

A Reality Double-Check

What mobile phones are telling us about RFID security.

March 6, 2006—At last month's RSA Conference, Adi Shamir (the 'S' in RSA) discussed an attack he devised with graduate student Yossi Oren against an important type of RFID tag known as an Electronic Product Code (EPC) tag (see [EPC Tags Subject to Phone Attacks](#)). An EPC tag is essentially a wireless bar code designed to supplant the black-and-white printed bar codes in widespread use today. Because EPC tags may someday find their way onto individual consumer items, leading to a range of privacy concerns, the tags include what's known as a kill function. When a reader transmits a kill command to an EPC tag, the tag self-destructs. (Dead tags don't betray privacy.) To protect against malicious destruction of tags, the kill function works only when accompanied by a tag-specific personal identification number, or PIN.

What Oren and Shamir have shown is that certain EPC tags (Class 1 Generation 1) are vulnerable to remote *power analysis*. These tags produce power spikes that are measurable over the air and can be exploited to reveal the PINs used to kill tags. They speculate that mobile phones, many of which operate in the portion of the radio spectrum referred to as ultrahigh frequency, could be modified to execute this attack against a very important emerging generation of EPC tags known as Class 1 Generation 2.

Power analysis is not new. It is well studied in the context of smart-card security, for instance. Oren and Shamir, though, are the first to demonstrate its practical importance to RFID.

Oren and Shamir's work has naturally attracted strong media coverage. Some of this coverage tends toward the sensationalist. As *RFID Journal* editor Mark Roberti has recently noted, the risk of such sensationalism (among those not yet jaded by it) is undue worry over security risks in RFID (see [RFID Security: A Reality Check](#)). However, there is also risk of the opposite happening—that the RFID industry will regard this vulnerability as a one-off problem that time and faded memories will redress. Such complacency is probably the greater risk.

Roberti downplays the Oren-Shamir attack for several reasons. First, he notes that the tag Oren and Shamir attacked has only an 8-bit PIN, while Class 1 Gen 2 tags have 32-bit PINs. A misunderstanding leads him to conclude that the attack will be many times harder for the latter type of tag—as much as brute force and, thus, exponential in the key length. He concludes, therefore, that such an attack would require an inordinate time to mount against Gen 2 tags. This is incorrect, however. In fact, the attack would probably only be about four times harder—i.e., linear in the key length. Basically put, the length of the PIN is of little consequence in the face of the Oren-Shamir attack.

Roberti also suggests the risk of an attacker running amok through a warehouse with a mobile phone is small, and that the design of the kill function in EPC tags is proportional to the threat. This is probably quite true today, but the EPC standard will persist for years—possibly even decades—and what is true today may not be the case tomorrow. When retail items carry EPC tags and tag-killing leads to easier shoplifting, then the threat will grow. When consumers carry live tags—as they eventually will for the many benefits RFID can bring to day-to-day life—and when hospitals, businesses and critical supply chains come to rely on functioning tags, then the stakes will grow further.

To carp about one flaw, however, is to miss the forest for the trees. The Oren-Shamir attack is important not because it reveals an implementation bug, but rather because it may point to a greater systemic problem. It seems an unshakable historical trend that serious attention to security in new technologies is deferred until problems become pressing and costly. Phishing and pharming tell this tale today on the Internet, and we've also seen it in cryptographic design flaws in 802.11 (Wi-Fi). We might ask ourselves now if this phenomenon is playing itself out in the world of RFID.

The kill function itself is an excellent example. [EPCglobal](#), the standards body responsible for the design and promotion of EPC tags, deserves kudos for anticipating consumer-privacy concerns and designing a privacy-protection measure. The industry, however, would benefit from further forethought. On the one hand, there is talk of killing tags to protect consumers. On the other hand, there is speculation about how tags can bring to consumers a rainbow of benefits like smart appliances—tag-interrogating washing machines and refrigerators, tag-reading and tag-bearing phones, receiptless item returns and so forth. The two visions are contradictory. In fact, consumers will very probably want to carry live RFID tags. We need to think about privacy beyond the point of sale.

Proximity cards provide another example. As recently [demonstrated by Jonathan Westhues](#), many of the contactless cards we use for building entry are themselves a kind of wireless bar code. Because they simply emit serial numbers, they are subject to cloning attacks. An attacker can easily skim a proximity card in your pocket and use a clone device in its place. Westhues has even been able to scan a proximity card through a wall.

As a team at [The Johns Hopkins University](#) and [RSA Laboratories](#) recently demonstrated, a popular antitheft RFID device present in tens of millions of automobiles contains only a 40-bit cryptographic key (see [Attack on a Cryptographic RFID Device](#)). The team built a special-purpose device able to crack such a key in about half an hour. (The manufacturer of the RFID device is, nonetheless, to be commended for including cryptographic protection at all.)

We must not overlay Oren and Shamir's work, as the practical, short-term implications are most likely small. Still, the long-term implications are not to be ignored. Their attack is an early warning that deployers of RFID should welcome and assimilate. To realize the tremendous promises of RFID, it behooves the industry to think about security and privacy early, and to treat them as important enabling aspects. Including top academic data-security researchers in the deliberations of EPCglobal and other standards bodies might be an excellent step in this direction.

Ari Juels is the principal research scientist and manager of applied research at [RSA Laboratories](#), the research center of RSA Security. His primary research area is data security, with emphases on authentication, biometrics, electronic voting and financial cryptography.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved