

Sicherheit in Wireless LANs

von

Cornelius Höchel-Winter

3.1.2 Authentisierung

Wie oben erwähnt, ist eine sichere Authentisierung der Kommunikationspartner untereinander in einem Funknetzwerk selbst bei unverschlüsselter Übertragung unverzichtbar.

Der 802.11-Standard sieht zwei mögliche Authentisierungsverfahren vor: „*Open System*“ und „*Shared Key*“.

Der **Open-System-Modus** ist kein wirkliches Authentisierungsverfahren und steht im Wortsinne für ein offenes System, denn in diesem Modus sollen alle Authentisierungsanfragen positiv beantwortet werden. Das Verfahren (siehe Abbildung 3.9) besteht aus zwei Managementframes (siehe Abbildung 2.4) vom Typ *Authentication*. Frame 1 wird vom anfragenden Client an den Access Point geschickt, die Antwort des Access Points in Frame 2 enthält im Wesentlichen nur ein Status-Feld, welches die Anfrage entweder bestätigt oder ablehnt. Das heißt eine Authentisierung im eigentlichen Sinne findet nicht statt, da gar keine relevanten Daten, die eine sichere Identifizierung des Clients ermöglichen würden, transportiert werden.

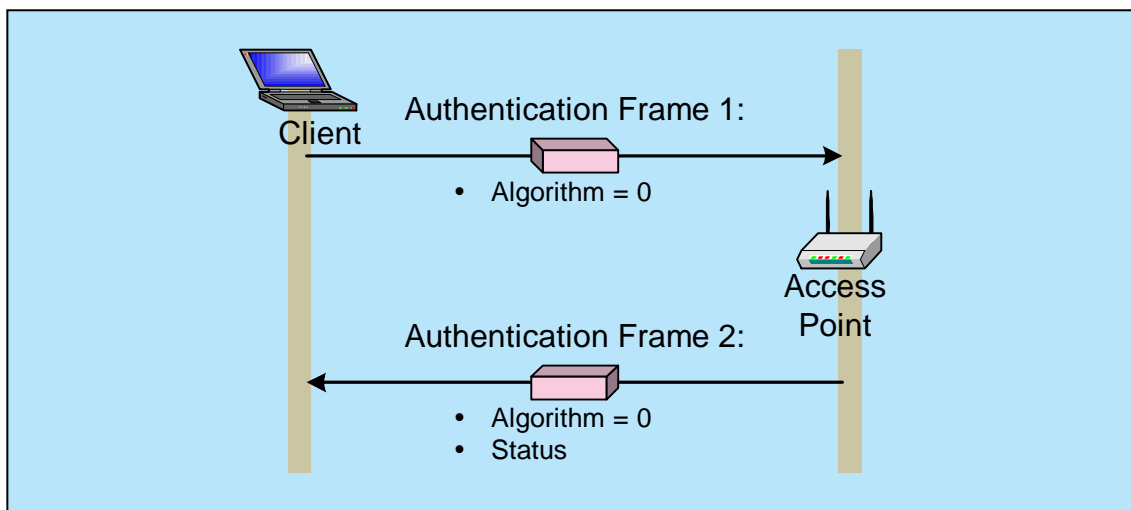


Abbildung 3.9: Authentisierung im Open-System-Modus

Der Access Point hat im Wesentlichen drei Kriterien zur Auswahl, anhand derer er eine Authentisierungsanfrage entscheiden kann:

- die Grundsatzentscheidung, ob der Open-System-Modus überhaupt zugelassen ist. Dies kann jeweils im Konfigurationsmenü der Access Points eingestellt werden.
- der SSID des WLANs. Der Standard sieht vor, dass sich Clients mit einer leeren SSID an allen WLANs anmelden können. Bei einigen Produkten kann man das verhindern, so dass sich nur Clients mit dem richtigen SSID anmelden. Allerdings teilen die Access Points ihren SSID in den regelmäßigen Rundsendungen (Beacons) mit, so dass der SSID kein wirkliches Ge-

heimnis darstellt. Daran ändern auch einige Herstellererweiterungen wie „Closed System“ (siehe Kapitel 3.1.2.1 unten) nichts.

