



SecureAire Supplicant

A Secure Embedded WLAN Client

SecureAire Supplicant is a comprehensive embedded 802.11 client (supplicant) software package which implements IEEE 802.11's supplicant functionality and supports the latest wireless security standards including Wi-Fi® Protected Access (WPA™) and WPA2/IEEE 802.11i. The software is designed as a set of modular, application-agnostic components that deliver Wi-Fi security and standards-compliance. Besides providing the functionality of a full-fledged secure 802.11 client, its unique capability lies in its ability to make these services available to an embedded application in any domain through flexible APIs and configuration mechanisms, to make secure Wi-Fi connectivity a convenient add-on to any embedded device. SecureAire Supplicant is standards-based and can interoperate with other IEEE 802.11 compliant systems running on any platform or OS.

Wireless Security

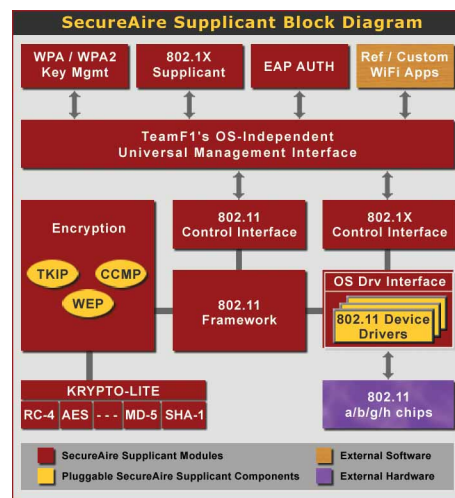
The use of a shared transmission medium -- airwaves with no well-defined physical boundary to be protected -- makes security a key issue in WLANs. Due to several deficiencies in the early 802.11 standard WEP (Wired Equivalent Privacy) security, the newer 802.11i standard and WPA2 is now implemented for most WLANs. Also, industry

standards such as Wi-Fi Protected Access (WPA) provide strong security while maintaining compatibility with legacy hardware. SecureAire Supplicant includes the latest wireless security technologies including 802.11i, as well as an implementation of WEP with static (104-bit or 40-bit) or dynamic keys which improves the security characteristics of the basic WEP functionality.

WPA / WPA2

SecureAire Supplicant includes support for Wi-Fi Protected Access (WPA) and the newer WPA2, which are currently the most popular and robust security mechanisms in use with WLANs.

SecureAire Supplicant supports 802.1x authentication with Extensible Authentication Protocol (EAP) which is a



Features

- ❖ Fine-grain developer (API) control of wireless features
- ❖ Support for 802.11e/WMM
- ❖ Concurrently supports various generations of 802.11 security
- ❖ Support for WEP, WPA and WPA2 in Personal and Enterprise modes
- ❖ Roaming between different APs using multiple profiles
- ❖ Migration mechanism for BSD/madwifi drivers
- ❖ Royalty-free full source distribution

required part of the WPA standard in Enterprise mode. For environments without a Remote Authentication Dial-In User Service (RADIUS) infrastructure, WPA offers the use of pre-shared keys (WPA-PSK), a feature built into SecureAire Supplicant. For data confidentiality, WPA defines the per-frame re-keying of the key used in unicast connections using the synchronized Temporal Key Integrity Protocol (TKIP). For data integrity, WPA defines the use of a 4-byte "MIChael" message integrity code. SecureAire Supplicant includes full support for TKIP and MIChael, both of which can leverage legacy hardware. SecureAire Supplicant also includes AES support in the "CCMP" mode of operation which is optional in WPA and mandatory in WPA2 / 802.11i.

802.11 Framework

SecureAire Supplicant divides the 802.11 supplicant functionality into two areas to allow simplified development of new chipset drivers by leveraging common elements of the 802.11 protocol implementation:

The Security Advantage

SecureAire Supplicant is a complete solution for network devices that require secure WLAN client functionality. It also includes Krypto-Lite, TeamF1's FIPS-certified common crypto framework, along with a suite of encryption and integrity components to secure and manage access point traffic. Krypto-Lite also allows the seamless integration of other optional security protocols developed by TeamF1 such as SSL/https, SSH and IPsec/IKE to meet additional security requirements.

- ❖ The generic 802.11 framework: includes common (device-independent) functionality of an 802.11 supplicant such as processing 802.11 management and data frames, key management and association to an access point (AP).
- ❖ 802.11 driver: works with specific 802.11 hardware and configures the device to send/receive frames.

