Reprint from The New York Times

Study Says Chips in ID Tags Are Vulnerable to Viruses

By JOHN MARKOFF
Published: March 15, 2006

A group of European computer researchers have demonstrated that it is possible to insert a software virus into radio frequency identification ta
a microchip-based tracking technology in growing use in commercial and security applications.

Skip to next paragraph

Don Bernstein/The Raytheon Company

Radio frequency identity tags are growing in popularity because they are easily scanned.

In a paper to be presented today at an academic computing conference in Pisa, Italy, the researchers plan to demonstrate how it is possible to i
tiny portion of memory in the chip, which can hold as little as 128 characters of information.

Until now, most computer security experts have discounted the possibility of using such tags, known as RFID chips, to spread a computer viru
of the tiny amount of memory on the chips.

The tracking systems are intended to improve the accuracy and lower the cost of tracking goods in supply chains, warehouses and stores. Radi store far more data about a product than bar codes and can be read more quickly. They have even been injected into pets and livestock for iden

The chips have already prompted debate over privacy and surveillance, given their tracking ability. Now the researchers have added a series of worrisome prospects, including the ability of terrorists and smugglers to evade airport luggage scanning systems that will use RFID tags in the

In the researchers' paper, "Is Your Cat Infected With a Computer Virus?," the group, affiliated with the computer science department at Vrije Universiteit in Amsterdam, also describes how the vulnerability could be used to undermine a variety of tracking systems.

The researchers said they realized that there are risks associated with publishing security vulnerabilities in computerized systems. To head off the possible attacks they described, they have also published a set of steps to help protect RFID chips from such attacks.

The group, led by Andrew S. Tanenbaum, an American computer scientist, will make the presentation at the annual Pervasive Computing and Communications Conference sponsored by the Institute of Electrical and Electronic Engineers. Mr. Tanenbaum is the author of the Minix oper system, an experimental project that became the heart of the Linux open-source operating system.

The researchers asserted that the RFID demonstration had not used the commercial software that collects and organizes information from RFID Rather, it used software that they designed to replicate those systems.

"We have not found specific flaws" in the commercial RFID software, Mr. Tanenbaum said, but "experience shows that software written by la companies has errors in it."

The researchers have posted their paper and related materials on security issues related to RFID systems at www.rfidvirus.org.

The researchers acknowledged that inside information would be required in many cases to plant a hostile program. But they asserted that the c software developed for RFID applications had the same potential vulnerabilities that have been exploited by viruses and other malicious softw malware, in the rest of the computer industry.

One such standard industry problem is a software coding error referred to as a buffer overflow. Such errors occur when programmers set aside to receive data temporarily, but fail to require a check on the size of the value that is moved to the allocated space. A larger-than-expected valu cause the program to break and trick the computer operating system into executing a malicious program. "You should check all of your input a time, but experience shows this isn't the case," Mr. Tanenbaum said.

Independent computer security specialists also said RFID systems were potential problem areas.

"It shouldn't surprise you that a system that is designed to be manufactured as cheaply as possible is designed with no security constraints wha said Peter Neumann, a computer scientist at SRI International, a research firm in Menlo Park, Calif.

Mr. Neumann is the co-author of an article to be published in the May issue of the Communications of the Association for Computing Machin risks of RFID systems. He said existing RFID systems were a computer security disaster waiting to happen.

He cited inadequate identification for users, the potential for counterfeiting or disabling tags, and the problem of weak encryption in a passport system being developed in the United States. But he said he had not previously considered the possibility of viruses and other malicious softwa programs.

An industry executive acknowledged that the companies that make computerized tracking systems faced potential security problems.

"We are very actively looking at the different way the technology is used," said the executive, Daniel P. Mullen, president of the Association f Automatic Identification and Mobility, an industry trade group. "It's an ongoing dialogue about protecting information on the tag and in the da

The association has a working group of experts assessing both security and privacy challenges, he said.

There are many types of RFID tag, and some of the sophisticated versions include security features like encryption of the identifying number c the chip.

But the Dutch research group warned that in a variety of situations it is possible for attackers to alter the information in an RFID tag to subvert purpose.

"RFID malware is a Pandora's box that has been gathering dust in the corners of our 'smart' warehouses and homes," they write in their paper.

In one example they offered, a virus from an infected tag on luggage passing through an airport could be picked up when it is scanned by the lı handling control systems and then spread to tags attached to other pieces of luggage.

Such an attack, they suggest, might spread luggage contamination to other airports. It might also be used by a smuggler to cause a piece of lug avoid security systems.

They also described situations of counterfeit RFID tags possibly being be used to subvert pricing and other aspects of commercial sales systen virus could be inserted into RFID tags used to identify pets.

1.