Project Tackles RFID Security

A Canadian university researcher is working on ways to provide security for RFID technology. His approach would let users know when a reader is accessing information on an RFID tag or enable them to control access to the data.

With RFID tags being embedded into security-sensitive items such as passports, credit cards, employee identification, and mass-transit passes, protecting the information they contain is a concern.

Many users are unaware that the embedded information can include, for example, their name, birth date, fingerprints, or a digital photo and is protected by little or no security, said University of Calgary doctoral student Nicolai Marquardt. He conducted the research with his faculty adviser, professor Saul Greenberg, and Microsoft Research in the UK.

They devised four secure RFID-tag designs.

The first notifies a user when an RFID reader is accessing the information on a tag. The tag would light up, emit a sound, or vibrate when it nears a reader's electromagnetic field.

In the future, the researchers plan to study ways users could defend themselves once these methods let them know someone is trying to access information on their tag.

Another design lets a user open or close the connection between a tag's RFID chip and antenna, which transmits signals, by depressing a button or sliding a switch on the tag itself.

A variant of this approach activates the tag only when the user touches it. In this case, a simple circuit measures the resistance between metal contacts around the tag and activates when it detects the resistance created by a hand touching it. Otherwise, the tag stays inactive and no one can access its data.

A third approach requires the presence of light or contact with a reader to activate the tag.

In the former technique, a photo transistor activates when the light surrounding it—measured by a circuit—meets a specific level. This would prevent hackers from accessing embedded data when the card is in a user's pocket or bag.

In the latter case, the tag doesn't have its own energy source and functions only when close enough to draw energy from the RFID reader.

Another secure-RFID design uses a variation of the technology in which proximity to the reader activates the tag. One approach works with two RFID chips. One chip would contain general information and enable over-the-air access by a reader, while the other would contain sensitive data and allow access only when the tag touches the reader. A variation uses a slider on the tag to vary and control the over-the-air distance at which data can be read.

Ari Juels, chief scientist and director of RSA Laboratories—a security research center—said that he's unfamiliar with Marquardt's technology but that controlling access to RFID tags is important in items with sensitive information, such as e-passports and credit cards.

All of Marquardt's prototypes were about 2.5 × 4 inches. This is large for RFID tags, which are generally very small for easy embedding. The prototypes were big to enable rapid development and easy viewing of their functionality. However, Marquardt added, they could be made considerably smaller.

Some of the prototypes require batteries to operate, which wouldn't be practical for commercial uses, according to Juels. However, production versions wouldn't necessarily need batteries, Marquardt said,

The experimental approaches wouldn't add much size to today's RFID tags but would be slightly more expensive, although probably not enough to discourage use given the security benefits, said Marquardt, who is continuing his research.

The work, which began at Microsoft when Marquardt was an intern there, was designed to explore RFID technology in general, said Alex Taylor, researcher in the company's Socio-Digital Systems Group.

News Briefs written by ***Linda Dailey Paulson****, a freelance technology writer based in Portland, Oregon. Contact her at ldpaulson@yahoo.com.*

Editor: Lee Garber, ***Computer*****;**
l.garber@computer.org