- die MAC-Adresse des Clients. Hierbei ist zu beachten, dass die MAC-Adresse stets im Klartext übermittelt wird und es kein großes Problem darstellt, die MAC-Adresse zu fälschen. Durch bloßes Zuhören erlangt man also Kenntnis von gültigen MAC-Adressen, die dann zum eigenen Senden genutzt werden können.

Bei der Frage, welche dieser Kriterien tatsächlich unterstützt werden, unterscheiden sich die Produkte. Eine große Mehrzahl lässt statische Accesslisten von MAC-Adressen zu, zum Teil auch mit Wildcards. Einige Hersteller unterstützen sogar die Abfrage gültiger MAC-Adressen bei einem zentralen RADIUS-Server. Dies wird oft als „RADIUS-Unterstützung“ vermarktet, darf aber nicht mit einer zentralen Authentisierung nach IEEE 802.1X verwechselt werden, die von den neuen Sicherheitsstandards WPA und 802.11i gefordert wird.

Letztlich muss man den Open-System-Modus als eine rein administrative Anmeldung des Clients beim gewünschten Netzwerk sehen und nicht als Authentisierungsverfahren. Die Frage, ob man den Open-System-Modus zulässt oder nicht, trägt wirklich nichts zur Sicherheit des WLANs bei.

So können beispielsweise MAC-Adressen wie auch SSID zur Aufteilung der Clients auf verschiedene WLANs genutzt werden, wenn mehrere WLANs am selben Ort betrieben werden.

Im Anhang B.1 ist ein kompletter Mitschnitt von Frames aufgeführt, die bei der Anmeldung eines Clients an einem Access Point im Open-System-Modus ausgetauscht werden.

Im Gegensatz zum Open-System-Modus setzt der **Shared-Key-Modus** die Kenntnis eines gemeinsamen, geheimen Schlüssels voraus. Da dieser Schlüssel natürlich nicht im Klartext übertragen werden kann, wird dieser Modus nur in Verbindung mit WEP und über verschlüsselte Frames durchgeführt. Bei dem gemeinsamen, geheimen Schlüssel handelt es sich um den WEP-Schlüssel.

Das Verfahren (siehe Abbildung 3.10) selbst besteht aus vier Managementframes vom Typ *Authentication*, wobei Frame 1 und Frame 4 die gleichen sind wie beim Open-System-Modus und die Anfrage des Clients und die Antwort des Access Points transportieren. Die beiden mittleren Frames dienen der Bestätigung, dass dem Client der korrekte WEP-Schlüssel vorliegt. Dazu sendet der Access Point nach der einleitenden Anfrage des Clients einen 128 Byte langen Zufallstext als Challenge, der Client sendet daraufhin genau diesen Challenge im dritten Frame zurück, verschlüsselt diesen allerdings mit dem entsprechenden WEP-Key. War der WEP-Key korrekt, kann die angefragte Station nun die Nachricht entschlüsseln und mit dem eigenen Text aus dem zweiten Frame vergleichen. Der letzte Frame teilt dem Client wiederum das Ergebnis der Authentisierung mit.

