Researchers to Boost 'Smart Tag' Security

September 26 2006

Johns Hopkins researchers will take part in a new multi-institution project to improve the security of "smart tags," the wireless devices that allow drivers to zip through automatic tollbooths and let workers enter a secured area with the flash of a card.

Some of the same characteristics that make these tags easy to use, researchers say, also make them vulnerable to high-tech thieves who wish to snatch important information from the tags, often without the user's knowledge. The issue is becoming increasingly important because smart tags are being used in more critical applications, such as paying for goods and services and accessing medical records.

To address these concerns, the National Science Foundation recently awarded a four-year $1.1 million grant to university and industry researchers who will study smart tag vulnerabilities and propose ways to make them more secure. The research effort will be led by Kevin Fu, a computer science professor at the University of Massachusetts Amherst; Wayne Burleson, an electrical engineering professor at the University of Massachusetts Amherst; and Adam Stubblefield, an assistant research professor in the Department of Computer Science at Johns Hopkins and a participant in its Information Security Institute. Ari Juels of RSA Laboratories in Bedford, Mass., will also take part in the project.

At Johns Hopkins, Stubblefield and two graduate students will use $350,000 of the grant money to study the protocol and architecture of smart tag systems, meaning the way that tags and reader devices "talk" to one another and allow a transaction or operation to proceed. "We want to

make it tougher for unauthorized readers to communicate with smart tags, and we want to do a better job of preserving people's privacy," Stubblefield said.

Smart tags — which include Radio-Frequency Identification (RFID) tags — are already used to track items from library books to merchandise to cattle. Increasingly, they are replacing the magnetic stripe cards used in security badges. The technology is also used in some mass transit cards and electronic cash systems, and is being incorporated into sensitive documents such as passports. Also, some hospitals are also using the technology to access patient medical records.

Most RFID tags contain a memory chip but no power source of their own. The coded data on the chip is read when the tag passes through the electromagnetic field of a reader antenna. This wireless technology eliminates the need to swipe a magnetic stripe card through a slot. But some scientists are concerned that with the right equipment, a thief could read and steal information from a smart tag that's inside a back pocket or a purse. This theft of personal data could take place while the unaware tag owner is engaged in a public activity such as standing in a cashier's line or sitting on a park bench.

The NSF grant will allow the researchers from UMass Amherst, Johns Hopkins and RSA Laboratories to collaborate on ways to preserve privacy and prevent fraud in RFID- based systems. The new consortium has been dubbed the RFID ConsortiUm for Security and Privacy or RFID-CUSP.

As part of the project, the researchers are working with the San Francisco Bay Area Rapid Transit District. The goal is to produce the first completely open, publicly available software for experimenting with RFID security and privacy.

Source: Johns Hopkins University