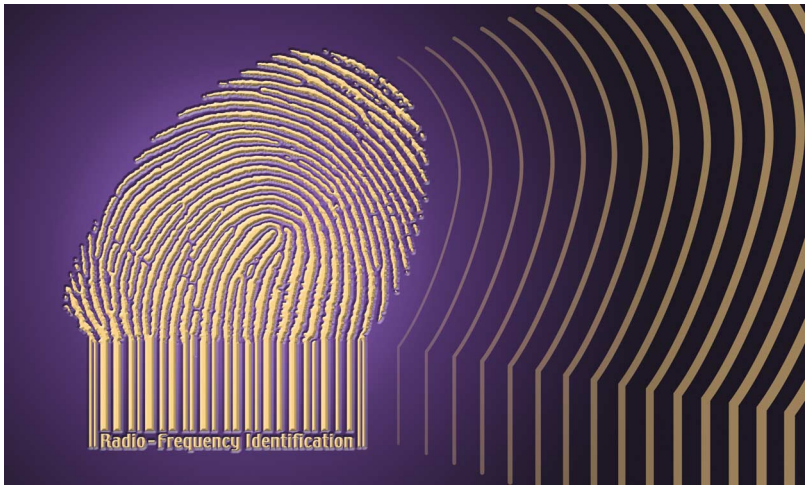
The Vision of Secure RFID

BY ARI JUELS



Radio frequency identification (RFID) is in essence a form of computer vision. RFID devices are wireless microchips conceived as a way of tagging objects for automated identification. In part, their purpose is to compensate for shortcomings in computer recognition of objects using cameras. Of course, RFID has an advantage over even the most acute eyes and brain: it is in fact a form of X-ray vision. When we hold wallets up to card readers to unlock doors, for instance, we experience the fact that RFID tags are readable through other, opaque objects. Under ideal circumstances, certain types of inexpensive RFID tags (with no embedded power source) are subject to reading at a distance of tens of feet.

RFID is poised then to become one of the sensory organs of our computing networks. Clarity in this emerging power of sight is important. Equally essential are the integrity of the data collected by RFID systems and appropriate curbs on the technology's X-ray power. In other words, the problems of *authentication* and *privacy* are fundamental to RFID security.

RFID is not in fact a single technology, but a spectrum of devices united by a single aim: To communicate the identity of an object or person through radio transmission. Much of the recent ferment around RFID has focused on a particular device known as an electronic product code (EPC) tag, a kind of next-generation barcode. Like a printed barcode, an EPC tag can carry a compact description of the object to which it is affixed. Additionally, though, an EPC tag carries a unique identifier, a serial number that distinguishes a given object—say a bar of chocolate—from all of the other millions of physically identical bars.

This serial number—along with RFID's potential for fast, automated scanning—implies a data-harvesting potential far beyond that of the ordinary, printed barcode. Employed as the pointer to an item-specific database record, the unique identifier in an EPC tag can index an arbitrarily rich pedigree or history for even the humblest of consumer items. (In the short term, RFID is largely serving to label crates and pallets, rather than individual packages, but the principle is the same.) In a seamless, global system, RFID can provide insight into the whereabouts and lifecycle events of billions of objects.

From this perspective, the problems of authentication and privacy seem to reside largely with databases. Consider, for example, RFID as an anti-counterfeiting tool—a role it is coming to play prominently in the pharmaceutical industry, for instance. Just as barcodes are easy to photocopy, basic EPC tags are easy to clone. It is a relatively straightforward matter to create a device whose radio emissions (if not physical appearance) are identical to those of a target tag. In other words, the very tool directed at combating counterfeiting is itself subject to counterfeiting.

This vulnerability is not immediately fatal, though. A comprehensive database with good monitoring tools could still protect against would-be counterfeiters. Suppose a counterfeiter wishes to introduce a crate of

Digital Object Identifier: 10.1109/JPROC.2007.900324

EPC-tagged counterfeit pharmaceuticals into a supply chain. She could tag her crate with the same serial number as an existing, legitimate crate. In that case, however, a single serial number would appear in the system *twice*—possibly in physically disparate locations. In a system with a global view of the supply chain, such duplication would signal the presence of a suspicious tag. Alternatively, the counterfeiter could concoct a new serial number. That event would likewise create an aberrance: an unregistered serial number.

Panoptic databases, however, are a convenient fiction, but an implausible reality. Supply-chain data systems today are highly fragmented, a state of affairs likely to persist in the face of the legal and procedural complications of data-sharing across organizations. As an RFID tag wends its way from one handler to the next—from factory to warehouse to the retail floor—it will spawn information across different systems. These systems may intercommunicate only sporadically and imperfectly. Thus, quick detection of cloned or forged EPC tags across a supply chain may prove difficult.

For this reason, it is valuable to build cloning resistance into or around RFID tags themselves. One intriguing approach involves the use of device or object "fingerprinting," essentially biometric identification for inanimate objects. Emerging research points at the possibility of inexpensive components that are difficult to duplicate even with physically invasive attack. (In fact, existing materials like paper may already carry this property.) The drawback to such fingerprinting approaches today is their reliance on direct optical contact, which negates the very benefit of X-ray vision that RFID confers. That said, anticounterfeiting strategies could rely on less frequent tag-scanning than inventorying operations. Moreover, some work suggests that "radio fingerprints" may one day be viable anti-counterfeiting tools.

In the short term, however, the most practical approach to RFID anti-counterfeiting is logical-layer authentication, that is, the use of secret data. For example, EPC tags may soon incorporate memory with password-protected read access. Suppose that a tag contains a secret S protected under a suitable password P. Even with direct radio access to the tag, a counterfeiter lacking knowledge of P will have difficulty extracting S. Thus, a trusted entity with knowledge of the secret pair (S, P) can check the authenticity of the tag simply by verifying the presence of the correct value S in its protected memory. (Irrespective of whether protected memory is available, the same goal is achievable by commandeering an existing, privacy-protecting feature on EPC tags known as the "kill" function.)

Full-blown cryptography is of course stronger than password-based authentication. An eavesdropper or rogue reader that intercepts the pair (S, P) can clone the target tag. If an RFID tag can perform a cryptographic challenge–response protocol, however, than eavesdropping attacks are no longer viable. Moreover, it is possible to entrust a reader with the ability to verify the authenticity of a tag but not to clone it. (Briefly, a reader may be given a *partial* secret—knowledge, that is, of a subset of the full challenge-response space.) Today, however, even symmetric-key cryptography is cost-prohibitive for inexpensive forms of RFID like EPC tags.

Cryptographic authentication is no panacea in any case. It introduces the overarching challenge of *key management*. In order to authenticate a tag, a reader must share a unique secret value with it—be it a password or a cryptographic key. The challenge of key management is this: How do we push secrets with appropriate protections through those supply chains whose very fragmentation demanded secrets to begin with? To our benefit, key distribution need not be real-time to operate effectively. But it is not a challenge to sniff at. The problem of key management lies at the heart of any security system, and will rear its head in any good secrets-based approach to RFID authentication or privacy. Techniques like public-key cryptography can help, but do not eliminate the problem— and they are expensive for small devices.

If there is any good advice in the face of these complications, it is to think early and carefully about how security should undergird essential RFID infrastructure. The Internet is already replete with security vulnerabilities. We do not want to add corrupted computer vision to the list. ■