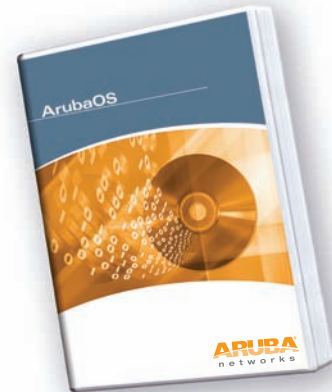




### ARUBAOS XSEC MODULE

xSec ist ein extrem sicheres Data Link Layer (Layer 2)-Protokoll, das durch strenge Verschlüsselungs- und Authentifizierungsmaßnahmen ein einheitliches System zur Sicherung sämtlicher kabelgebundener und drahtloser Verbindungen bietet. Das bei xSec eingesetzte Verfahren hält die Federal Information Processing Standards (FIPS) ein, um identitätsorientierte Sicherheitsfunktionen für Behörden und Unternehmen bereitzustellen, die sensible Daten über Drahtlosnetzwerke versenden müssen. Neben längeren Schlüsseln kommen bei xSec auch FIPS-validierte Verschlüsselungsalgorithmen (AES-CBC-256 mit HMAC-SHA1) sowie verschlüsselte Layer 2-Headerinformationen (inklusive der MAC-Adressen) zum Einsatz, wodurch eine höhere Sicherheit als bei anderen Technologien zur Layer 2-Verschlüsselung erreicht wird. xSec ist eine gemeinschaftliche Entwicklung von Aruba Networks und Funk Software, einem Unternehmensbereich von Juniper Networks.



#### EINHEITLICHES SICHERHEITSSYSTEM

- Universelle Authentifizierung und Verschlüsselung für kabelgebundene wie drahtlose Benutzer, unabhängig von der Zugriffsmethode auf das Netzwerk

#### FIPS-VALIDIERT

- FIPS 140-2-konform und -zertifiziert

#### SCHUTZ VORHERIGER INVESTITIONEN

- Dank der Software-basierten Client-Lösung müssen alte Wireless Access Points und NIC-Karten nicht ausgetauscht werden.

#### AUF KOMPATIBILITÄT AUSGELEGT

- Basiert auf dem IEEE 802.1x-System mit Support für sämtliche sicheren EAP-Methoden

#### SCHUTZ VOR NICHT AUTORISIERTEN ACCESS POINTS

- RErkennung, Klassifizierung, Lokalisierung und automatische Eindämmung nicht autorisierter Access Points

#### WARUM LAYER 2-VERSCHLÜSSELUNG NOTWENDIG IST

Verschlüsselung wurde bisher normalerweise immer in Form von IPsec auf Layer 3-Ebene durchgeführt. IPsec verwendet dabei eine 3DES- oder AES-Verschlüsselung und kann das IP-Paket inklusive der Quell- und Ziel-IP-Adresse im Header verschlüsseln. Diese Technik stellt eine allgemein anerkannte, sichere Methode zur Kommunikation über nicht vertrauenswürdige Netzwerke dar, da die einzigen Informationen, die hierbei unverschlüsselt bleiben, die Paket-Header sowie der pure Layer 2-Datenverkehr wie beispielsweise ARP (Address Resolution Protocol)- und DHCP (Dynamic Host Configuration Protocol)-Pakete sind.

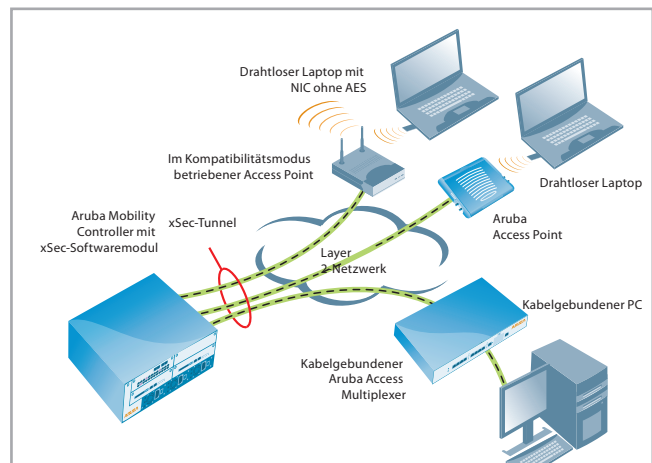
Während die Vertrauenswürdigkeit der IPsec-verschlüsselten Daten also nicht in Frage gestellt wird, besteht trotzdem die Möglichkeit, dass ein Angreifer mit direktem Zugriff über den Link-Layer auf andere Geräte im Netzwerk Angriffe gegen eben diese Geräte durchführen kann. So können in einem drahtlosen Netzwerk, das mit WEP und IPsec gesichert ist, die Client-Geräte in Gefahr sein, wenn ein Angreifer in den Besitz des WEP-Schlüssels gelangt und Layer 2-Zugriff auf das Netzwerk erhält. Darüber hinaus gibt es die Sorge, dass offenliegende Header-Informationen als Grundlage für einen Angriff ausgenutzt werden könnten.

So hat für viele Behörden und Unternehmen der Einsatz leistungsfähiger Layer 2-Verschlüsselungstechnologien oberste Priorität, um einen möglichst vollkommenen Datenschutz zu gewährleisten. Bei vielen Behörden auf dem Verteidigungssektor ist eine Verschlüsselung auf Layer 2-Ebene außerdem bereits Voraussetzung für die Übertragung von Daten über kommerzielle Drahtlosgeräte. Kryptografische Systeme, die für sensible Kommunikation von US-Behörden eingesetzt werden, müssen

die FIPS 140-2-Anforderungen erfüllen. xSec wurde genau dafür entworfen und bietet darüber hinaus noch weitere Vorteile.

