The Real RFID Security Issue

March 22, 2006

By Eric Lundquist

BOSTON—Are RFID systems secure? This is a good question and one that should be asked before your company jumps on the RFID bandwagon.

The question recently acquired an added urgency when a Dutch researcher presented a paper outlining a possible security hole. The answer may lie in cats, cell phones and making sure that you treat all the data in your network as worthy of security scrutiny regardless of the source.

In the research paper, a group of researchers from the Computer Systems Group at Vrije University in Amsterdam raised the issue of an RFID tag being used as a carrier for SQL injection attack on the underlying software identification and tracking system. The paper is available as a pdf here and its presentation set off a storm of attacks, not from virus writers but from RFID vendors and consultants downplaying the likelihood of such an attack.

RELATED LINKS

- Dutch Researchers Create RFID Malware
- Wal-Mart Forges Ahead with RFID
- RFID's High Cost Deters Businesses
- Microsoft Reveals Details of Its RFID Infrastructure
- The RFID Hype Effect

"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," stated AIM Global president, Dan Mullen.

Dutch researchers create RFID malware. Click here to read more.

"In other words, the 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."

AIM is a trade organization representing automatic identification vendors, among others. In the controversial Dutch research paper titled, "Is Your Cat Infected with a Computer Virus?" the researchers note that, "RFID systems as a whole are often treated with suspicion, but the input data received from individual RFID tags is implicitly trusted."

The researchers contend that the implicit trust is unfounded and, "The security breaches that RFID deployers dread most—RFID malware, RFID worms and RFID viruses—are right around the corner."

Viruses entering an RFID system would indeed be a massive problem. Tracking down and eradicating viruses in e-mail systems is an ongoing and costly battle for IT administrators the world over.

But e-mail systems dealing with thousands (and even at big companies, tens of thousands) of messages a day are still small systems compared to the millions of inputs that an RFID system tracking every product in a company's inventory would generate as those products move along the supply chain.

While the researchers are essentially saying that if you take a good RFID chip, replace it with a virus's coded chip, let the scanning take place as usual and soon you have that piece of bad code doing its dastardly deeds in your RFID system.

The cat in the paper's title refers to a hypothetical veterinarian pet identification system that gets infected and ultimately freezes and displays, "the ominous message: All your pet are belong to us." The bad English is a take off on a phrase that appeared in the Japanese game Zero Wing and refers to a self-propagating phrase for the whole story.

The research findings have been attacked by RFID defenders as faulty. RFID chips, while simple devices, can be locked down, encrypted and don't present any more vulnerabilities than any other system such as bar codes, goes the argument.

According to RFID defenders, if you incorporate bit checking, parameter checking and all the other safeguards associated with good system design in this era of security concerns, your cat will be safe.

I think the researchers were right to raise the issue and the RFID defenders were right to raise their rebuttals.

Next Page: Assume nothing about RFID security.

So what should you do as someone considering developing or deploying RFID systems at your company?

"Companies who use tags must not assume that the data they read from the tags was not put there by somebody else. Just like when writing Web applications, you have to assume any input from the outside world may contain malicious or corrupted data," stated Yossi Oren, a researcher at the Weizmann Institute of Science in Israel in an e-mail exchange.

I contacted Oren because he was the researcher who, along with Adi Shamir (a professor at the institute and one of the world's top security authorities), sent a shock wave through the RFID community when speaking at the RSA Security conference. Shamir outlined the possibility of hacking RFID chips with a cell phone.

While RFID chips don't have a built-in power supply, they do signal their identity to a reader using the reader's power. Through the use of a directional antenna and measuring power consumption, Shamir contended a hacker could discover a password based on the RFID system's reaction to a "bad bit." Once discovered, the password can be used to shut down the chip.

"What are the implications for the future?," Shamir asked the attendees at RSA. "I think the first generation [RFID chips] are very, very vulnerable to a very cheap kind of attack. While we haven't implemented it, we believe the cellular telephone has all the ingredients needed to carry out such an attack.

Click here to read about how RFID's high cost is detering businesses.

"It [the cell phone] has a software radio and if you can tweak it enough you can just walk around and kill all the RFID tags in the vicinity," said Shamir.

I asked Oren if, since that presentation, their concerns about RFID vulnerability via power consumption

metering had been confirmed for newer chips (Gen 2) as well as the older ones.

"We are currently working on applying our results to newer [Gen 2] tags. We have some in the lab right now. When we have convincing results, they will be posed on the Web site.

The lesson for IT executives is don't assume your RFID system is secure simply because you are using hardware chips in the process. You need to apply the same security best practices to your RFID system that you would to any critical corporate information system.

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at eWEEK.com Security Center Editor Larry Seltzer's Weblog.