Security Mechanisms in 3eTI Products
Executive Summary

Public and private key encryption and authentication techniques both have merit and are both used in real-world systems. However, it is clear that for wireless security, symmetric-key encryption using U.S. Government-endorsed AES is an accepted methodology that is a critical building block in both IEEE 802.11i and IEEE 802.15.4 (ZigBee), which together cover high and low-data-rate, low-power wireless applications. IEEE 802.11i, IEEE 802.15.4, and Bluetooth all employ a cross-layered approach to security; however, Bluetooth currently implements SAFER+ for baseband encryption, while 802.11i and 802.15.4 employ AES for both encryption and authentication. All three wireless protocols rely on private encryption keys; therefore, key management and distribution over the insecure wireless channel has emerged as a problem that is at least as important as the underlying encryption cipher that is chosen within the wireless system.

The Standard Encryption Cipher: AES

Strengths of AES CCMP

AES CCMP mode provides both authentication and encryption using the AES block cipher. The CCMP protocol combines Counter (CTR) mode encryption for data privacy or confidentiality, and Cipher Block Chaining Message Authentication Code (CBC-MAC) authentication, for an authenticate-and-encrypt security process on each data block that is processed. CCMP has two prominent advantages for IEEE 802.11 security. First, it is particularly useful because it computes the CBC-MAC over the IEEE 802.11 header length, selected parts of the IEEE 802.11 MAC Payload Data Unit (MPDU) header, and the plaintext MPDU data; whereas the old IEEE 802.11 WEP mechanism provided no protection to the MPDU header. Secondly, both CCMP encryption and decryption employ only the forward AES block cipher function. In this way CCMP avoids use of the inverse AES cipher which is more costly and processing-intensive. Using only the AES forward cipher leads to significant savings in code and hardware size. Also, the CCMP implementation does not have to complete calculation of the message authentication code before CTR encryption can begin, allowing parallel implementation and further streamlining of AES CCMP in hardware or software. The benefits of both authentication and encryption on each data packet are clear. The CCMP mode of AES encryption is currently under consideration by the 802.11i task group for use in future wireless devices. 3eTI is working to implement AES CCMP and other 802.11i constructs throughout its product line of 802.11a/b/g compliant wireless Access Points, Bridges, and Client devices.

Secure Key Management and Distribution over Wireless

802.11i and Key Management Standards

The IEEE 802.11i proposed standard goes beyond the simple, flawed encryption mechanism of 1999 802.11 WEP standard to include specifications on encryption, authentication and key management in a multi-layered approach to security. IEEE 802.1X-based authentication mechanisms are used, with AES in CCMP mode, to establish an 802.11 Robust Security Network (RSN). IEEE 802.1X-2001 defines a framework based on the Extensible Authentication Protocol (EAP) over LANs (also known as EAPoL). EAPoL is used to exchange EAP messages. These EAP messages execute an authentication sequence and are used for key derivation between a Station (STA) and an EAP entity known as the Authentication Server. IEEE 802.11i defines a

Comparison of FIPS 140-2 and 802.11i Requirements

FIPS 140-2	802.11i
AES, 3DES, or Skipjack in ECB, CBC, CFB, OFB or CTR modes	AES-CCM (not NIST approved)
Mandated by US Government for SBU Cryptographic Systems (NSA Type 3)	Emerging Commercial Standard (prior standards not accepted by Government – e.g. WEP, TKIP)
Secure Channel between AP and AS for DKE	Does not address DKE (3eTI is working with Intel and Cisco on a NIST approved Key Wrapping Solution)
Requires individual implementation to go through validation	FIPS 140-2 validation is not a given – individual implementation must be separately validation (3eTI would like to provide validated client SW Driver for Centrino)
System must indicate when in FIPS mode vs. not (e.g. TKIP, WEP are not FIPS 140-2 compliant) 3eTI has experience architecting multi-mode FIPS compliant SW.	FIPS Mode indication not part of standard

four-way handshake using EAPoL for key management and pairwise and group key derivation.

