BWCAMPUSNETZ

Zukunftsfähige Konzepte für die Campusnetze
an Universitäten und Hochschulen

WLAN-Zugang für IoT-Devices

Federführung bei der Erstellung dieses Dokuments: Karlsruher Institut für Technologie
Kontakt: team@bwcampusnetz.de

Inhalt

1 Anforderungen

In modernen WLAN-Netzwerken spielt die Sicherheit der Authentifizierung eine zentrale Rolle, wobei hierfür traditionell Mechanismen wie 802.1X eingesetzt werden, die eine zentrale Authentifizierung mittels eines RADIUS-Servers ermöglichen. Diese Methode wird besonders in großen Netzwerken wie in Unternehmen oder in Bildungseinrichtungen mittels eduroam realisiert. Allerdings stoßen solche Ansätze im Bereich des Internet of Things (IoT) und bei Geräten mit eingeschränkten Funktionalitäten auf praktische Grenzen. Viele IoT-Geräte, wie smarte Thermostate, Überwachungskameras, Drucker oder Sensoren, verfügen nicht über die notwendige Hardware, Software oder Rechenleistung, die für 802.1X erforderlich sind.

Da diese Geräte keine 802.1X-Authentifizierung unterstützen, sind sie auch nicht in der Lage, sich mit Netzwerken wie eduroam zu verbinden, selbst wenn dies technisch wünschenswert wäre. Für Bildungseinrichtungen, die eduroam als primären WLAN-Dienst verwenden, stellt dies eine besondere Herausforderung dar: Geräte wie IoT-Sensoren oder smarte Konferenzsysteme können nicht ohne Weiteres in das bestehende Netzwerk integriert werden. Hier bietet gerätespezifisches Pre-Shared Key (PSK), auch bekannt unter den Bezeichnungen Dynamic PSK (DPSK), Multi PSK (MPSK), Identity PSK (IPSK) oder Private PSK (PPSK), eine praktikable Lösung. Dieses Verfahren erlaubt es, Geräte ohne 802.1X-Unterstützung dennoch sicher und effizient in ein Netzwerk einzubinden, indem der MAC-Adresse jedes Geräts ein individueller, eindeutiger Schlüssel zugewiesen wird.

Ein wesentlicher Vorteil von gerätespezifischem PSK gegenüber herkömmlichem PSK besteht in der granularen Kontrolle und erhöhten Sicherheit, die durch die Verwendung individueller Schlüssel ermöglicht wird. Während bei einem einfachen PSK alle Geräte denselben Schlüssel teilen, was im Falle einer Kompromittierung des Schlüssels zu einem Sicherheitsrisiko für das gesamte Netzwerk führt, erhält bei gerätespezifischem PSK jedes Gerät bzw. dessen MAC-Adresse, einen eindeutigen Schlüssel. Dies bedeutet, dass ein kompromittierter Schlüssel nur den Zugang des betreffenden Geräts beeinträchtigt und keinen Einfluss auf andere Geräte hat. Darüber hinaus erleichtert gerätespezifisches PSK das Management, insbesondere in Umgebungen mit häufig wechselnden Geräten oder Benutzern, da der Zugang eines einzelnen Geräts einfach widerrufen werden kann, ohne den Schlüssel für das gesamte

Netzwerk zu ändern. Zudem ermöglicht gerätespezifisches PSK eine bessere Rückverfolgbarkeit, da jeder Schlüssel einer spezifischen Identität zugeordnet ist, was die Überwachung und Fehlerbehebung erheblich erleichtert. Dadurch stellt gerätespezifisches PSK eine flexible und sichere Lösung dar, insbesondere in Netzwerken mit heterogenen Anforderungen wie in Bildungseinrichtungen mit gemischten Benutzergruppen.

2 Terminologie

Gerätespezifisches PSK bezeichnet eine Sicherheitslösung, bei der jedem Gerät ein individueller PSK zugewiesen wird, basierend auf der MAC-Adresse des Geräts. Verschiedene Hersteller haben dabei ihre eigenen Implementierungen entwickelt, verwenden jedoch teils identische Bezeichnungen für unterschiedliche Implementierungen: Ruckus Networks, Inc. nennt seine Lösung DPSK (Dynamic PSK), ebenso wie Huawei Technologies Co., Ltd., Aruba Networks bezeichnet sie als MPSK (Multi-PSK), Aerohive Networks, Inc. (jetzt Teil von Extreme Networks, Inc.) verwendet den Begriff PPSK (Private PSK), und Cisco Systems, Inc. den Begriff iPSK (Individual PSK). Im Kern zielen alle diese Ansätze darauf ab, MAC-Adressen spezifische Schlüssel zuzuweisen, wodurch eine eindeutige Bindung zwischen Gerät und PSK entsteht.

Einige Hersteller bieten jedoch auch geräteunspezifische PSK-Lösungen an. Cisco Systems, Inc. ermöglicht beispielsweise mit seiner MPSK-Lösung, mehrere PSKs für eine SSID zu konfigurieren, ohne diese spezifischen Geräten bzw. MAC-Adressen zuzuordnen. Ähnlich bietet Huawei Technologies Co., Ltd. eine PPSK-Lösung an, bei der mehrere geräteunspezifische PSKs auf dem Controller hinterlegt werden können.

