

Study says RFID tags are vulnerable to viruses

Last modified:

March 14, 2006, 11:05 PM PST

By John Markoff

[The New York Times](#)

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

In a paper to be presented Wednesday at an academic computing conference in Pisa, Italy, the researchers plan to demonstrate how it is possible to infect a 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 virus because of the tiny amount of memory on the chips.

advertisement



The tracking systems are intended to improve the accuracy and lower the cost of [tracking goods in supply chains](#), warehouses and stores. Radio tags 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 identification.

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 future.

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 some of 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. Tanenbaum is the author of the Minix operating 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 readers. Rather, it used software that they designed to replicate those systems.

Software errors

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

The researchers have posted their paper and related materials on security issues related to RFID systems at [Rfidvirus.org](#).

The researchers acknowledged that inside information would be required in many cases to plant a hostile program. But they asserted that the commercial software developed for RFID applications had the same potential vulnerabilities that have been exploited by viruses and other malicious software, or 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 memory 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 value can cause the program to break and trick the computer operating system into executing a malicious program. "You should check all of your input all of the time, but experience shows this isn't the case," 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 whatsoever," said Peter Neumann, a computer scientist at SRI International, a research firm in Menlo Park, Calif.

Neumann is the co-author of an article to be published in the May issue of the Communications of the Association for Computing Machinery on the 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-tracking system being developed in the United States. But he said he had not previously considered the possibility of viruses and other malicious software 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 for Automatic Identification and Mobility, an industry trade group. "It's an ongoing dialogue about protecting information on the tag and in the database."

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 carried by 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 its 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 luggage-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 luggage to avoid security systems.

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

Entire contents, Copyright © 2006 The New York Times. All rights reserved.

[1 Home](#) [2 E-mail this](#)

Copyright ©2006 CNET Networks, Inc. All rights reserved.