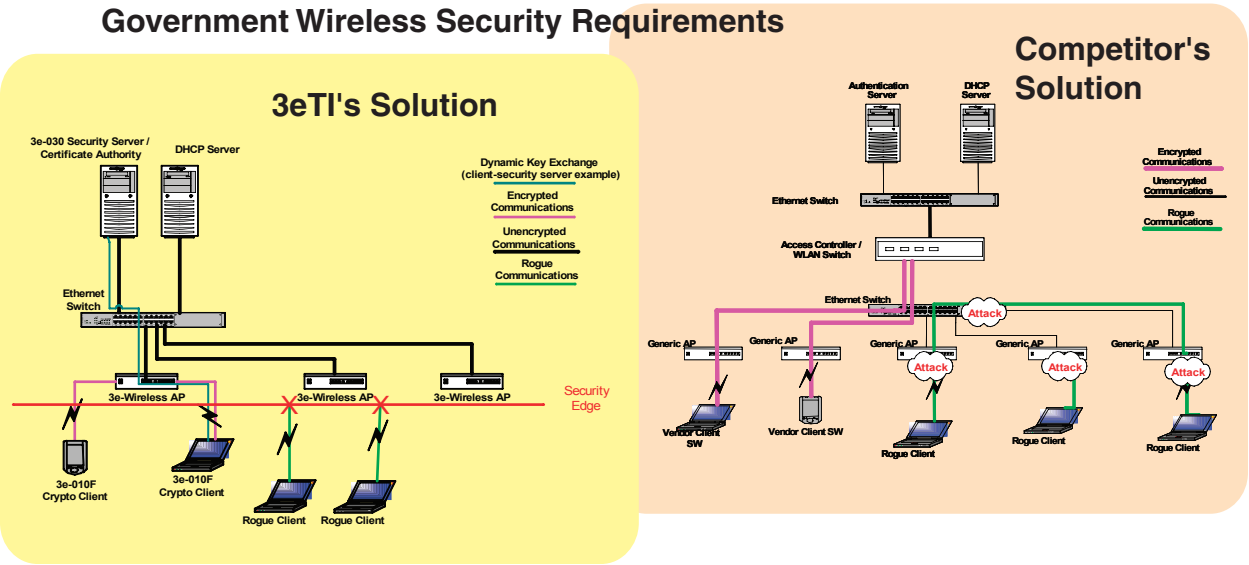
OSI Layer 2 Protection combined with IPSec Layer 3 VPNs

Readers familiar with networking systems will recall the Open System Interconnection (OSI) 7-layer model, which defines a networking framework for implementing protocols in these layers. IPSec provides an Encapsulating Security Payload (ESP), which is a protocol header inserted into an Internet Protocol (IP) datagram at the (layer 3) network layer. IPSec is intended to provide confidentiality, data origin authentication, antireplay, and data integrity services to IP frames. Virtual Private Networks (VPNs) typically rely on IPSec for implementing secure tunnels. The drawback to this approach is that for wireless systems, the datalink layer (layer 2) and physical layer (layer 1) frames are completely unprotected using IPSec alone. Spoofing and replay attacks on the MPDU and physical layer packets are possible. In general, for wireless traffic, security at layer 2 and above is advisable. 3eTI is developing AES for encryption and authentication at the datalink layer in accordance with IEEE 802.11i, providing secure protection of the wireless packet(s). As mentioned earlier, AES CCMP is particularly useful because it computes the CBC-MAC over the 802.11 header length, selected parts of the 802.11 MAC packet header, and the plaintext MAC packet payload. This approach , combined with dynamic key exchange and careful key management, provides strong protection of the wireless frames. IPSec can and should be used in the network above AES CCMP, for multi-layer security to provide comprehensive protection. Note that AES CCMP is recommended although FIPS 140-2 currently mandates use of the simpler AES ECB mode. Thus, a "best practice" recommendation would be that NIST incorporate the CCMP mode into its FIPS 140-2 standard.

3e Technologies International's Security Solutions

3e Technologies International (3eTI) has long been working in the forefront as a wireless solution provider. It is the leading provider of the most secure wireless infrastructure and applications utilizing FIPS 140-2 Validated™ wireless products, 802.11 Wireless Networking Solutions, Condition-based and Location-based Telematics Solutions, and Bluetooth Networking Solutions. 3eTI's solutions are aimed at multiple markets: U.S. Department of Defense, Federal Agencies, Enterprise, Manufacturing, and Industrial.

3e Technologies International Serves as Architect for Government Wireless Security Requirements



	3eTI Solution	3rd Party VPN
Distributed Architecture	Each AP encrypts multiple clients Each AP carries small load	Server handles all Clients Server carries full load
Ease of Use	Login connection is seamless	Often requires dual logins.
No Central Bottleneck	Server centralizes authentication, encryption distributed	Server handles everything in one box
Robust and Reliable	Loss of one or more APs reduces coverage, not security	Loss of VPN server could lead to total loss of security

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

3eTI Dynamic Key Exchange and Robust AES Encryption

Dynamic Key Exchange: 3eTI has developed an innovative Dynamic Key Exchange (DKE) technique for effective key management in wireless systems involving a Security Server (SS), an Access Point (AP) and multiple wireless Client devices. The communication channel between the AP and the Client devices is wireless IEEE 802.11, while the channel between the AP and the SS is wired. The description of the DKE process follows: First, the SS and Client devices must obtain X.509 certificates from a 3rd party Certificate Authority. This can be accomplished in a number of ways. Typically, RSA is used to authenticate these certificates.