SecureAire Supplicant includes reference drivers for popular radio chipsets and also provides a template driver to aid in the development of new drivers.

802.1X Access Control

SecureAire Supplicant includes a full implementation of the port-based network access control supplicant-side state

Standards Support

IEEE wireless standards

| | |
|--------------|---------|
| 802.11 a/b/g | 802.11i |
| 802.11d | 802.11e |

Security

TKIP & MIChael
 AES/CCMP
 WPA/WPA2 Pre Shared Key
 WPA/WPA2 Enterprise
 WEP (64/128 bit)
 Dynamic WEP re-keying with 802.1X
 Weak IV avoidance

EAP Support

EAP-MD5
 EAP-TLS
 EAP-TTLS/MS-CHAPv2
 EAP-TTLS/EAP-MS-CHAPv2
 EAP-TTLS/EAP-MD5
 EAP-PEAP/EAP-MS-CHAPv2
 EAP-PEAP/EAP-MD5
 EAP-MS-CHAPv2
 EAP Framework to support addition of new EAP types

machine defined by IEEE 802.1X. While 802.1X provides a framework for EAP-based authentication, it does not define the actual authentication mechanisms.

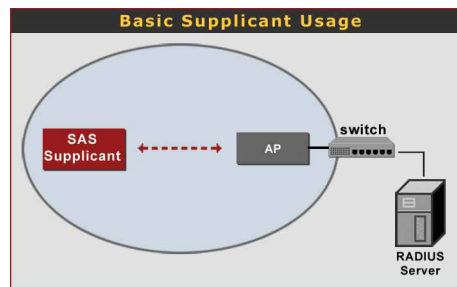
SecureAire Supplicant includes all popular EAP authentication mechanisms (MD5, TLS, TTLS and PEAP) and also provides an EAP framework to add new EAP types. New EAP types can be added using the existing APIs without requiring any change in the application.

Connection Profiles

SecureAire Supplicant also includes the ability to store and prioritize the order of wireless networks the supplicant can connect to, and API driven connection management with the ability to store the settings of a connection and then apply it on the interface which will eventually connect to the given AP in the profile.

Cryptography

SecureAire Supplicant includes **TeamF1's** FIPS certified **Krypto-Lite** software crypto



library including support for a variety of encryption and hash algorithms: DES, 3DES, AES, MD5, SHA. Other ciphers such as Arcfour, Blowfish, CAST128, RIPE-MD are available. The built-in cryptographic library can be used by the embedded application to implement additional security in the device. It can also be used by custom EAP authentication methods to provide X.509 certificate-based and other types of secure access control. The **Krypto-Lite** library includes support for FIPS certified

Also Available

- ❖ **SSecure Family**
Security protocols (SSL, SSH, IPsec/IKE)
- ❖ **AuthAgents**
Authentication agents: Kerberos, RADIUS, X.509
- ❖ **ASAP**
Air Secure Access Point
- ❖ **INSECTS**
Firewall, NAT and QoS disciplines

Custom Solutions

TeamF1's professional services can provide the resources and expertise to build customized applications with **SecureAire Supplicant** including wireless device driver development for additional chips.

algorithms - AES, DES/3DES, SHA, DSA, overridable PRNG and seeding capabilities, support for advanced cipher modes including AES-CCM-128, support for advanced SHA2 Message Digest Algorithms - SHA2-256, SHA2-384, SHA2-512, Diffie-Hellman groups: 1, 2, 5, 14. Optionally a FIPS 186-2 Appendix 3.1 PRNG is also available from TeamF1 for Krypto-Lite. The cryptographic library can be shared with other **TeamF1** security protocols for maximum reuse and code footprint efficiency, as well as ease of certification and export classification.

Built for Embedded Use

SecureAire Supplicant is a drop-in supplicant designed for embedded use. It has been extensively validated on a variety of CPU architectures, which minimizes development and integration efforts. **SecureAire Supplicant** is optimized with enhanced memory management & abstractions that are lean, yet fast. A common code base is provided for all supported target environments such as embedded variants of *Linux*®, *VxWorks*®, and others.

Email: sales@TeamF1.com
 Web: www.TeamF1.com
 Ph: 510-505-9931 ext. 5
 Fax: (510) 505-9941



© 2003-2006 TeamF1, Inc.