RED HERRING THE BUSINESS OF TECHNOLOGY

RFID Virus Threat Downplayed

Radio frequency ID industry dismisses Dutch scientists' study of virus vulnerability in tags.

March 15, 2006

A group of scientists said Wednesday that RFID systems are vulnerable to viruses because the tags, which are usually attached to goods or shipment crates, can be compromised despite the limited storage space available to would-be hackers.

But the response from the RFID industry was immediate.

Kevin Ashton, vice president of marketing for ThingMagic, a Cambridge, Massachusetts-based designer of reading devices for RFID systems, said the paper was highly theoretical and the theoretical RFID viruses could be damaging only to an "incredibly badly designed system."

'You can't infect the phone system by typing in the wrong phone number.'
-Kevin Ashton, ThingMagic

According to the study, done by scientists attached to the Faculty of Sciences in Amsterdam, hackers can infect the tag, which has at most about 1,024 bits of storage. Then the virus can be passed to the back-end database when the infected tag is scanned by the RFID reader.

In the paper, the scientists said they are making the RFID vulnerabilities public so the industry can correct them before the hackers figure out how to compromise the systems.

"It is a lot better to lock the barn door while the prize racehorse is still inside than to deal with the consequences of not doing so afterwards," said the report.

RFID is still in its early stages of evolution. The technology, which has found a reliable testing ground in the supply chain arena, has also found a home in automated toll collection systems and implantable tracking devices for pets.

Big Plans for RFID

RFID has been touted as significant in areas such as passport management, and even in tracking humans, such as prisoners or detainees. But some observers have raised caution flags about the possible tracking of "consumers" in their homes.

Whether or not Big Brother applications are on the agenda, the technology does carry an aura of conspiracy. But Mr. Ashton believes the RFID malware paper is "a bit of a stretch."

"It's like saying we just proved that cars are insecure because, without steering wheels, they will run off the road," he said. "You can't infect the phone system by typing in the wrong phone number. Similarly you can't infect an RFID system by compromising the tag."

The paper gives a number of scenarios where a hacker could possibly compromise an RFID system. One involves a hacker replacing a legitimate store RFID label on a product, like a can of shaving cream, with one he makes himself from commercially available RFID writing systems.

Unimaginable Compromises

He returns the shaving cream to the store and the worker at the return counter scans it into the system. Then the infected tag compromises the system in heretofore unimaginable ways.

But Mr. Ashton thinks the possibility of this happening is much more plausible in academia than in the real world.

"The tag carries a number that refers to information in the system," he said. "There is not much that you could do with it unless you've happened upon a truly badly designed system."

Most RFID systems are custom-designed, he noted, so a hacker does not have the benefit of predictability that he or she has with a system such as Windows, which is installed on millions of computers.

"With an RFID system, the hacker would have to know a lot about a particular system and he will be able to attack just that one system," said Mr. Ashton. "The idea of RFID tags spreading viruses seems quite far-fetched to us."