Once the X.509 certificates are in place, to initiate the DKE sequence, a Client device first associates with an AP. Once association is successful, authentication messages (and only authentication messages) are permitted to flow between the Client and the SS through the AP. Next a mutual authentication process between the Client, AP, and SS will ensue, followed by a key exchange process. In the authentication process, EAP-TLS is used for mutual authentication. EAP-TLS encapsulates EAPoL, which is used to achieve mutual authentication between the Client and the AP. Meanwhile, between the AP and the SS, Remote Authentication Dial In User Service (RADIUS) protocol using HMAC-SHA1 keyed authentication is used to establish mutual authentication over the wired channel. EAP-TLS is then used to establish mutual authentication between the Client and the SS. At this point, authentication, or proof of valid identity, has been established throughout the wireless network (Client, AP, SS).

Following successful authentication, the dynamic key exchange process is initiated. As a result of the completed authentication process described above, a Pairwise Transient Key (PTK) was generated at the Client device and the SS. Next, Diffie-Hellman protocol is used to exchange an AES encryption key between the SS and the AP. Then, FIPS 197-compliant AES is used to encrypt a message that transfers the PTK from the SS to the AP. In this way, the PTK is securely passed to the AP. Now, both the Client and the AP have the PTK. This PTK will be used to AES-encrypt all unicast traffic between the AP and Client. A FIPS 140-2 compliant random key generator is used at the AP to generate the key which will be used to AES-encrypt all broadcast traffic between the AP and Client. Next, FIPS 197-compliant AES is used to encrypt a message that transfers the broadcast key from the AP to the Client. At this point, the AP and Client have both the unicast key and the broadcast key to perform layer 2 AES protection of the wireless channel. This DKE process can be selectively re-invoked whenever a Client device initiates the process by associating to an AP, or when a new Client joins the wireless network.

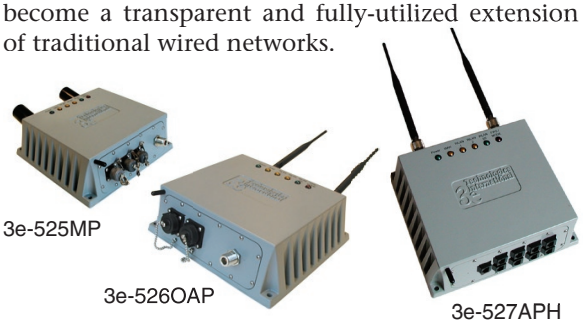
FIPS 140-2 Validation: The 3eTI DKE process and 3eTI AP and Client devices have received FIPS 140-2 validation (refer to NIST certificates #355 and #367). The FIPS 140-2 validation process entails rigorous testing and proof-of-secure-design that is administered by a NIST-endorsed independent laboratory. FIPS 140-2 Validation is required for all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106 . This process ensures that the wireless cryptographic systems fielded by 3eTI are sufficiently robust and secure for use by all U.S. Federal agencies to protect sensitive information. Furthermore, the physical security required by FIPS 140-2 has been leveraged in 3eTI products to produce ruggedized enclosures that are suitable for use in harsh environments typically found in multi-service battlespaces, including Navy shipboard control and monitoring rooms, and - potentially - mobile Army caravans and vehicles. FIPS 140-2 validation ensures correct construction and implementation of the cryptographic functions within a rigorously defined “cryptographic boundary”.

CC Certification: The Common Criteria (CC) contains 15 international recognition participants and is an international standard for Information Assurance (ISO/IEC 15408). All IT security products purchased by the U.S. Government for National Security Systems are required to be Common Criteria certified as of July of 2002 if corresponding Protection Profiles are approved for that type of product. In anticipation of Protection Profiles gaining final approval, many government agencies (especially the DoD) are writing CC validation into new RFPs requiring government vendors to comply with this directive. Currently, 3eTI is the only vendor that claims conformance to the new, NSA-sponsored Basic Robustness Protection Profiles for WLAN Access System and WLAN Client devices.

