InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Trade Group Attacks RFID Virus Claims

Researchers claimed to have discovered a way to infect an RFID chip with a virus, but in fact they just built a poorly designed system, said an RFID trade association.

By John Walko, EE Times
March 17, 2006
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=183700674

LONDON — The trade association for automatic identification and mobility, AIM Global, attempted to refute key findings of an IEEE conference paper presented this week that suggested RFID tags could be used to corrupt databases and even spread computer viruses.

The paper, by Melanie Rieback, a third-year PhD student at Amsterdam's Vrije University, was presented at the IEEE conference in Pisa, Italy, on Wednesday (March 15), sent shock waves through the RFID industry.

Titled "Is Your Cat Infected with a Computer Virus?" the paper suggested computer viruses could spread from RFID tags through readers into poorly written middleware applications and backend systems and databases.

"Many of the basic assumptions in the paper overlook a number of fundamental design features necessary in automatic data collection systems and good database design," asserted AIM Global President Dan Mullen.

Mullen suggested that researchers built a system with a weakness and then proceeded to show how the weakness could be exploited. "Not surprisingly, poor system design, whether capturing RFID tag information, bar code information or keyboard-entered data, will create vulnerabilities."

The association said it recognizes the efforts of university researchers is designed to highlight RFID security issues. "But the methodology of

this particular research is questionable," added Mullen.

Responding to the paper, RFID experts and International Organization for Standardization scientists, meeting this week in Kyoto, Japan, to debate RFID standards, emphasized that fixed data RFID tags, such as those used to identify pets, cannot be changed and therefore are immune to infection by a virus.

They skirted the issue of whether other types of tags, such as those where data can be changed, are prone to attacks. The experts did note that specific attributes in RFID systems can protect the overall system.

For instance, they stressed that most RFID applications, including EPC Gen2, look for specific kinds of data. Poor reader design might allow detection of a "rogue" tag, but a secure system will verify data against predefined parameters, as do current bar code systems.

The ability to insert a virus implies that a tag contains executable code that is recognized by software. This, they assured, is impossible with most RFID applications since specific kinds of data are sought and systems will either flag or reject anything that doesn't fit the data template.

Other industry reaction to the paper was mixed, but many agree it presented a wake-up call.

"With respect to the students involved, the paper as presented is rather weak," said Kevin Ashton, ThingMagic Inc. vice president, and co-founder of the Massachusetts Institute of Technology (MIT) Auto-ID Center. "The 'real' virus they claim to demonstrate in the paper is not a virus, just a self-replicating piece of SQL code."

The paper, however, does call attention to an obvious problem the software industry has faced for years, suggested Julie England, vice president at Texas Instruments. "Companies need to provide multilevel security and take responsibility for testing before releasing applications to the market," said England.

Last month, cryptographers reported weaknesses in the underlying RFID chips and hashing algorithms. In a panel discussion during the RSA Conference, Adi Shamir, professor of computer science at the Weizmann Institute, disclosed that he had recently applied power analysis techniques to crack passwords for the most popular brand of RFID tags.

At the same panel, Ron Rivest, who co-developed the RSA algorithms with Shamir, called for an industry effort to create a next-generation hashing algorithm to replace SHA-1, which is used broadly for computer security.