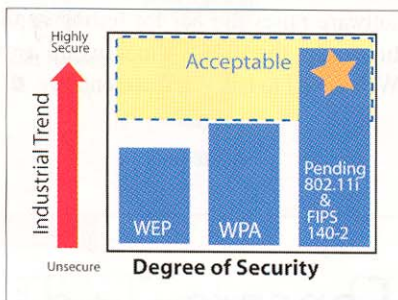


The Case for Advanced Wireless Security Systems

Make your data hackproof with AES and dynamic key technology.

3e Technologies International
700 King Farm Blvd., 6th Floor
Rockville, MD 20850
301-670-6779
Fax: 301-670-6989
bdrake@3eti.com
www.3eti.com



**Highly Secure
Wireless Solutions**

**FIPS 140-2
Validated™ Products**

3e-8210P Wireless Access Point
3e-82510G Wireless Access Point
3e-4107 Crypto Client Software
3e-3000P Wireless Access Point

Wireless sensor and control signal transmission has become technically and economically attractive. With cabling costs at \$100+/ft., wireless signaling provides an economical alternative well within the factory floor geometry. However, concern is regularly expressed regarding measures taken for signal authentication and encryption. A typical response usually is, “I don’t care if someone ‘listens in’ and sees what the pressure in Tank 3 is. It’s not like credit card data or company secrets.” That may be true, but the impact should be completely evaluated.

When multiple wireless security approaches (WEP, WPA, LEAP, etc.) were found to be vulnerable, the U.S. government halted use of off-the-shelf commercial wireless technologies. A DOD order banning wireless without approved and tested security was issued. The task of evaluating security technologies, devising standards, and testing was assigned to the National Institute for Standards and Technology in partnership with the National Security Agency. The result was a wireless security validation process—Federal Information Processing Standard (FIPS) 140.

Consider the Possibilities

A competitor sits outside your plant and monitors process signals, keeping track of inventories and production capabilities. This strategic information is then used to secure customers with delivery commitments that the competitor knows you cannot meet. Think about a plant malfunction requiring a quick delivery of some supply to clean things up and bring systems back online. Your competitor monitored your signals, knew about the problem, and tied up availability of required supplies. The result: You’re shut down while the competitor takes customers. Your sensor signal information was not secure, and it was openly broadcast, for free, beyond your factory fence!

A computer hacker—or, even worse, a terrorist—monitors your signals and figures out the format and content. He or she then modifies your communication and transmits it back with broadcast power greater than your transmitter’s. Your wireless receiver shifts to the stronger signal and receives highly abnormal readings, which trigger tragic results.

802.11i with AES and Dynamic Key Distribution to the Rescue

Wireless technologies need to have advanced encryption such as AES, which makes it so difficult to intercept and decode that hacking attempts would produce an unusable result. Transmitted information contains the encryption method and key, so it is also important to continuously modify the key. This is critical for systems that transmit repetitive information such as tank readings. With repetitive digits (e.g., tank levels that change slowly), the encoding could easily be compromised. With dynamic keys, transmitted data are repeatedly re-scrambled and the correlation between data and digits transmitted is not obvious.

The Security Solution to Enable Your Wireless Signaling Project

3e Technologies International’s (3eTI) wireless products have passed the U.S. government’s FIPS 140-2 testing and meet the DOD’s Security Directive 8100.2. Additionally, 3eTI’s security suite is a pre-802.11i solution that delivers rock-solid wireless protection with AES encryption, authentication certificates, and dynamic key management. It is a distributed OSI Layer 2 solution vs. a Layer 3 VPN approach, which is vulnerable to Trojan attacks and single point of failure. In addition to 802.11a/b/g networking, 3eTI has developed 1451.5-based Bluetooth and ZigBee enhancements. 3eTI delivers industrial-strength solutions with hardened security and high performance for harsh environments. ■