SEATTLE POST-INTELLIGENCER
http://seattlepi.nwsource.com/business/262986_radiotag15.html

Viruses can taint radio frequency ID tags

Technology could be used to aid terror, research says

Wednesday, March 15, 2006

By JOHN MARKOFF
THE NEW YORK TIMES

A group of European computer researchers has 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 today 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 chips that is frequently large enough to hold only 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.

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 already have prompted debate about 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, Netherlands, 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 published a set of steps to help protect RFID chips from such attacks.

The group, led by Andrew 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.

"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 on the Internet 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 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.