Apply Security Standards to Wireless Problems

Jon Titus, Senior Technical Editor

Wireless communications, unlike their wired point-to-point cousins, can reach far and wide and thus prove more susceptible to hacking, spying, and damaging attacks. But you might think, "We only transmit digital temperature values that mean nothing to anyone else, so wireless security isn't a big deal."

But even in such a case, you must worry about security. "People could monitor data to determine its format and then mount a spoofing attack," explained John Schwartz, technology strategist at Digi International. "They could then send your control equipment false temperatures that alter a process. Security becomes important even for what people think of as mundane data."

"While security always comes at an additional cost, it is important to stress the cost depends on what you want to protect" stressed V.C. Kumar, program manager for embedded RF at Texas Instruments. "There's a difference between protecting communications from wireless bar-code readers in a store and securing wireless communication of financial information. So how important is securing information, for example, and what does it cost in time, material, engineering, and manufacturing to add the needed security? Unfortunately, sometimes when product designers look at wireless-security issues, they want to take a cookbook approach and use a single security model across applications, but usually that's not efficient or effective."

"When you plan for wireless security, always ask, 'What data will I send?' 'How important is it?' and 'What happens if someone gets their hands on it?'" said Schwartz. "At a minimum, we recommend people use the Advanced Encryption Standard [AES]. Then when a manufacturer produces a wireless product it includes a pre-shared key so every wireless packet gets encrypted with it."

Many equipment designers will not have to create or license an AES algorithm, though. Transceivers that comply with the IEEE 802.15.4 standard, for example, must include AES capability with a 128-bit key. That means protocols such as ZigBee, RF4CE, and 6LoPAN, which operate through such transceivers, already have built-in encryption as well as their specific security elements.

"The ZigBee Smart Energy profile has its own security that involves a level of trust

based on a pre-shared key," said Schwartz. A device can use its key to join a Smart Energy network but before the network lets this device transmit or receive information, the network's 'trust center' asks the device for a certificate. If the center verifies the authenticity of the certificate it shares a new security key with the device that may then communicate information. Certicom Corporation issues the certificates to equipment vendors who then "bind" a certificate to the MAC address for each network-capable device. So far, Certicom has issued over 16-million ZigBee Smart Energy certificates.

"Because so many wireless applications rely on standards, such as ZigBee, Bluetooth, and WiFi, you already have security supported in hardware and software," said Kumar. "And designers have choices. They might say, 'I don't need the entire suite of security options, I just need authentication and encryption.' Just because additional security capabilities exist, they don't need to use them. If you require compatibility with third-party ZigBee devices, though, you must adhere to the security in the standard."

Some hack-proofing security comes built into hardware that conforms to a standard such as 802.15.4. "That standard includes direct-sequence spread spectrum and it provides for many channels at 900 MHz and 2.4 GHz," said Schwartz. "Usually a device has a Personal Area Network [PAN] identifier and it will communicate only with devices that have the same PAN ID value. Designers can create combinations of many radio-operating parameters to make their device somewhat unique and they could change them day by day or even hour by hour. The next time a 'spy' looks for a transmission it might operate on a different frequency and in a different format."

"When you communicate financial or personal-identity information, you must demonstrate that your protocols adhere to a standard and provide a specific level of security," explained Kumar. "You can work with certification bodies and third parties to verify your security implementation. The Federal Information Processing Standards [FIPS] publications, provided by the US National Institute of Standards and Technology, offer information about security. Industry bodies such as the Bluetooth Special Interest Group, ZigBee Alliance, and the Wi-Fi Alliance also provide information about certified test labs for their standards."

"Always view communication security from an end-to-end perspective," cautioned Schwartz. "When engineers design a small wireless link, 128-bit AES encryption might provide their entire security. But information might go through a gateway that connects to the Internet and a 'cloud' database. Then you have users who access the data via an iPhone app. Each communication section has security that you must ensure people use. And you must ensure people can't get into other parts of your system or databases just because they have a valid user name and password. Your entire security protocol can be compromised by a secretary with her user name and password taped to her computer display."

For more information

Lemos, Robert, "Hacking the Smart Grid," MIT Technology Review, April 5, 2010. www.technologyreview.com/printer_friendly_article.aspx?id=24977.

Masica, Ken, "Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments, April 2007. tinyurl.com/3v32zpt.

NIST Releases Update to Smart Grid Framework. www.nist.gov/smartgrid/grid-102511.cfm.

Padgette, John and Karen Scarfone, "Guide to Bluetooth Security," NIST Special Publication 800-121 Rev. 1. csrc.nist.gov/publications/drafts/800-121r1/Draft-SP800-121_Rev1.pdf.

Schneier, Bruce, "Secrets and Lies: Digital Security in a Networked World," Wiley, 2004. ISBN: 978-0471453802.