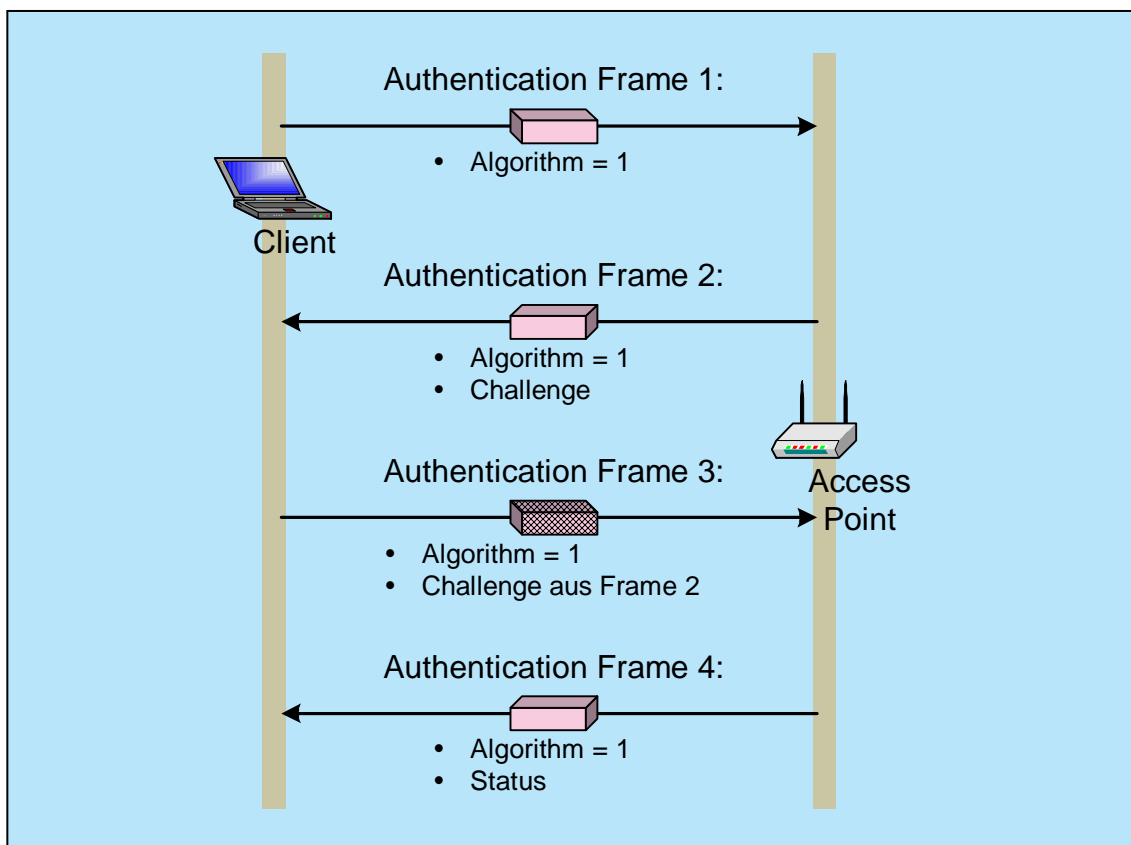


Abbildung 3.10: Authentisierung im Shared-Key-Modus

Dieser Modus beruht also darauf, dass der Access Point die Kenntnis eines gemeinsamen Geheimnisses – vergleichbar mit einem Passwort – überprüft. Soweit die Theorie ...

Tatsächlich hat dieser Modus so schwer wiegende Mängel, dass von seinem Einsatz dringend abgeraten werden muss.

Stattdessen sollte der Open-System-Modus in Verbindung mit WEP-Verschlüsselung verwendet werden.

Die Probleme des Shared-Key-Modus werden weiter hinten in Kapitel 3.2.1.9 besprochen.

3.1.2.1 Hersteller-Erweiterung Closed System

Da Clients so konfiguriert werden können, dass sie sich nur Access Points mit passendem SSID aussuchen, drängt sich die Idee auf, den SSID als geheimes Passwort für den Netzzugang zu nutzen. Fahrlässigerweise wird genau diese Strategie auch in vielen Benutzerhandbüchern empfohlen.

Aber der SSID wird immer unverschlüsselt übertragen, auch bei aktivierter WEP-Verschlüsselung!

In einer Standardkonfiguration wird der SSID regelmäßig in allen Beacons und Probe-Response-Frames bekannt gegeben, auch der Client sendet in Frames

vom Typ *Association Request* und *Probe Request* seinen SSID im Klartext über den Äther.

Einige Hersteller haben einen erweiterten „Sicherheits“-Modus unter Bezeichnungen wie „Closed System“ oder ähnlichen etabliert. Sobald dieser Modus aktiviert ist, übermittelt der Access Point in seinen Beacons keinen SSID mehr, der Netzwerkname bleibt also zunächst geheim und kann von den Clients nicht mehr ohne weiteres ausgewertet werden.

