LANCOM Techpaper

LEPS / PPSK (Private Pre-Shared Key)

Mit den Verschlüsselungsverfahren WPA2 und WPA3 wird der Datenverkehr im WLAN gegen unerwünschte „Lauschangriffe“ geschützt. Die Verwendung einer Passphrase als zentraler Schlüssel ist dabei sehr einfach zu handhaben, ein RADIUS-Server wie in 802.1X-Installationen wird nicht benötigt.

Dennoch leiden diese abhörsicheren Verfahren an einigen Mängeln:

- **Eine Passphrase (Pre-shared Key, PSK) gilt global für alle WLAN-Clients**
- **Die Passphrase kann durch Unachtsamkeit ggf. an Unbefugte weitergegeben werden**
- **Mit der „durchgesickerten“ Passphrase können Angreifer in das Funknetzwerk eindringen**

In der Praxis bedeutet das: Falls die Passphrase verloren geht oder ein Mitarbeiter mit Kenntnis der Passphrase das Unternehmen verlässt, müsste aus Sicherheitsaspekten die Passphrase im Access Point geändert werden – und damit auch in allen WLAN-Clients. Da das nicht immer sichergestellt werden kann, würde sich also ein Verfahren anbieten, bei dem nicht eine globale Passphrase für alle WLAN-Clients gemeinsam gilt, sondern für jeden Benutzer im WLAN eine eigene Passphrase konfiguriert werden kann.

Seit Anfang 2000 bietet LANCOM mit LEPS-MAC (LANCOM Enhanced Passphrase Security MAC) bereits die Möglichkeit, die entstehenden Unsicherheiten durch die Nutzung einer globalen Passphrase zu vermeiden. Ab LCOS 10.20 bietet LANCOM ein weiteres effizientes Verfahren, genannt LEPS-U (LANCOM Enhanced Passphrase Security User),

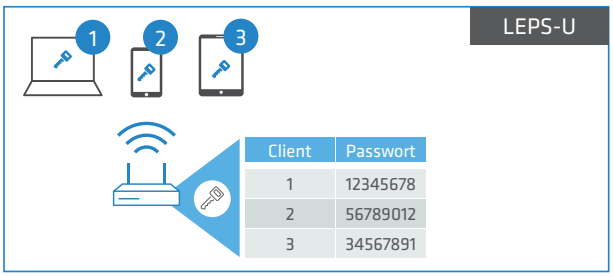
welches auf der PPSK-Methode basiert. Durch LEPS-U können Sie die einfache Konfigurierbarkeit von IEEE 802.11i mit Passphrase nutzen und dabei die möglichen Unsicherheiten bei der Nutzung einer globalen Passphrase vermeiden.

Mit LEPS-U vergeben Sie einzelnen Benutzern oder ganzen Gruppen ein individuelles WLAN-Passwort (Private Pre-Shared Key, PPSK) für eine SSID. Über LEPS-MAC authentifizieren Sie die Clients noch zusätzlich anhand ihrer MAC-Adresse – ideal für sichere Unternehmensnetzwerke!

LANCOM Enhanced Passphrase Security User (LEPS-U)

Mit LANCOM Enhanced Passphrase Security User (LEPS-U) können Sie bei WPA2 (PPSK-Methode) mehrere Passphrasen konfigurieren, die dann den einzelnen Benutzern oder Gruppen zugeordnet werden können. Somit gibt es nicht eine globale Passphrase für eine SSID, sondern mehrere, die dann individuell verteilt werden können.

