

Ensure It's Secure

Validated security protects your wireless network

By John Jacobs

3e Technologies International

Remember the scene from Ocean's Eleven, when hackers broke into the computerized security system at the Bellagio, letting thieves walk away with millions of dollars? Threats to security are not simply fodder for motion pictures—they are a reality that must be

The implementation of the security algorithm is as important—if not more important—than the algorithm itself. In wireless networks, WPA and 802.11i are known to offer true Layer 2 (LAN networking) protection.

dealt with proactively and aggressively. A data compromise at the hands of hackers could prove disruptive to operations—not only in slowing valuable production output and draining financial resources, but also in putting intellectual and physical property at risk.

For example, in a short film created by Idaho National Laboratories, they show results of a simulated attack on a power network, including a turbine that dramatically overheats and shuts down. The simulation demonstrated the devastating impact of the shut down—a type of situation that can be avoided through wireless equipment monitoring.

When Honeywell and 3e Technologies International (3eTI) teamed to create the mesh capabilities of the OneWireless universal network, providing state-of-the-art security was a top design consideration from the outset. The 3eTI multinode module creates an integrated, secure mesh network designed specifically to prevent breaches of data security without adding complexity to the OneWireless solution.

ADAPT to Emerging Threats

Today's threats to data integrity are very real and require a proactive, multi-pronged approach to total network security. The multinode was designed to ADAPT to the most challenging security dangers.

Access is the first step in controlling who is allowed on the network. While a

proper system design gives access only to authorized users, that access needs to be layered with authentication to ensure the true identity of the person on the network. Authentication is achieved via the use of passwords, digital certificates, control lists, and EAP-Transport Layer Security.

Denial of service prevents outsiders from jamming or interfering with a network. To stay ahead of hackers, tech-

niques such as frequency hopping, spread spectrum, and RF beam steering are used. Denial of service can be achieved via the placement of directional and polarized antennas, and by ensuring perimeters are secure.

Authenticity—also known as anti-spoofing or repudiation—is a means of refusing network access. Effectively denying access requires both authentication and ongoing monitoring. Examples of functions used to ensure authenticity include HMAC, or Hash Method Authentication Code.

Privacy is a primary goal of network security—providing data only to those who need it, ensuring confidentiality and preventing hacking. Privacy is achieved via encryption, system planning and design, and system monitoring. Some common examples of encryption algorithms are AES and 3DES.

Testing devices against proven standards by independent third parties is a best practice in ensuring network security, since not all security is created equal. The implementation of the security algorithm is as important—if not more important—than the algorithm itself. In wireless networks, WPA and 802.11i are known to offer true Layer 2 (LAN networking) protection. It is also important to independently certify the security works to the extent it claims to work, which is why the U.S. Department of Defense and many international users now require 802.11i and FIPS 140-2 Validation of encryption devices.

Proven Security in Hostile Environments

Because the Department of Defense requires the utmost in wireless networking security, only those solutions with proven track records of safeguarding data are implemented in military applications. 3eTI's mesh nodes have been proven to withstand the rigorous requirements of one of the most challenging environments: aboard vast war-fighting ships traveling in dangerous open seas.

Confidential, secure wireless communications aboard navy vessels are essential for sailors performing the thousands of tasks associated with ship operations. 3eTI designed a shipboard wireless local area network (WLAN) that allowed installation of sensors on critical equipment to report status in real time. The system—which also enabled sailors to send data securely over a wireless network—is ideal for use in industrial applications requiring streamlined, secure operations.

The WLAN designed for the U.S. Navy meets the Department of Defense's requirement for the FIPS 140-2 Validated security needed to protect soldiers and critical assets. 3eTI was one of the first companies to have its WLAN infrastructure FIPS 140-2 Validated, and has since had more than 14 wireless products validated to the standard. ■

3eTI High Performance Mesh for Industry

The mesh network design begins with a root node that acts as a gateway to the wired network. As nodes are added, they are automatically discovered by the mesh, and secure virtual bridge connections are established to each new node. The mesh intelligently selects the shortest, "lowest cost" paths, which are continuously optimized. If a node should fail, the mesh detects the failure and automatically reconfigures the network around it. As the mesh network grows, redundant root nodes can be added to enable expansion to cover additional geography throughout an operation.