PHYS.ORG

NIST Issues Guidelines for Ensuring RFID Security

April 27 2007

Retailers, manufacturers, hospitals, federal agencies and other organizations planning to use radio frequency identification (RFID) technology to improve their operations should also systematically evaluate the possible security and privacy risks and use best practices to mitigate them, according to a report issued today by the National Institute of Standards and Technology.

“RFID tags, commonly referred to as smart tags, have the ability to improve logistics, profoundly change cost structures for business, and improve the current levels of safety and authenticity of the international pharmaceutical supply chain and many other industries,” said Under Secretary of Commerce for Technology Robert C. Cresanti. “This important report lays the foundation for addressing potential RFID security risks so that a thoughtful enterprise can launch a smart tag program with confidence.”

RFID devices send and/or receive radio signals to transmit identifying information such as product model or serial numbers. They come in a wide variety of types and can be as small as a grain of rice or printed on paper. Unlike bar coding systems, some RFID devices can communicate without requiring a line of sight, and over longer distances, for faster batch processing of inventory. They can be outfitted with sensors to collect data on temperature changes, sudden shocks, humidity or other factors affecting products.

However, as RFID devices are deployed in more sophisticated applications from matching hospital patients with laboratory test results to tracking systems for dangerous materials, concerns have been raised about protecting such systems against eavesdropping and unauthorized uses. The new NIST report focuses on RFID applications for asset management, tracking, matching, and process and supply chain control. It lists of recommended practices for ensuring the security and privacy of RFID systems, including firewalls that separate RFID databases from an organization's other databases and information technology (IT) systems, encryption of radio signals when feasible, shielding RFID tags or tag reading areas with metal screens or films to prevent unauthorized access, and other security measures.

Two case studies—in health care and supply chain settings—provide examples for identifying and minimizing security risks throughout the various stages of an RFID project.

Citation: T. Karygiannis, B. Eydt, G. Barber, L.Bunn and T. Phillips. Guidelines for Securing Radio Frequency Identification (RFID) Systems (Special Publication 800-98), 154 pages. Available on-line at csrc.nist.gov/publications/nis … 800-98_RFID-2007.pdf .

Source: NIST

Citation: NIST Issues Guidelines for Ensuring RFID Security (2007, April 27) retrieved 19 April 2024 from https://phys.org/news/2007-04-nist-issues-guidelines-rfid.html