

Achieving Wireless Security with Interoperability

by: Ryon Coleman, 04/29/2005

<http://www.securitydocs.com/library/3241>

Abstract

Though the concept of an ultra-high level of wireless networking security and information assurance is somewhat opposed to the concept of open interoperability with a wide spectrum of 3rd party vendors' wireless equipment, this paper is intended to show that 3eTI FIPS 140-2 validated and Common Criteria certified wireless equipment are interoperable with multiple vendors' IEEE 802.11-compliant equipment, and that 3eTI solutions are non-proprietary. 3eTI has blazed the trail in marrying the IEEE 802.11i commercial standard for enhanced wireless security with FIPS 140-2 validation requirements per the NIST Cryptographic Module Validation Program (CMVP). 3eTI wireless equipment will meet the IEEE 802.11i specification, WiFi certification requirements, as well as the stringent security requirements for U.S. Federal Agencies specified by FIPS 140-2 Level 2 and Common Criteria EAL2+ and EAL4+ assurance levels. 3eTI, working together with Cisco and Intel, has developed an IETF RFC draft to further standardize the key exchange technique employed between an Authentication Server (AS) and Wireless Access Point (WAP), that was left outside the scope of IEEE 802.11i. 3eTI continually leads the industry in standardizing proven techniques and algorithms through the IEEE and the IETF, in order to provide the best value and choice of vendors to the U.S. Department of Defense, other Federal Agencies, and security-minded enterprises.

Wi-Fi Certification of 3eTI Wireless Products

In order to interoperate with a large market share of industry-standard wireless equipment which are based on the Intersil and Atheros chipsets and drivers, 3e supports a non-FIPS mode which is fully Wi-Fi compliant. Today, 3e equipment is compatible with Intersil Prism 2.5 and higher (Linux and Windows drivers), Atheros (Linux and Windows drivers), and Centrino (Linux driver). The near-term 3e roadmap is to interoperate with as many wireless cards and drivers as possible in the commercial wireless market. In fact, interoperability testing with 3rd party equipment is a cornerstone of standard ETP (Engineering Test Planning) at 3eTI. Recent standards activities, such as the ratification of 802.11i, ensure that interoperability testing will prove successful. The primary difference in the 3e solution and others is that we replace the active NDIS driver from the manufacturer with our 3e driver (Crypto) NDIS. While this does require us to build drivers for each chipset type, it also offers a greater level of layer 2 encryption over other solutions which only really achieve layer 2.5 of the OSI model without directly building a NDIS driver. The Prism2.5 and Prism3 chipsets are evolutions of the PrismII chipset, offering even higher integration, lower cost and backward compatibility. With respect to the driver, these (3) chipsets look the same, and therefore the 3e driver supporting PrismII hardware also supports Prism2.5 and Prism3 hardware. Therefore, 3eTI's solution is not proprietary, but rather delivers added wireless security at a lower level in the system to make it more secure than Layer 2.5/3 solutions.

IEEE 802.11i and IETF Key Management

IEEE 802.11i goes beyond the simple, flawed encryption mechanism of 1999 802.11 WEP 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 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 (AS).

IEEE 802.11i defines a four-way handshake using EAPoL for key management and pairwise and group key derivation. 3eTI has been instrumental in developing an IETF RFC to further standardize the portion of key exchange that must take place between the Authentication Server and the Wireless Access Point (WAP). 3eTI, along with Cisco and Intel, recognizes the merits of standardizing this technique, so that interoperability among multiple 802.11i-compliant vendors can be achieved.

EAP is not tied to any particular authentication algorithm and is therefore highly extensible. It defines a small number of messages used to communicate between the Authentication Server and the EAP Client. This design allows the two peer entities to mutually determine whether or not the newly connected device should be granted access to the network, based on the algorithm-specific authentication credentials, such as the user's identification and password. The Authenticator is able to interpret the outcome of the negotiation without being required to participate in the negotiation itself, by simply recognizing an EAP-Success or EAP-Failure message. EAPoL carries EAP messages between the Supplicant, for example a wireless client device, and the Authenticator. The Authenticator acts as a relay for EAP packets by extracting them from within the EAPoL frames and sending those EAP packets to the Authentication Server. The authentication process allows the Authenticator and the Supplicant to prove to each other that they both know a shared secret, the Pairwise Master Key (PMK). It is essential that this be done without divulging the PMK to eavesdroppers. The Supplicant and the Authenticator cannot trust each other until they have securely determined that each party knows the PMK. In order to establish that trust relationship, the Authenticator and Supplicant use the 802.11i four-way handshake to convince each other that they are who they claim to be, and to mutually derive the necessary encryption and authentication keys from the PMK. The four-way handshake does not reveal any essential keying information to eavesdroppers, but does provide each party with proof that they both know the PMK. 802.11i provides crucial security enhancements to 802.11 wireless, including complete protection of the Layer 2 packet, i.e. both header and payload. It also provides the framework for strong, mutual authentication between the Supplicant (client) and the Authenticator (security server). Through 802.11i and the IETF RFC for key exchange, 3eTI promotes interoperability and includes it as a requirement with ongoing product development. 3eTI uses strong security at Layer 2 that is compatible with 802.11i for commercial interoperability, while at the same time this security conforms to FIPS 140-2 requirements to meet rigorous Federal guidelines. 3eTI is on-track to begin 802.11i Wi-Fi interoperability testing as soon as it becomes a component of Wi-Fi (expected Q42004).

