

EDITORIAL

Truth: RFID Can Be Hacked

A discussion of the failings of RFID and its unsuitability for authentication applications

The truth about RFID is beginning to emerge. The technology's effectiveness as an anti-counterfeiting tool is exaggerated. The faith placed in it by major organizations such as national health regulators and the military (especially in the USA) is cause for alarm. For example, earlier in the month, Lester Crawford, the acting commissioner of the US Food and Drug Administration said 'RFID is the cornerstone technology in the fight against counterfeit drugs because of its ability to track, trace and authenticate packages of drugs.' He did not reference other emerging technologies, despite many coming to market that may be more suited for anti-counterfeiting.

The problem is that this 'cornerstone' technology - recommended to authenticate drugs for the largest consuming market - can be easily hacked. This is because most supply chain software is written without security in mind, says Lukas Grunwald a self-professed computer geek and consultant at DN-Systems Enterprise Solutions.

Hackers are already having what they call 'fun' by reprogramming RFID tags. It doesn't seem that difficult. Grunwald says that RFID tags can be read by everyone. Electronic Product Codes (EPC) which are the codes used to track and trace tagged items can easily be re-programmed, he said. All you need is an RFID reader (which is publicly available - he uses a Multi-Tag Reader from ACG Germany), an antenna field, tags, a PC and a free downloadable software tool he built. Grunwald's form of fun in the grocery store includes reprogramming codes for X-Rated movies into G-Rated (now kids can buy them with a self-checkout) and converting expensive just-issued DVDs into sale items. Grunwald's software tool seems quite simple. It reads and writes ISO tags and smart-labels, detects nearly all smart-labels, requires an ACG Compact-Flash RFID Reader and can even run on a PDA. The software is available on his company's web site - www.rfdump.org

Public Safety Issues

All this would be amusing if we weren't dealing with issues of public safety, as is the case with pharmaceutical protection or auto parts, or with detection and prevention of IPR infringement (with its consequent loss of commercial and tax income). Since RFID is recommended as a major anti-counterfeiting breakthrough, the notion that the tags can be reprogrammed is shocking. In addition, there are also major concerns of privacy surrounding the technology. Marketers can read what type of underwear you are wearing, and what else you have in your shopping bag. Data can be collected on what type of books you read, what type of pharmaceuticals you use, and so on. With the advent of RFID chips to store biometric data in passports, the

holder's key identifier items could be scanned from several meters distance by an identity thief using an unobtrusive PDA. Imagine the goldmine of identities that could be stolen in a busy international airport departure lounge!

Even its proponents are backing away from RFID as an anti-counterfeiting tool. Representatives from Marks & Spencer and Philips recently presented at the PISEC conference in Vienna; M&S is moving from box-level tagging to item tagging, both for greater efficiency in distribution and inventory control. Philips has developed RFID-based systems for distribution and inventory control in the fashion industry and sees this having benefits in helping to control counterfeiting. So M&S is a real world adoption of RFID with no

aspect of authentication, while RFID manufacturer Philips sees it as a side-benefit, not the key driver of its marketing to the fashion industry.

False Assumptions

The support for this technology as an authentication tool also appears to be based on an assumption that the cost of each chip will fall, thus enabling it to be implemented affordably at unit-level packaging. But there is no indication that the price will fall to an acceptable unit-level, often estimated at cost of one cent per chip. According to a report by Highjump Software, a 3M subsidiary, users can expect to pay about 20 cents for a standard EPC-compliant tag. Readers are priced at approximately \$1,000 each.

What is frustrating about the run toward RFID in anti-counterfeiting is that there are many technologies that can perform similar roles which are much more difficult to alter. Elsewhere in this issue of Authentication News, we explore DNA taggants, which are offered by a variety of companies. DNA taggants are very difficult to replicate and can hold a number of codes far beyond that of EPC. DNA is only one of many examples. The list of these sorts of technologies is huge, and many of them would require much less infrastructural changes and less cost than RFID poses.

The FDA's original position in its Task Force *Report on Counterfeit Drugs*, released in February 2004, recommends the use of multiple layers of security technologies. This is sensible policy and one that is supported by Authentication News. The FDA, other health regulators and other key stakeholders should consider RFID as only part of an effective anti-counterfeiting solution. Perhaps this is still part of the main thrust of the FDA's policy. Crawford's recent remarks, however, gave little indication that the FDA realizes that a combination of security technologies is needed to help ensure the safety of medicines throughout the world.

RFID experts say there is no question the technology is easily altered with the assistance of a home computer
