NIST Advises on RFID Security Risks

May 1 2007

The National Institute of Standards and Technology describes some potential dangers of implementing RFID and offers guidelines and best practices for mitigating the risks.

Recognizing the potential risks inherent in the use of RFID technology, the National Institute of Standards and Technology, a nonregulatory agency of the U.S. Department of Commerce, has published its guidelines for deploying radio-frequency identification.

The Guidelines for Securing Radio Frequency Identification Systems, released April 27, are geared toward retailers, manufacturers, hospitals, federal agencies and other organizations that might utilize RFID along their supply chains. The 154-page document describes potential risks to data security and privacy that RIFD might engender. It also offers best practices and guidelines on how to mitigate some of those risks.

The NISTT Information Technology Laboratory is well suited to the task of handing down RFID best practices. The group develops tests, test methods, reference data, proof-of-concept implementations and technical analysis in order to "advance the development and productive use of IT," according to the guidelines.

The guidelines discuss the nature of RFID systems that companies might implement, the type of data that might be relayed from one system to another and the risks associated with implementing the technology. The paper lists four major risks companies face: business process risk; business intelligence risk, privacy risk and externality risk.

Business processes are at risk through potential "direct attacks" on RFID system components and could potentially undermine the processes the RFID system was designed to enable, according to the paper. The authors of the report - Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn and Ted Phillips - give the example of a warehouse that relies solely on RFID to track items. An attack on system components could result in an inability to process orders.

A business intelligence risk could happen when an adversary or competitor gains unauthorized access to RFID-generated information and uses that information to "harm the interest of the organization," the report said.

"The example here is someone using an RFID reader to determine whether a shipping container holds expensive electronic equipment, and then targeting that container for theft. Privacy risks - particularly personal privacy rights - are at risk when someone uses what is considered personally identifiable information for a purpose other than it is intended or understood.

"As people possess more tagged items and networked RFID readers become ever more prevalent, organizations may have the ability to combine and correlate data across applications to infer personal identity and location, and build personal profiles in ways that increase the privacy risk," wrote the report's authors.

Finally, externality risk occurs when RFID technology presents a threat to non-RFID networked or co-located systems, assets and people. The report gives the example of an adversary gaining unauthorized access to computers on an enterprise network through IP-enabled RFID readers if the readers are not designed and configured properly.

To protect against these risks, NIST suggests that companies take the

time to do some risk assessment, and then choose a mix of management, operational and technical security controls. There are many factors that need to be taken into account, including regulatory requirements, the magnitude of each threat and the cost of technology.

While the paper gives some specific guidelines and best practices, the overall message is that companies planning, implementing or managing an RFID system "should always consult the organization's privacy officer, legal council and CIO."

Copyright 2007 by Ziff Davis Media, Distributed by United Press International

Citation: NIST Advises on RFID Security Risks (2007, May 1) retrieved 12 September 2024 from https://phys.org/news/2007-05-nist-rfid.html