Future initiatives

IEEE 802.11i, AES CCMP, ECC, and IPSec are useful techniques for certain purposes and pieces of an overlapping, comprehensive security solution; however, they are all passive network intrusion prevention techniques. 3eTI sees a growing trend toward including active intrusion prevention, along with traditional passive encryption, authentication, and network-based and host-based intrusion detection techniques to secure future networks. Certain emerging active intrusion prevention constructs are designed primarily to protect wireless networks, including the use of directional antennas, with adaptive beamforming and null-steering, to effectively provide an “invisible fence” or RF-boundary (layer 1)

around the deployed wireless LAN. Smart antennas are coming down in cost and therefore becoming more practical for enterprise or company-wide 802.11 networks. These smart antennas will be used to complete the multi-layered security approach by adding physical-layer security techniques to the existing datalink and higher-layer techniques previously described in this paper. 3eTI has used Small Business Innovation Research (SBIR) contract vehicles to actively pursue research in the area of 802.11 intrusion prevention and smart antenna development, which will in the future reinforce the wireless infrastructures that since the days of 802.11 WEP have steadily gained a reputation of inherent insecurity. Adaptive beamforming and beamsteering, coupled with 802.11i constructs and other higher-layer intrusion prevention techniques, provide a multi-layered approach to security that is necessary to ensure wireless LANs become a transparent and fully-utilized extension of traditional wired networks.



3e-525MP

3e-526OAP

3e-527APH

Competitive Analysis

Features	AP Layer 2 Encrypt.	Switch Layer 2 Encrypt.	Switch Layer 3 Encrypt.	AP Layer 3 Encrypt.
	3eTI	**Air Fortress Cranite**	**Reef Edge**	**Colubris (L3)**
Built-in Redundancy	✓			✓
Distributed Bandwidth	✓			✓
Wired Equivalent – Per Connection Privacy	✓	✓	✓	✓
Login handled like wired clients (i.e. domain authen)	✓			
Seamless Subnet Roaming	✓	✓	✓	
Security perimeter at edge / minimize security risk	✓			✓
Clients have one point of administration – don't need to configure wireless card and VPN client.	✓			
Immune to VPN split tunnel / L2 Trojan attacks	✓			

Summary

This paper has discussed the benefits of AES CCMP, ECC, IPSec, EAP-TLS, and other IEEE 802.11i constructs for encryption, authentication, and key management. A combination of some or all of these techniques will result in a cross-layered approach to security that provides more comprehensive protection of the dataflows in either wired or wireless systems. We have explained in our analysis of OSI Layer 2 Protection vs. IPSec Layer 3 VPNs that for wireless traffic, security at layer 2 and above (i.e. layers 3 and 4) is advisable. This methodology is underscored in the 3eTI approach and design of a Dynamic Key Exchange system. The need for FIPS 140-2 validation and CC certification for use in cryptographic systems fielded by U.S. Federal agencies was reviewed.

3eTI has placed secure wireless networks on U.S. Navy ships and military bases, proving the power and efficacy of our wireless networking solution. Our 3e-521NP and 3e-530NP Access Points both contain FIPS 140-2 Validated Level 2 secure encryption modules, coupled with the 3e-030 Security Server software using the DKE Key exchange method and clients fully encrypted using the 3e-010F FIPS 140-2 Validated Level 1 secure encryption modules. 3eTI is working to include 802.11i and to include it in a FIPS 140-2 validated solution in future wireless products. Our new line of Access Points (3e-525MP, 3e-526OAP, and 3e-527APH) combine IEEE 802.11b, 802.11g, and 802.11a functionality into multiple platforms for use indoors and outdoors, as stationary or mobile wireless bridges, repeaters, and LAN switches. All of the new APs employ FIPS 140-2 Certified Crypto Modules to deliver the most secure encryption available - AES or 3DES. All of the new APs meet the most stringent military specifications for vibration, shock, EMI, humidity, temperature, and close proximity ordinance. Upgrades to the 3e-525MP and 3e-527APH models will include Department of Defense Public Key Infrastructure (PKI). PKI is the mechanism needed to support critical DoD applications with public key certificates. PKI-based applications afford confidentiality and authentication to communications or network transactions, as well as verification of the data integrity and non-repudiation of these transactions.

As with 3eTI's current FIPS 140-2 certified products, the new products are integral components of the 3e WLAN Security Suite, which offers supplemental Security Server Software for dynamic user keys. For added security, a VPN can be used in addition to AES and DKE security solutions to complete the multi-layered approach. This multi-layered solution of end-to-end, FIPS-compliant hardware and software provides an easy to install and manage high security wireless solution, for Government Agencies and discerning security-mindful consumers.