlikely to be in a dictionary attack. Using a relatively small random value represented in hexadecimal, and entering it as a passphrase will expand it to a proper 256bit PSK.

Summary

Anyone with knowledge of the PSK can determine any PTK in the ESS through passive sniffing of the wireless network, listening for those all-important key exchange data frames.

Also if a weak passphrase is used, for example a short passphrase, an offline dictionary attack can readily guess the PSK.
Since the common usage will be a single PSK for the ESS, once this is learned by the attacker, the attacker is now a member of the ESS, and the whole ESS is compromised. The attacker can now read and forge any traffic in the ESS.

Pre-Shared Keying is provided in the standard to simplify deployments in small, low risk, networks. The risk of using PSKs against internal attacks is almost as bad as WEP. The risk of using passphrase based PSKs against external attacks are greater than using WEP. Thus the only value PSK has is if only truly random keys are used, or for deploy testing of basic WPA or 80.211i functions. PSK should ONLY be used if this is fully understood by the deployers.

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