News

Viruses to spread soon via RFID tags?

Gregg Keizer, TechWeb News , 16-Mar-2006

At an IEEE conference in Italy, a PhD student at Amsterdam's Vrije Universiteit presented a paper that outlined the threat to RFID systems.

Radio frequency identification tags (RFID) can be used to spread computer viruses and attack middleware applications and the databases behind them, a group of Netherlands-based scientists said Wednesday.

At IEEE's conference on pervasive computing in Pisa, Italy, Melanie Rieback, a third-year PhD student at Amsterdam's Vrije Universiteit, presented a paper that outlined the threat to RFID systems and laid out how the small amount of memory in a tag -- in some cases as little as 128 bytes -- could be used to corrupt databases.

RFID tags have been promoted as a more efficient and economical way of tracking products -- from manufacturers to end-users -- and have been thought to be immune from such hacks.

Not so, said Rieback, a U.S. citizen who has studied in the Netherlands for the past five years. "This is a real threat, and it's going to be a larger threat if it's not taken care of," she said Wednesday after presenting her paper "Is Your Cat Infected with a Computer Virus?".

Once a hacker has created a miniature virus -- and perhaps planted a malicious tag on a product in store -- the attack begins as soon as the RFID tag is scanned. Attacks on middleware and the back-end databases, she said, could take the form of buffer overflows, code insertions, and SQL injections (a type of specialized code insertion that tricks a database into running SQL code).

To combat such attacks, middleware and database creators -- including big names like Oracle and SAP -- must harden their products to account for viral infections.

"We wanted to get the message out," she added. "Now they have warning."

Viruses could spread from tag to database, then to other tags in settings where RFID chips are written to, leading to scenarios where one incoming malicious tag leads to a factory sending out millions of infected chips to its customers.

"There are real-world consequences here," said Rieback. "Some car plants use tags on chassis to identify what color the car is to be painted. If a virus instructs the database to write tags that tell [the machinery to] switch colors, you're talking about destroying cars."

Andrew Tanenbaum, Rieback's supervising professor at Vrije Universiteit, had even more dire attacks in mind.

"In an airport that's tagging luggage [with RFID chips], drug smugglers would love for their bags to disappear," said Tanenbaum. "It would make it that much harder for any AI used by the airport or customs to spot suspicious bags."

Likewise, terrorists might be able to circumvent RFID-based security measures -- such as those planned to track shipping containers -- or evade bomb-sniffing systems, such as the one set to debut this spring at Las Vegas' McCarran International Airport, where tags will be used to verify that bags have been checked for explosives.

Viruses on tags can cross borders with ease, said Rieback. Although RFID tags use locally-determined frequencies to transmit data, there are widely-used international standards. A product marked in Germany with a malformed tag might be able to infect systems in the U.S., although the virus itself would likely be middleware- or database specific.

"But that's not a problem," said Tanenbaum. "Back-end vendors are usually public knowledge. When a customer signs with an RFID vendor, both usually issue press releases."

Rieback's presentation included a proof-of-concept virus created by a masters-level student of the university, Patrick Simpson, to demonstrate the attack.

"If we didn't [create a proof-of-concept exploit] no one will believe us," Tanenbaum said. "The RFID middleware makers, they'll all deny that there's a problem." he continued.

"The surprising thing about this all is how easy it was to write a virus," he said. "It took Patrick just four hours."

"This is a wake-up call," concluded Tanenbaum.

Related Articles

- Microsoft Office bug may lead to drive-by downloads
- McAfee update breaks hundreds of apps
- Microsoft plans two patches this week
- Phishers dodge shutdown
- New IM worms delete and hijack

About CMPnetAsia | Contacts | Subscription

TechWeb Network Sites: Byte.com | CMPmetrics | ITpro Downloads | Financial Technology | InformationWeek | Insurance & Technology | Network Computing | TechCalendar | TechEncyclopedia | TechLearning | TechWeb Today | Wall Street & Technology

Affiliate Network Sites: ChannelWeb | Communications Convergence | Computer Reseller News | Dr. Dobbs | DV.com | Gamasutra | Intelligent Enterprise | IT Architect | Software Development | Sys Admin Magazine | UnixReview.com | VarBusiness | Indian Express | Express Computer | Network Magazine India