InfoWorld

Back to article

Print this

Update: RFID tags are subject to viruses, says study

Researchers have created a proof-of-concept, self-replicating RFID virus

By Jeremy Kirk, IDG News Service

March 15, 2006

Three computer science researchers are warning that viruses embedded in radio tags used to identify and track goods are right around the corner, a danger so far overlooked by the industry's high interest in the technology.

No RFID (radio frequency identification) viruses have been released live of now, according to the researchers at Vrije Universiteit Amsterdam in the Netherlands. But RFID tags have several characteristics that could be engineered to exploit vulnerabilities in middleware and back-end databases, they wrote in a paper presented Wednesday at a conference in Pisa, Italy

"RFID malware is a Pandora's box that has been gathering dust in the corner of our 'smart' warehouses and home," the paper stated.

The attacks can come in the form of a SQL injection or a buffer overflow attack even though the tags themselves may only store a small bit of information, the paper said. For demonstration purposes, the researchers created a proof-of-concept, self-replicating RFID virus.

It only took a master's student at the university, Patrick Simpson, four hours to write a virus small enough to fit on a RFID tag, something previously thought unworkable, said Andrew S. Tanenbaum, a professor at Vrije Universiteit Amsterdam. RFID tags can contain as little as 114 bytes of memory, he said.

Tanenbaum expects vendors to be angry about the publishing of the code. Vendors have dismissed the possibility of RFID viruses, saying that the amount of memory in the tags is too small, he said.

"You publish all of the code on the Web site, and all of [a] sudden, [vendors] are going to start panicking," Tanenbaum said. "This hopefully will make them take it seriously. This is a wake-up shot before this stuff is deployed in a large scale."

But the researchers did take precautions to ensure RFID viruses won't immediately circulate. They wrote their own middleware that mimicked traits of products on the market, said Melanie R. Rieback, one of the paper's authors.

"It's not like we are providing a cookbook for basically wanna-be hackers to hack real RFID systems," Rieback said.

The homespun middleware connected to back-end databases from vendors such as Oracle and Microsoft along with open-source databases such as MySQL and Postgres, Rieback said. The experiment used RFID equipment from Philips Electronics, she said.

"It was actually quite interesting to see that some of the databases were susceptible to some kinds of attacks," Rieback said. "Other ones actually had natural protection mechanisms built in that made them more resistant."

The purpose of the exercise, the authors wrote, is to encourage RFID middleware designers to be more careful when writing code. Back-end middleware can contain millions of lines of source code, and if software faults number between six to 16 per 1,000 lines of code, the programs are likely to have many vulnerabilities, the paper said.

RFID tags are increasingly being used in a variety of industries to track items and give a real-time view of inventories. The tags contain data on a particular object or, in some cases, embedded in animals, and that data is typically stored in a database.

Companies can save money by using the tags to keep closer tabs on their property. However, this "pervasive computing utopia has its dark side," the authors wrote.

RFID systems may be attractive to criminals since the data contained on them may have a financial or personal nature, such as information stored on digital passports. In addition to causing damage to computer systems, RFID malware may have an effect on real-world objects, the paper said.

Airports are looking to RFID tags to better track baggage. But Tanenbaum warned that this application could pose a large problem if an RFID tag is read and delivers a much larger set of data in return.

A false tag on a piece of baggage could exploit a buffer overflow, delivering a virus to the RFID middleware, according to Tanenbaum. Once the virus code is on the server, it can infect the databases and corrupt subsequent tags or install "backdoors" -- small programs that allow for the extrication of data over the Internet, he said.

"You can hide baggage," Tanenbaum said. "You can reroute baggage to the wrong place -- all kinds of mischief. That's I think a very, very serious thing that even has national security implications."