



ARUBAOS XSEC MODULE

xSec is a highly secure data link layer (Layer 2) protocol that provides a unified framework for securing all wired and wireless connections using strong encryption and authentication. xSec provides a Federal Information Processing Standard (FIPS)-compliant mechanism to provide identity-based security to government agencies and commercial entities that need to transmit extremely sensitive information over wireless networks. xSec provides greater security than other Layer 2 encryption technologies through the use of longer keys, FIPS-validated encryption algorithms (AES-CBC-256 with HMAC-SHA1), and the encryption of Layer 2 header information including MAC addresses. xSec was jointly developed by Aruba Networks and Funk Software, a division of Juniper Networks.



UNIFIED SECURITY FRAMEWORK

- Universal authentication and encryption for wired and wireless users, regardless of network access method

FIPS VALIDATED

- FIPS 140-2 compliant and certified

LEGACY INVESTMENT PROTECTION

- Software-based client solution means legacy wireless access points and NIC cards do not need to be replaced

DESIGNED FOR COMPATIBILITY

- Based on IEEE 802.1x framework with support for all secure EAP methods

ROGUE AP PREVENTION

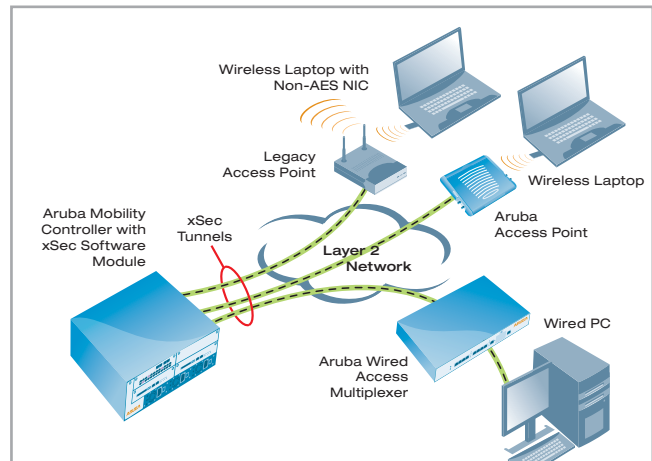
- Rogue AP detection, classification, location and automatic containment

THE NEED FOR LAYER 2 ENCRYPTION

Traditionally, encryption has been performed at Layer 3 (Network Layer) in the form of IPsec. IPsec uses 3DES or AES encryption and can encrypt the IP packet including the source and destination IP addresses in the header. IPsec provides a commonly accepted, secure method of communication over untrusted networks since the only information left unencrypted are packet headers and pure Layer 2 traffic such as ARP (Address Resolution Protocol) and DHCP (Dynamic Host Configuration Protocol) packets.

While the confidentiality of IPsec-encrypted data is not in question, the possibility exists that an attacker with direct link-layer access to other devices on a network could carry out attacks against those devices. For example, a wireless network secured with WEP and IPsec could put client devices at risk if an attacker obtains the WEP key and gains Layer 2 access to the network. In addition, there is concern among many security groups that exposure of any packet header information could be used as the basis of an attack.

For this reason, many government agencies and commercial entities mandate that strong Layer 2 encryption technologies be deployed to ensure absolute data privacy. Many defense agencies require that all data transmitted using commercial wireless devices be encrypted at Layer 2. Cryptographic engines used for all sensitive U.S. government communications must be validated as meeting FIPS 140-2 requirements, and xSec has been designed to address this requirement plus provide a number of additional benefits.



Wired and Wireless Device Connectivity Using xSec

UNIFIED SECURITY FRAMEWORK

xSec enables universal authentication and encryption regardless of access method. Every client that connects to the network, wireless or wired, can authenticate to an Aruba Mobility Controller using an xSec client. Authentication inside the xSec protocol is accomplished using standard 802.1x EAP (Extensible Authentication Protocol) and a standard RADIUS server to validate credentials. xSec supports authentication using passwords, certificates, smart cards, token cards, and other credentials supported by the chosen EAP type.

ARUBAOS XSEC MODULE

FIPS VALIDATED

Through the use of AES-CBC with a 256-bit key length for encryption, xSec provides the only COTS (Commercial Off-the-Shelf) Layer 2 protocol that is FIPS validated. As a result, xSec is an ideal solution for security-sensitive applications in the government, finance, and healthcare markets. FIPS is a more stringent security standard than those required in the commercial sector, and therefore more suitable for compliance with commercial regulations such as HIPAA and GLBA.

LEGACY INVESTMENT PROTECTION

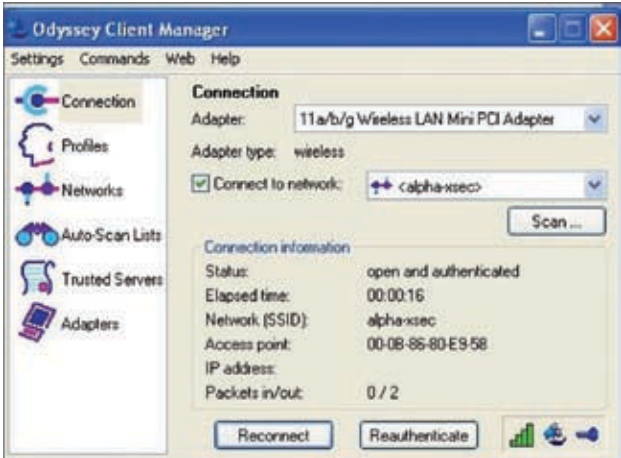
Most legacy equipment cannot be upgraded to support the latest security standards such as 802.11i and WPA2. xSec encryption, however, is performed in hardware by the Aruba Mobility Controller, and in software at the client level, meaning that an existing network can be upgraded to support the latest security technology without replacing older access points or wireless NICs (network interface cards).

DESIGNED FOR COMPATIBILITY

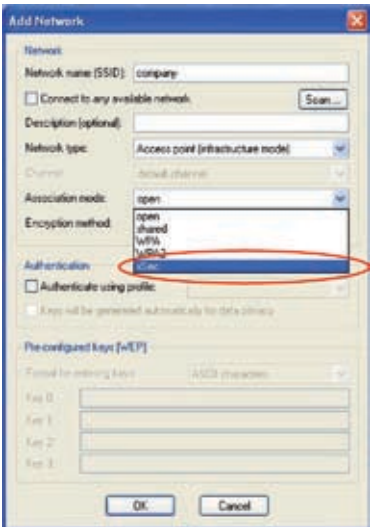
xSec is based on the IEEE security standard 802.1x. Secure EAP methods supported include EAP-TLS, TTLS and PEAP, making xSec compatible with existing security mechanisms such as RSA Tokens and PKI certificates. xSec is designed to be transparent to the Layer 2 infrastructure and can operate through a switched Ethernet network without the risk of EAP frames being intercepted by 802.1x-aware Ethernet switches. Juniper Networks' Odyssey Client with xSec support is available for Windows 2000, Windows XP and Windows Mobile.

DEPLOYMENT SCENARIOS

xSec is deployed by activating the xSec software license on an Aruba Mobility Controller and by installing Juniper Networks' Odyssey Client on a wired or wireless PC. xSec can be used to secure traffic between an Aruba mobility controller and a wireless client, between a Mobility Controller and a wired client, or between two Mobility Controllers on the same VLAN.



Odyssey Client connected to SSID "alpha-xsec" using xSec protocol



Configuring client to use xSec encryption on 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