

EPC Tags Subject to Phone Attacks

At last week's RSA security conference, renowned cryptographer Adi Shamir said EPC RFID tags are very vulnerable to attack—one that could be deployed using a cellular phone.

By Mary Catherine O'Connor

Feb. 24, 2006—Each year, data security specialists attend RSA Security's annual conference to learn about the most recently discovered breaches in data security and encryption. When attendees gathered for the Cryptographers Panel during the RSA Conference 2006 last week in San Jose, Calif., they learned that one of these threats loom around RFID.

Adi Shamir, professor of computer science at the Weizmann Institute of Science, announced that he and a fellow Weizmann researcher, Yossi Oren, were able to kill an EPC Class 1 Gen 1 passive tag after hacking it to determine its kill password. (For the detailed results of the tests, go to <http://www.wisdom.weizmann.ac.il/~yossio/rfid/>.) While his experiment demonstrated only the ability to use a password to kill a tag, Shamir noted that in the future, passwords will likely be used to protect sensitive information encoded to EPC tags, and this same attack could be used to determine those passwords. In fact, according to Oren, the same method could be used to find the larger kill passwords required to kill Gen 2 tags and *could* potentially be used to crack the protections around data on other types of tags, such as the account information and other personal data on RFID tags embedded in some credit cards.

To determine the kill password, Shamir and Oren used what is referred to as a side-channel attack. Rather than confronting the data protection straight on, such as attempting a long list of passwords to deduce the correct one, Oren explains, a side-channel attack analyzes the behavior of the protected devices to "slowly insinuate" the correct password or key needed to access the protected data. Side-channel attacks are executed by watching the power consumption or variations in the timing of the energy output of the devices (in this case, an EPC Gen 1 Class 1 tag) as they attempt to process collections of bits of data. In a power-analysis attack, the amount of energy the device consumes spikes when it receives inaccurate bits, and falls when the bits are correct. Because they constantly learn which bits work and which don't, hackers using side-channel attacks are guided more quickly to the correct data than hackers just trying to break the data protections without analyzing how the power consumption fluctuates with each bit of information.

Shamir and Oren pointed a directional antenna, attached to an oscilloscope, toward the tag—the manufacturer of which they would only describe as "one of the biggest"—as the tag was receiving bits of data sent to perform a kill command. As they sent each bit of data, they used the antenna to "see how thirsty the tag was," says Oren. Completing the attack on the Gen 1 tag in the lab took the pair three hours, but most of that time was reportedly spent transferring the data from the oscilloscope to a PC. Oren predicts that since a cell phone would not need to perform this step, it could complete the attack in about a minute. An EPC Gen 1 tag requires only an 8-bit password, whereas the EPC Gen 2 protocol uses a 32-bit password, so figuring out a Gen 2 tag's password would take more time.

Perhaps most troubling was Shamir's prediction that a power analysis attack on an RFID tag could be performed using a very common device. "While we have not implemented it, we believe that the cellular

telephone has all the ingredients needed to carry out such an attack [to decipher a tag's password]," he said at the conference. Oren explains that this would require the creation of firmware written to alter the phone's RF capability so that rather than communicating voice or data over a given phone network, it would instead search for EPC tags. The firmware running on the phone's operating system would then execute the attack. Phones using Global System for Mobile Communications (GSM) technology commonly transmit at 900 or 1,800 MHz. Phones employing Code Division Multiple Access (CDMA) technology, used mainly in the United States and Canada, transmit at 850 or 1,900 MHz. Because both types of phones operate within the UHF band, says Oren, they could be used to communicate with UHF EPC tags.

"How easy or hard it would be to write this firmware, I can not say," Oren allows. "What the firmware would do depends on what the tag maker is trying to hide [what data it is protecting]." The firmware could be written to use power analysis to determine a password, a technique Shamir and Oren proved possible. Oren says he does not know how close a phone would need to be to the tag, but a supplemental antenna could boost the phone's range.

Ari Juels, principal research scientist at RSA Laboratories, says this type of power analysis could also be used to crack key cryptography, used to protect account data encoded to the tag embedded in some credit cards. Juels does not know the amount of time or distance from the tag an attack on an HF tag would require. He says, however, that if firmware were written to perform power analysis in order to determine the cryptographic key, thieves could use that key to make clones of the cards. This wouldn't necessarily require the thief to make an exact clone of the tag or card, he says, adding, "You could rejigger your mobile phone to simulate the credit card, and then go into a store to use your phone to make a payment." A growing number of merchants are enabling their POS systems to accept RFID payments. And while cellular phones operate in the UHF band, those enabled for the near field communication protocol contain an RFID module that operates in the HF range (13.56 MHz), which is what the RFID credit card payment systems use.

Still, Juels and Oren point out that power analysis is not a new type of data attack, and that the same type of protections contact-based smart cards use to protect those cards from hacking through power analysis could also be used to protect RFID tags. These protections mask the spikes in power consumption—but in so doing, they force the hardware to consume more energy overall. Tag makers, on the other hand, are always looking for ways to reduce the amount of energy passive tags must consume to make them more efficient.

"There are fairly well-studied mechanisms to find ways to withstand these attacks," says Juels. "I don't think [Shamir's] results show an immediate threat to payment devices, but they do show that attacks that have been done on other technologies could also succeed on RFID devices." He adds, "This is something that exploits some of the naivety that has gone into security designs for EPC tags. For [EPCglobal](#), the cost to counteract these threats shouldn't be too high, and might not require changing the [air-interface] standard."

By next week, Oren says he hopes to publish details on the power analysis attack they performed. He says he sent all of this documentation to EPCglobal already, and assumes the technologists there are reviewing it. EPCglobal US says it is studying Shamir's findings.

"Security is very important to us, and we are taking a proactive role in addressing security at all levels of the EPCglobal Network," explains Sue Hutchinson, director of industry adoption for EPCglobal US. "In fact, security has been a focus for both the hardware and software action groups and is currently the focus of our Architecture Review Committee, which is looking at security, not only on the tag but for all levels of information flow in the EPCglobal Network."