

# RFID Security: A Reality Check

The news that someone might be able to kill your EPC tags with their cell phone is not as scary as some news stories made out.

By Mark Roberti

Feb. 27, 2006—Two weeks ago, the *EE Times* reported that Adi Shamir, professor of computer science at the [Weizmann Institute of Science](#), told the [RSA conference](#) he was able to crack the passwords for the most popular brand of Gen 1 EPC tags and kill them. According to the *EE Times*, Shamir told the audience that “a cell phone has all the ingredients you need to conduct an attack and compromise all the RFID tags in the vicinity.”

When I read this article, I was extremely confused. How could a cell phone be used to kill the tags? Was he talking about 13.56 MHz tags and using a [Nokia](#) phone with a 13.56 MHz interrogator built in? But there are no high-frequency Gen 1 EPC tags. The article also failed to point out some very relevant facts—such as that Gen 1 EPC tags were not designed to be used in situations where security was a real concern.

*RFID Journal* associate editor, Mary Catherine O’Connor, followed up on the initial *EE Times* story and clarified these and other issues. She explained how a cell phone might be used to achieve what Shamir and fellow Weizmann researcher Yossi Oren did, using a directional antenna and digital oscilloscope. She also put the issues in context (see [EPC Tags Subject to Phone Attacks](#)).

Shamir and Oren used what’s called a side-channel attack. Instead of sending possible passwords until hitting on the right one, the hacker analyzes the behavior of the protected devices to “slowly insinuate” the correct password or key needed to access the protected data. Oren told O’Connor that using a cell phone, which operates in the UHF band, to do this kind of attack 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. Oren and Shamir didn’t create the firmware, and Orem told O’Connor he didn’t know how easy or hard it would be to do so. Therefore, a phone attack is only theoretical at this point. If Shamir mentioned these salient facts at the conference, they were not reported in the *EE Times* story.

The bigger problem with the original story and other articles that picked it up was the lack of context provided. The *EE Times* article says: “Shamir said the pressure to get tags down to five cents each has forced designers to eliminate any security features, a shortcoming that needs to be addressed in next-generation products.” There are two problems with this statement. First, it assumes every tag needs a great deal of data protection, regardless of its application. Second, it shows an ignorance of the fact that the next generation already has greatly enhanced security features.

The amount of security required for anything depends on the value of the thing being protected and the application involved. While my son Thomas’s drawings are precious to me, protecting them doesn’t require the same level of security as protecting a Van Gogh. The Gen 1 tag was designed for use in the supply chain, simply to track goods moving from point to point. The original idea was that there was no need for any security on the tags because they would have only a serial number and all the data about the product would be

secured in a database. Concerns that some tagged items could wind up in consumers' hands led the Auto-ID Center to introduce the kill command, which necessitated a security code to prevent people from killing tags accidentally or maliciously.

The possibility that someone would gain access to a Target distribution center or the back of a Wal-Mart store and start killing tags willy-nilly was remote, so the designers of the original Gen 1 tags decided that an 8-bit security code was sufficient. Given that millions of Gen 1 tags have been flowing through the supply chains of Wal-Mart and others without any incidents of Gen 1 tags being killed (outside of the Weizmann Institute), the practical decision made would seem to be the right one.

Whether Shamir and the EE Times are aware of it or not, EPC technology has already evolved to another level. The second-generation EPC protocol calls for a 32-bit security code. With an 8-bit code, there are 256 possible kill codes. If a cell phone could be used to hack a Gen 1 tag, Oren estimates it might take about a minute (but admits he's guessing because they didn't have a phone that could actually kill tags). A 32-bit kill code has more than 4 billion possible kill codes. Someone might have to spend hours (perhaps days) in the back of your warehouse pointing his cell phone at the tag on one of your cases to kill one tag. And for what? They would accomplish nothing more than proving an academic theory.

Security is becoming increasingly important as companies consider new applications for EPC tags. Pharmaceutical companies are looking at using EPC tags to create secure electronic pedigrees. Boeing and Airbus want to store parts' histories on tags. These companies are realizing that more secure tags are needed—tags that can't be hacked, spoofed or cloned. So groups within EPCglobal and the Auto-ID Labs are looking at whether there are any vulnerabilities in the Gen 2 tags and, if so, how they might be addressed.

There is value in academics pointing out that EPC and other RFID tags—especially those used by toll collection systems, contactless credit cards and other payment devices—have vulnerabilities. Once the makers of RFID devices know the vulnerabilities, they can address them.

There is also value in keeping the industry—and public—informed. The problem is that stories about security weaknesses get overplayed in the media. Journalists love to scare people because it encourages them to read articles. They love to use phrases such as “security expert,” “encryption algorithm” and “researchers at (fill in the blank) university” to give credibility to claims. They tend, however, to leave out the context that makes the story less frightening, which means end users could make bad business decisions based on misinformation, and people are led to worry more than they need to about these issues.

My view is that we should report the facts, present them in context and let people know when security weaknesses are a threat to their business. And right now, I don't think anyone should be losing any sleep over the possibility of a hacker killing the tags on cases in their supply chain with a cell phone.

*Mark Roberti is the founder and editor of RFID Journal. If you would like to comment on this article, click on the link below.*

Copyright ©2005 RFID Journal, Inc. All Rights Reserved