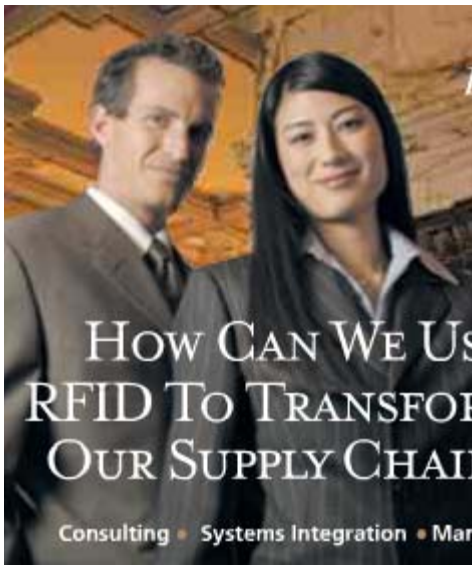
See the new Boxster up close.
Watch the "Overdrive" film ▸
PORSCHE

ADVERTISEMENT


end ad

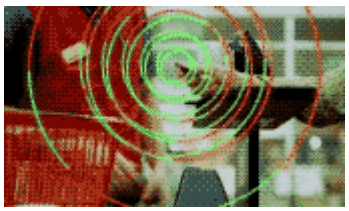
Retail

DODGE GRAB LIFE BY THE HORNS

A Hacker's Guide To RFID

Arik Hesseldahl, 07.29.04, 2:49 PM ET

Of all the things that radio frequency identification technology was supposed to do for retailers--simplifying inventory management and supply chain issues, for instance--creating a new type of theft wasn't one of them. But that is exactly what could happen, and a German information security consultant can prove it. Consider the following scenario.



A would-be scofflaw heads into a grocery store where all the products have RFID tags on them. Rather than paying $7 for a bottle of shampoo, he'd rather pay $3. To make that happen, he whips out a PDA equipped with an RFID reader and scans the tag on the shampoo. He replaces that information with data from the tag on a $3 carton of milk and uploads it to the shampoo bottle tag. When he reaches the check-out stand--which just happens to be automated--he gets charged $3 instead of $7, with the store's computer systems none the wiser.

Lukas Grunwald, the German consultant, says this is not only possible, he's done it. That is, he's changed the information on the RFID tag. He didn't actually steal anything. To prove his point and let others learn about RFID tag security, he's created a free software program called RFDump that is the result of a few years of research into RFID. He presented his findings and announced the release of

RFID: The Revolution Awaits
Pentagon: Rough RFID Ride Ahead?
Will Store Tags Tag You?
Buy With A Wave Of A Phone
Master Of The RFID Universe
Tiny Chips Could Combat Counterfeit Pills
Shopping For An RFID Play
Symbol of Hope
Wall-to-Wall Wal-Mart

Free Trial Issue of *Forbes* Gi

E-Mail Alerts
Get stories by e-mail on this topic.
Companies
Kraft Foods Target
Gillette Procte
Topics
RFID Radio Identif
Inventory Theft
Enter E-Mail Address: FAQ |
Sign Me U

the software at the Black Hat Security Briefings conference in Las Vegas today.

"There is a huge danger to customers using this technology, if they don't think about security," Grunwald says.

This kind of disclosure--complete with a software release that could potentially be misused--is not unusual for Black Hat, a gathering where IT security pros talk frankly about the latest in computer security problems and how to solve them. But don't put your Luddite hat back on just yet.

Companies like **Wal-Mart Stores** (nyse: WMT - news - people) and **Target** (nyse: TGT - news - people) are slowly embracing RFID as the next great boost to their supply chains. But they, like most companies, aren't yet tagging individual items, which is what Grunwald hacked at a store belonging to the Metro retail chain. Instead, they are putting RFID tags only on large cases and shipping pallets until the cost of item-level tagging comes down. A Wal-Mart spokesman says there is no price information on its pallet tags.

Albrecht Truchsess, a spokesman for Metro, says the company is now creating item-level tags for three products: cream cheese from **Kraft Foods** (nyse: KFT - news - people), Pantene Shampoo from **Procter & Gamble** (nyse: PG - news - people) and razor blades from **Gillette** (nyse: G - news - people). He also says that since the tags are being tested only at Metro's Future Store, a demonstration project bringing together several new retail technologies, their security isn't strong by design.

"What we're doing in the Future Store is using the RFID tags for smart-shelf applications," says Truchsess, referring to shelves that track what has been placed on them. "And the sort of tags we're using are very basic. It's really just a test right now."

Metro expects it will take ten years or more before all store items have their own RFID tags on a regular basis. "The ones we're using now cost about 30 or 40 cents each," says Truchsess. "More secure tags are too expensive right now."

Pete Abell, an RFID consultant at Boston-based EPCGroup, says that as stores adopt the technology beyond the test phase, any shopper who brought his own RFID reader into a store would likely be detected. Secondly, he says, tags on products would be programmed to respond only to authorized readers. Finally, he says, the industry is working on stronger encryption than what is available now. "Currently there's only 8-bit encryption available, and that is pretty easy to get around," he says. "And in this case I doubt even that was in place."

E-mail | Print | Comments | License Reprints | E-Mail Newsletters | RSS XML

News Headlines | More From Forbes.com | Special Reports

Subscriptions >

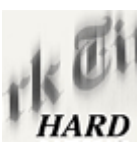
Free Trial Issue of Forbes **Forbes Gift Subscription**
Subscribe To Newsletters **Subscriber Customer Service**

E-MAIL NEWSLETTERS DE

LendingDirect.com
Should I Refinance?
Lendin

Interactive Directory

CEO Book Club
NEW & NOTABLE
Boardroom Bad Boys



BOOK REVIEW
Hard News
Bruce Janicke
Seth Mnookin shows how

hubris--toppled a powerful editor, *The N*
Howell Raines.

Search Books
Title
Go
Advanc
New &

Beginner Stock Trading
Go

SITEMAP HELP CONTACT FORBES.COM INVESTOR NEWSLETTERS FORBES CONFERENCES FORBES MAGAZINES

Ad Information Forbes.com Wireless Reprints/Permissions Subscriber Services

© 2005 Forbes.com Inc.™ All Rights Reserved Privacy Statement Terms, Conditions and Notices

Delivered By mirror image
Tested By SPIRENT
Market Data By REUTERS

Stock quotes are delayed at least 15 minutes for Nasdaq, at least 20 minutes for NYSE/AMEX. U.S. indexes are delayed at least 15 minutes with the exception of Nasdaq, Dow Jones Industrial Average and S&P 500 which are 2 minutes delayed. Disclaimer Forbes 40 Index powered by Telemet. News may include latest headlines from Reuters. Exchange trademark and copyright notices.

Powered By AT&T Intelligent Content Distribution System