Dieses Dokument befasst sich jedoch ausschließlich mit gerätespezifischem PSK, bei dem eine direkte Zuordnung zwischen MAC-Adresse und PSK besteht. Die Zuordnung von MAC-Adresse zu PSK kann dabei entweder direkt auf dem Access Point (AP), auf dem WLAN-Controller oder innerhalb des RADIUS-Backends erfolgen, wobei die Beispielimplementierung im Folgekapitel die Verwendung eines RADIUS-Backends aufzeigt.

3 Implementierung

Wie bereits beschrieben wird eine ähnliche Technologie (MPSK) von verschiedenen Herstellern leicht unterschiedlich implementiert. Im Folgenden wird die Implementierung am Beispiel der Aruba-WLAN-Lösung, basierend auf Aruba AOS-8, beschrieben. Bei anderen Herstellern kann sich die Implementierung dementsprechend unterscheiden, z.B. in den tatsächlich benötigten RADIUS-Attributen. Die MPSK-Technologien unterliegen bei verschiedenen Herstellern weiterhin verschiedenen Einschränkungen. Im Falle von Aruba lässt sich MPSK z.B. nur mit der Verschlüsselungsmethode WPA2-PSK-AES nutzen. WPA2 mit TKIP bzw. WPA3-SAE werden bei dieser Lösung nicht unterstützt.

Die technische Umsetzung von MPSK mit der Aruba-WLAN-Lösung ähnelt stark an die 802.1X-Authentifizierung: Auch bei MPSK übernimmt der Access Point oder Controller die Rolle des Vermittlers und leitet Authentifizierungs-Anfragen an einen RADIUS-Server weiter. Im Gegensatz zu 802.1X wird jedoch keine komplexe EAP-Authentifizierung durchgeführt, sondern stattdessen die MAC-Adresse des Clients als Identifikationsmerkmal an den RADIUS-Server übermittelt, auf Basis derer dieser über den weiteren Verlauf der Authentifizierung entscheidet. Die beispielhafte Konfiguration eines WLAN-Controllers kann Abbildung 3.1 entnommen werden.

Der RADIUS-Server gleicht dazu die übermittelte MAC-Adresse des Clients (und ggf. weitere übermittelte Merkmale wie die IP-Adresse des anfragenden Access-Points) mit einer Datenbank ab und liefert nicht nur die Informationen zum zu verwendenden VLAN (VLAN-ID), sondern gleichzeitig auch die für den jeweiligen Nutzer vorgesehene Passphrase. Der Controller bzw. Access Point prüft daraufhin, ob der Client mit dieser Passphrase authentifiziert werden kann. Ist das erfolgreich, erhält der Client nicht nur seine individuelle Verschlüsselung, sondern wird auch automatisch in das passende VLAN verbunden. Dieser Vorgang wird in Abbildung 3.2 skizziert.

In der Praxis müssen dafür vom RADIUS-Server die folgenden Attribute an den WLAN-Controller/AP zurückgegeben werden:

Tunnel-Private-Group-Id VLAN-ID des Netzes, in welches der Client verbunden werden soll

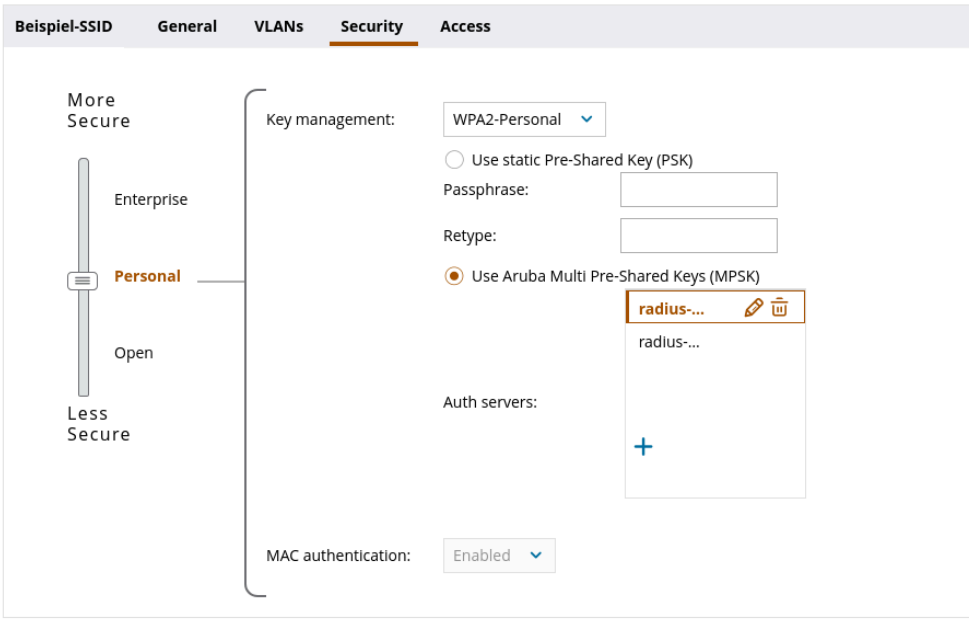

Abb. 3.1: MPSK: Beispielhafte Konfiguration der RADIUS-Server mittels Aruba Mobility Conductor