Dies kann für das Onboarding von Geräten in das Netzwerk genutzt werden. Wenn ein Netzwerk-Betreiber z. B. mehrere WLAN-Geräte in verschiedene Bereiche seines Netzwerks „onboarden“, aber die Geräte nicht selber

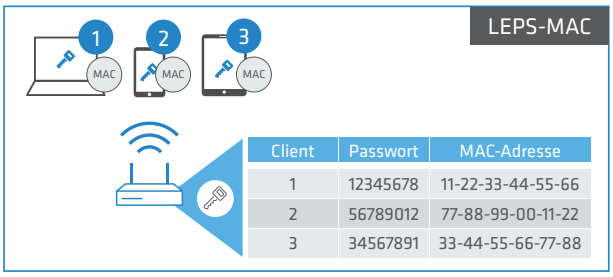


konfigurieren will, da dies die Benutzer der Geräte selber erledigen sollen. In diesem Fall erhalten die Benutzer lediglich einen Pre-Shared Key für das Firmen-WLAN ausgehändigt, welchen die Benutzer selber für ihre Geräte verwenden können. Je nach Pre-Shared Key werden die Benutzer automatisch durch Zuordnung zu einem VLAN einem bestimmten Netzwerk zugewiesen. Da LEPS-U ausschließlich auf der Infrastrukturseite konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Die zuvor beschriebene Unsicherheit von globalen Passphrasen wird durch LEPS-U grundsätzlich behoben. Jedem Benutzer wird hierbei seine eigene individuelle Passphrase zugewiesen. Falls eine einem Benutzer zugeordnete Passphrase verloren geht oder ein Mitarbeiter mit Kenntnis seiner Passphrase das Unternehmen verlässt, dann muss nur die Passphrase dieses Benutzers geändert bzw. gelöscht werden, um die mögliche Sicherheitslücke zu schließen. Alle anderen Passphrasen behalten ihre Gültigkeit und Vertraulichkeit.

LANCOM Enhanced Passphrase Security MAC (LEPS-MAC)

Bei LEPS-MAC wird jeder MAC-Adresse in einer zusätzlichen Spalte der ACL (Access Control List) eine individuelle Passphrase zugeordnet.



Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point. Da Passphrase und MAC-Adresse eindeutig miteinander verknüpft sind, ist auch das Spoofing der MAC-Adressen wirkungslos – LEPS-MAC schließt damit auch einen möglichen Angriffspunkt gegen die ACL aus. Wenn als Verschlüsselungsart WPA2 oder WPA3 verwendet wird, kann zwar die MAC-Adresse abgehört werden – die Passphrase wird bei diesem Verfahren jedoch nie über die WLAN-Strecke übertragen. Angriffe auf das WLAN werden so deutlich erschwert, da durch die Verknüpfung von MAC-Adresse und Passphrase immer beide Teile bekannt sein müssen, um eine Verschlüsselung zu verhandeln.

LEPS-MAC kann sowohl lokal im Gerät genutzt als auch mit Hilfe eines RADIUS-Servers zentral verwaltet werden. Dies funktioniert mit sämtlichen am Markt befindlichen WLAN-Clients, ohne dass dort eine Änderung stattfinden muss. Da LEPS-MAC ausschließlich im Access Point (Direkt oder indirekt per RADIUS) konfiguriert wird, ist hier ebenfalls jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Im Vergleich zu LEPS-U ist bei LEPS-MAC lediglich der Verwaltungsaufwand etwas höher, da für jedes Gerät die MAC-Adresse eingetragen werden muss.

Fazit

Bewahren Sie sich mit Private Pre-Shared Keys (PPSK) via LEPS die volle Kontrolle darüber, wer sich in Ihrem WLAN befindet. Mit LEPS-U vergeben Sie einzelnen Clients oder ganzen Gruppen ein individuelles WLAN-Passwort (Private PSK) für eine SSID. Über LEPS-MAC identifizieren Sie die Clients noch zusätzlich anhand ihrer MAC-Adresse.

Dabei kombiniert LEPS die einfache Konfigurierbarkeit von IEEE 802.11i mit Passphrase und vermeidet gleichzeitig die möglichen Unsicherheiten bei der Nutzung einer globalen Passphrase.

LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Würselen I Deutschland I E-Mail info@lancom.de

LANCOM Systems