Tag hackers raise major security questions

Wednesday, August 23 2006

Massive data sharing presents the biggest threat

By Anne Zieger, Contributor, RFID Operations

This article originally appeared in a 2005 issue of RFID Operations.

Over the last few months, some high-profile hacks have brought attention to the security problems individual RFID tags face.
In one recent case, a hacker changed data found in retail smart labels, using only a PDA-based reader and home-brewed software. In another, researchers compromised tags used for millions of car immobilizers and Smart Tag toll systems.

With the publicity those hacks have gotten, managers rolling out RFID may be wondering if tag security will become their next major headache. As it turns out, though, those concerns are probably misplaced.

While tag vulnerabilities are definitely worth keeping in mind, there are far more important security challenges for RFID operations managers to consider over the next year or two, experts say.

In building a rich database full of RFID-enhanced data—and sharing that data with partners—enterprises are taking on far more risk than any breach of an individual tag could create, says Dave Harty, chief technology officer of Marlton, N.J.-based Acsis Inc., a consulting firm specializing in enterprise data collection.

"If we're going to gather all of this data, in a world where people are talking about sharing it all, that's where you have to worry," Harty says. "It's a flood of data that paints a picture that currently doesn't exist."

New worries?

On the surface, the security flaws exposed by these recent exploits might seem to be enough to give RFID executives new worries.

In one case, using software he designed for the purpose, German consultant Lukas Grunwald removed read-only data from passive-tag smart labels and inserted data from other retail products. The exploit took place at a "Future Store" demonstration site run by the Metro retail chain. (Grunwald's software is available for download at no cost at www.rf-dump.org/).

In another incident, consultants from RSA Security teamed with researchers from Johns Hopkins University to crack the security on widely-used chips found both in car immobilizer systems and "Smart Tag" systems used to pay highway tolls. The student-consultant team broke into a proprietary 40-bit encryption system found on the Texas Instruments digital signature transponder. Once inside the DST, they retrieved password information, then used the stolen password to buy gasoline with an illicit SpeedPass at an ExxonMobil station. (Details available at www.rfidanalysis.org.)

While the two security breaches are quite different technically—the German hacker changed a few bits, while the research team had to guess an encrypted password—both draw attention to the fact that there's only so much you can do to protect individual tags.

"As long as the tags are going to be really inexpensive and sold in high volume, it's

Free Newsletter
Enter your email address:
Submit

Related
A long-established campus card provider brings a "NuVision" to card program security
INTERVIEW: Talking contactless and EMV with Visa's Patrick Gautier
Michielsen Watch: Defcon Hackers
Pennsylvania university finds security solution to protect its campus network

Featured Events
Securing our First Response: FIPS-201 Products aid in disaster recovery
2006 Smart Card Alliance Annual Conference
ISC East 2006
CARTES 2006

E-Mail This Article
Email this article to:
Your email address:
Send

Subscribe to the Contactless News Library
Gain access to the largest collection of Auto-ID analysis on the Internet.

Ads by Avisian

Place your ad here for just $200

Text ads on ContactlessNews bring 70,000 impressions each month.

Click to learn more

Mobile ID Solutions

Barcode and magstripe, age