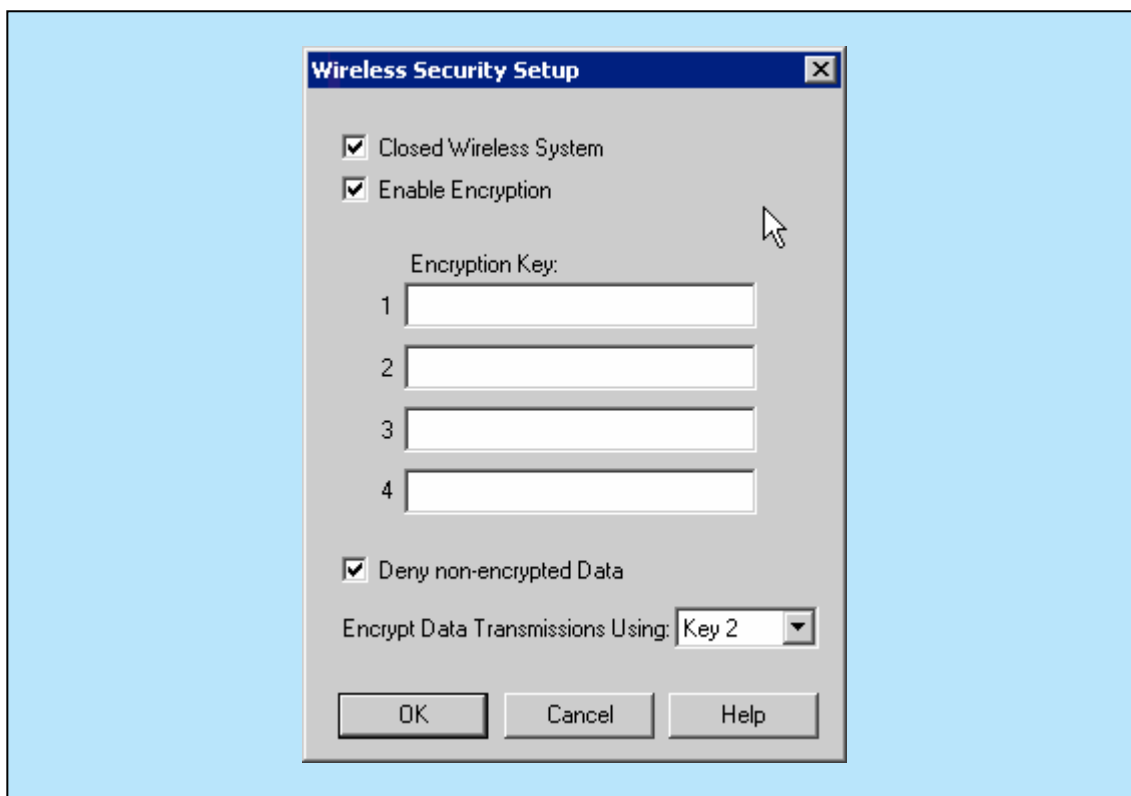


Abbildung 3.11: Konfiguration eines Closed System

Trotzdem wird der SSID auch in diesem Modus weiterhin von Frames des Typ *Probe Response* und von den Frames der Clients übertragen. Mithörenden Lauschern wird also auch in diesem Modus der SSID eines Funk-LANs nicht sehr lange unbekannt bleiben. Im Anhang B.2 ist ein kompletter Mitschnitt aller Frames aufgeführt, die bei der Anmeldung eines Clients an einem Access Point im Closed-System-Modus auftreten. Dort kann man im Detail vergleichen, welche Informationen bei welchen Frametypen ausgetauscht werden.

Einen gewissen Vorteil dieses Modus kann man höchstens darin erkennen, dass einige einfache Spionagetools (siehe auch Kapitel 3.2.2) ihre Erkenntnisse ausschließlich aus der Auswertung der Beacons ziehen, für solche Tools bleiben WLANs im Closed-System-Modus unsichtbar.