

# Can Tag Viruses Infect RFID Systems?

A group of European computer researchers have issued a study warning that RFID middleware and applications are vulnerable to viruses encoded into a tag's memory.

By Jonathan Collins

Mar. 15, 2006—A group of European computer researchers at Vrije University in Amsterdam, the Netherlands, have published a paper they claim shows how RFID tags, including those compliant with EPCglobal standards, could be used to transmit computer viruses capable of bringing down and compromising entire computer systems.

"Even a tag with just 112 bytes available can create a buffer overflow or an SQL injection attack," says Andrew Tanenbaum, professor of computer science at the university.

RFID software designers have long thought the memory of passive RFID tags too small to pose any likely security threat, the researchers explain, saying their work shows that threats are possible by using tags to exploit long-standing vulnerabilities in the middleware and application software.

However, the group's claims were immediately rejected by some members of the RFID industry, including Kevin Ashton, cofounder and former executive director of MIT's Auto-ID Center and now vice president of marketing for RFID interrogator manufacturer ThingMagic.

"A typical EPC tag has 96 bits of memory with an ID number," Ashton notes. "For any such threat to be credible, there would have to be more memory, a read-write tag and variable-length tag reads. It would also need a reader and a system stupid enough and vulnerable enough to allow executable malicious code."

Sue Hutchinson is the director of product management for EPCglobal US, the U.S. arm of EPCglobal, a GS1-sponsored organization working to commercialize EPC technology and RFID standards. She says the security features built into the latest EPC tag and reader standard, Class 1 Gen 2, make the air interface protocol very different than the tags and readers used in the Dutch study.

Studies such as the one done at Vrije University are important because "they keep us thinking about these things, and it's of critical importance," says Hutchinson, "but it's a grand leap to say that [what was shown in the study] could happen to EPC tags and readers."

"We've been taking a very proactive stance at looking at security in the EPC Gen 2 protocol," she says. To strengthen security, the Gen 2 protocol includes two key safeguards: the ability to lock a tag so that only an authorized interrogator can write any data to it, and the use of RF masking, which adds a random number to a tag's ID and requires the tag and reader to exchange what she likens to a handshake before they can exchange any data. These features "make it much harder to introduce a virus into the system," she says, than using the method in the study.

According to a paper written by the Dutch researchers, the group carried out multiple tests of RFID tags made

with Philips UHF I-Code SL1 chips, which, according to the paper, had 896 bits of memory. During the tests, the tags were programmed with a number of viruses and other types of malware developed at the university. The group used its own RFID middleware and a number of commercially available databases in its trials. The tests showed that tags could be employed to instigate a number of malicious attacks on the databases and middleware used in an RFID network, including buffer overflow and SQL injection, and even open a back door to the RFID application server.

"A lot of these attacks are common knowledge to IT security professionals, but what is different is that no one expects these attacks to come from an RFID tag," says Melanie Rieback, a Vrije University Ph.D. student who presented the group's findings today in a paper at the IEEE conference Pervasive Computing and Communications (IEEE PerCom) in Pisa, Italy. The paper, entitled "Is Your Cat Infected With a Computer Virus?," is available at the group's Web site.

The goal of the group's work, says Rieback, is to ensure that commercial RFID middleware developers, as well as RFID deployers developing their own middleware, address the potential of security attacks emanating from tags. "It is early enough not to cause too much damage," she says. "What would have been worse is if this threat had been discovered only through the work of a malicious hacker in five years' time, when many RFID systems have been deployed."

According to Ashton, the group's development of its own middleware to test the system underestimates the security built into commercially developed RFID middleware. "The RFID industry is an offshoot of the IT industry, and that industry has always taken security very seriously," he says. "Some of the earliest work at the Auto-ID Center addressed security."

"We've built security features into every part of the EPCglobal Network," says Hutchinson, "not just in the air-interface protocol, but also into the application-level events protocol and into the higher-level [elements] used for data discovery and track-and-trace applications."

While such virus attacks may be possible in theory, says Ashton, good software development practices would ensure that these vulnerabilities would be extremely unlikely to be found in any RFID network. "There are any number of hurdles that a piece of malicious code would have to overcome [to do any damage]," he claims, adding that RFID interrogators alone would detect rogue tags or rogue software on tags as part of the verification process of reading them.

Nonetheless, Tanenbaum believes a system using read-write tags are at the greatest risk because a system compromised by a single malicious tag could be used to create many more infected tags. One example is the tag used in RFID-enabled baggage-handling systems already in operation at Las Vegas' McCarran Airport. Once infected, Tanenbaum claims, baggage tags could be used to infect baggage-handling systems worldwide as bags with infected tags move to and are read at other airports.

The potential threat from RFID viruses is compounded further, say the researchers, by the interaction RFID tags enable between physical objects and events and computer systems. "In the past, if these attacks were used on a PC, then it might crash the computer, but RFID merges the real world and the virtual world, and so there is the potential for real and much more severe consequences," Tanenbaum says.

Ashton, however, asserts that the comparison with PC systems underlines a problem in the research group's work. "RFID systems are built using middleware, software and database systems, as well as custom software to act as a glue between these elements," he explains. "Every [RFID system] is unique, not like a PC desktop system. There would have to be stupid holes in the system vulnerable to attack, and the attacker would need intimate knowledge of those holes. If that were ever the case, the attacker wouldn't use RFID as a weapon of choice."