DoD PKI & PKE Applications

Many programs supporting the Department of Defense (DoD) missions require security services, such as authentication, confidentiality, non-repudiation, and access control. To help address these security problems, the DoD developed a Public Key Infrastructure (PKI). The DoD PKI provides products and services that enhance the security of networked information systems and facilitate digital signatures. DoD PKI is a requirement to ensure interoperability throughout DoD local and wide-area network infrastructure, both ashore and afloat, across multiple services. 3eTI already uses an X.509 certificate-based architecture in the WLAN encompassing its Security Server, Wireless Access Points, and Wireless Clients. This architecture is being modified to support JITC-approved certificates, multiple root certificates, the Certificate Authority hierarchy, and posted Certificate Revocation Lists (CRLs), all in compliance with DoD PKI. The JITC PKI Test Certificate Lab provides test certificate services in support of DoD and commercial partners to help successfully deploy a fully interoperable PKI. Applications must be tested to ensure they are enabled correctly, and are interoperable with the DoD PKI. The DoD PKI Program Office established the JITC DoD PKE Certification Lab as an independent testing facility to perform interoperability testing on PKE applications. It is DoD policy that enabled applications be tested to ensure interoperability and compatibility with the DoD PKI. The JITC DoD PKE Certification lab supports this policy through the interoperability certification process. The certification process is based on a master test plan containing all DOD PKE requirements and associated tests. This plan is used as a guideline for testing individual applications. Through this independent testing process, 3eTI WLAN equipment is certified compliant with the DoD PKI and therefore interoperable across multiple DoD agencies. DoD PKI is not targeted toward the commercial user, and as such is not used by commercial customers. For commercial users, DoD PKI can be disabled and simpler static or RADIUS-like dynamic key management can be used, for easy interoperability with non-DoD PKI commercial equipment.

IPSec and VPN for Interoperability

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, anti-replay, and data integrity services to IP frames. Virtual Private Networks (VPNs) typically rely on IPSec for implementing secure tunnels. VPNs with IPSec, though not as strong as layer 2 security for

wireless, permit interoperability with many vendors, and across wireless as well as wired LANs. The drawback to this approach is that for wireless systems, the datalink (layer 2) and physical (layer 1) frames are completely unprotected using IPSec alone. Spoofing and replay attacks on the MPDU (MAC Payload Data Unit) and physical layer packets are possible. In general, for wireless traffic, security at layer 2 and below 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). AES CCMP as per 802.11i is particularly useful because it computes the CBC-MAC over the 802.11 header length, selected parts of the 802.11 MPDU header, and the plaintext MPDU data. This approach, combined with dynamic key exchange and careful key management, provides strong protection of the wireless frames. IPSec can still be used in the network above AES CCMP, for multi-layer security to provide comprehensive protection. By incorporating 802.11i at layer 2, as well as IPSec VPN at layer 3 and a standards-based RFC for extended key exchange, 3eTI is adhering to standards-based technology and will provide several interoperable modes of operation. If additional security is required, 3eTI provides an enhanced feature set of FIPS validated and CC certified features that can be enabled for increased security, when interoperability is not of chief concern.

As a caveat, it should be pointed out that the use of VPNs do not guarantee interoperability. There are many cipher suites supportable with IPSec, which is used by typical VPNs, and there is no guarantee that a "VPN client" will be using the same IPSec cipher suite as, say, a "VPN Access Controller". VPNs are not only layer 3, but often run outside of the firewall, effectively forcing all clients to look like remote users, whereas the 3eTI solution seamlessly extends the wired network. However, if the IPSec cipher suites are agreed upon, VPNs can be used as an interoperable solution. Between VPN use and implementations of 802.11i for the wireless link, 3eTI adheres to standards-based, interoperable architectures.

Conclusion

3eTI provides high levels of security in its wireless products. 3eTI also recognizes the merits and value to the customer of providing interoperable solutions. This paper has shown that through WiFi certification, IEEE 802.11i and IETF standard key exchange techniques, DoD PKI and PKE compatibility, and IPSec for VPNs, 3eTI goes to great lengths to ensure interoperability requirements are met for its customers. 3eTI actively participates in the IEEE and IETF standards bodies and development procedures, in order to ensure that the most technically robust and proven techniques are adopted within standards bodies. 3eTI is committed to meeting these standards and achieving interoperability constraints for all of its DoD customers, as well as for enterprise markets. 3eTI's solutions have the appearance of being proprietary because the user must use the 3eTI supplied wireless client driver, but this is necessary to implement a layer 2 wireless solution. Any solution that uses the existing Windows NDIS driver is actually a layer 2.5/3 solution and is susceptible to attack. By complying with 802.11i at layer 2, 3eTI ensures a wide range of interoperability now that 802.11i has been officially ratified.