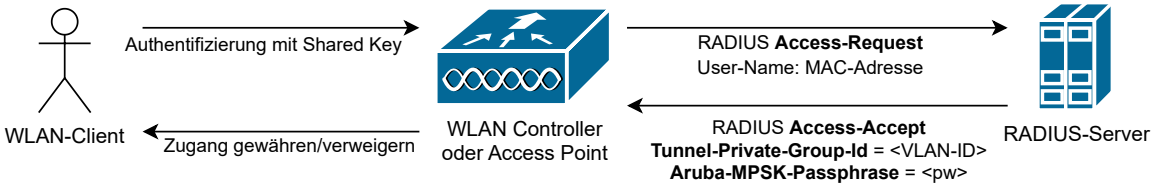

Abb. 3.2: MPSK: Interaktion zwischen den beteiligten Komponenten

Tunnel-Type VLAN

Tunnel-Medium-Type IEEE-802

Aruba-MPSK-Passphrase Passphrase, welche der Client zur Authentifizierung nutzen muss

Während das Attribut `Aruba-MPSK-Passphrase` spezifisch für die Aruba-basierte Lösung benötigt wird, können auch andere als die Aruba-eigene RADIUS-Lösung konfiguriert werden, dieses Attribut zurückzugeben. Insbesondere ist eine Implementierung mittels der Open-Source-Software FreeRADIUS möglich, welche in Listing 3.1 skizziert wird.

List. 3.1: MPSK: Beispielhaftes Setzen der benötigten Attribute durch FreeRADIUS basierend auf in einer Datenbank hinterlegten MACAdressen, VLANIDs und Passphrasen

```
mpsk {
    if ("%{sql:SELECT COUNT(*) FROM macauth WHERE mac='%{User-Name}'}" >
       ↪ 0) {
       update reply {
           Tunnel-Private-Group-Id := "%{sql:SELECT vlan_id FROM macauth
              ↪ WHERE mac='%{User-Name}'}"
           Tunnel-Type := VLAN
           Tunnel-Medium-Type := IEEE-802

           Aruba-MPSK-Passphrase := "%{sql:SELECT passphrase FROM macauth
              ↪ WHERE mac='%{User-Name}'}"
         }
         update {
            control:Auth-Type := Accept
         }
     }
     else {
        reject
     }
}
```

4 Fazit

Gerätespezifisches PSK bietet eine sichere und praktische Alternative für die Authentifizierung von Geräten, die keine Unterstützung für den 802.1X-Standard bieten. Diese Lösung ist besonders in Bildungseinrichtungen sinnvoll, die primär auf WLAN als Netzwerkdienst angewiesen sind und häufig mit einer Vielzahl an IoT-Geräten arbeiten müssen.

Mit der im vorherigen Kapitel dargestellten Lösung müssen die Nutzer lediglich die MAC-Adresse des Geräts sowie gegebenenfalls das VLAN in einem Self-Service-Portal hinterlegen. Alternativ, falls dieser Schritt noch manuell erfolgt, können die Informationen an die entsprechende Netzwerkabteilung übermittelt werden, welche anschließend die entsprechenden Einträge in der Datenbank vornimmt. Dieser Ansatz vereinfacht den Prozess erheblich, da der administrative Aufwand für die Konfiguration und Verwaltung für Geräte minimal ist.

Des Weiteren hat Wi-Fi Easy Connect, eingeführt von der Wi-Fi Alliance im Jahr 2018, das Potenzial, mittelfristig eine bedeutende Rolle bei der Netzwerkkonfiguration zu spielen. Dies wurde entwickelt, um Herausforderungen bei der sicheren und effizienten Integration von Geräten zu bewältigen, insbesondere von IoT-Geräten, die häufig keine Benutzeroberfläche besitzen.

Im Kern wird hierbei das Device Provisioning Protocol (DPP) verwendet, welches auf moderner Kryptographie basiert, darunter Elliptic Curve Cryptography (ECC) und dem Advanced Encryption Standard (AES). Der Einbindungsprozess wird hierbei durch QR-Codes, NFC-Tags und cloudbasierte Gerätekonfiguration vereinfacht. Ein Gerät, welches eine Netzwerkverbindung benötigt (sog. Enrollee) kann durch einen Konfigurator (engl. Configurator) - z.B. ein Smartphone, sicher ins Netzwerk aufgenommen werden, was bspw. durch einfaches Scannen eines QR-Codes auf dem Enrollee erfolgt. Jeder neue Teilnehmer erhält dabei individuelle Anmeldedaten. Unterstützt wird hierbei sowohl WPA2 als auch WPA3.

5 Versionsverlauf

Version	Datum	Änderungen
1.0	06.10.2025	Initiale Veröffentlichung