#### EINHEITLICHES SICHERHEITSSYSTEM

xSec ermöglicht unabhängig von der Zugriffsmethode eine universelle Authentifizierung und Verschlüsselung. Jeder Client, der sich mit dem Netzwerk verbindet – ob drahtlos oder kabelgebunden – kann sich an einem Aruba Mobility Controller über einen xSec-Client authentifizieren. Die Authentifizierung innerhalb der xSec-Protokolle erfolgt über standardisiertes



Drahtlose und kabelgebundene Gerätekonnektivität mit xSec

802.1x-EAP (Extensible Authentication Protocol) sowie einen standardgemäßen RADIUS-Server zur Validierung der Berechtigungen. xSec unterstützt die Authentifizierung über Kennwörter, Zertifikate, Smartcards, Token sowie sämtliche andere Berechtigungsmethoden, die vom gewählten EAP-Typ unterstützt werden.

#### FIPS-VALIDIERT

Durch den Einsatz von AES-CBC mit einer Schlüssellänge von 256 Bit für die Verschlüsselung bietet xSec das einzige FIPS-validierte COTS (Commercial Off-the-Shelf)-Layer 2-Protokoll, weshalb es sich als ideale Lösung für sicherheitssensible Anwendungen in Behörden sowie auf dem Finanz- und Medizinsektor anbietet. FIPS selbst ist ein strengerer Sicherheitsstan-

# ARUBAOS XSEC MODULE

ard als er auf dem Wirtschaftssektor eigentlich vorgeschriebene ist und deshalb besser geeignet für die Einhaltung dort geltender Bestimmungen wie HIPAA und GLBA.

## SCHUTZ VORHERIGER INVESTITIONEN

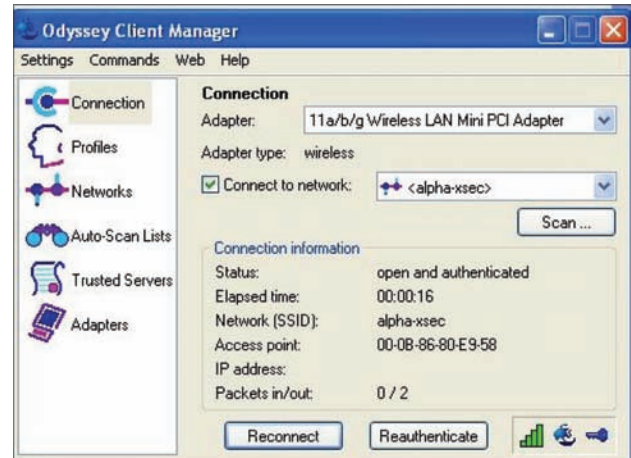
Ein Großteil der bereits vorhandenen Ausrüstung kann nicht aktualisiert werden, um neueste Sicherheitsstandards wie 802.11i und WPA2 zu unterstützen. Die Verschlüsselung von xSec wird dagegen hardwareseitig vom Aruba Mobility Controller und softwareseitig auf Client-Ebene durchgeführt, wodurch ein bestehendes Netzwerk aufgerüstet werden kann, um die aktuellsten Sicherheitstechnologien zu unterstützen, ohne dass ältere Access Points oder drahtlose NICs (Network Interface Cards) ersetzt werden müssen.

## AUF KOMPATIBILITÄT AUSGELEGT

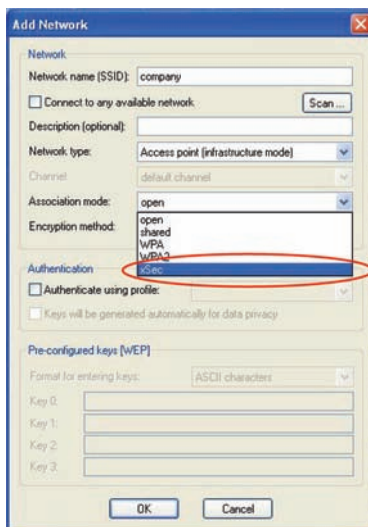
xSec basiert auf dem IEEE-Sicherheitsstandard 802.1x. Zu den unterstützten sicheren EAP-Methoden gehören EAP-TLS, TTLS sowie PEAP, wodurch die Kompatibilität von xSec mit bestehenden Sicherheitsmechanismen wie RSA-Token und PKI-Zertifikaten gewährleistet wird. xSec ist auf Transparenz zur Layer 2-Infrastruktur ausgelegt und kann durch ein Switched Ethernet-Netzwerk betrieben werden, ohne zu riskieren, dass EAP-Frames von 802.1x-fähigen Ethernet-Switches abgefangen werden. Der Odyssey Client mit xSec-Unterstützung von Juniper Networks ist für Windows 2000, Windows XP und Windows Mobile erhältlich.

## EINSATZSZENARIEN

Der Einsatz von xSec geschieht durch die Aktivierung der xSec-Softwarelizenz auf einem Aruba Mobility Controller und der Installation des Odyssey Clients von Juniper Networks auf einem PC mit kabelgebundenem oder drahtlosem Netzzugriff. Mögliche Einsatzorte von xSec sind die Sicherung des Datenverkehrs zwischen einem Aruba Mobility Controller und einem drahtlosen Client, zwischen einem Mobility Controller und einem kabelgebundenem Client oder zwischen zwei Mobility Controllern im selben VLAN.



Odyssey Client, verbunden mit dem SSID „alpha-xsec“ über das xSec-Protokoll



Konfiguration des Clients zum Einsatz der xSec-Verschlüsselung im SSID „company“



[WWW.ARUBANETWORKS.COM](http://WWW.ARUBANETWORKS.COM)

1322 Crossman Avenue, Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550