RFID Is X-Ray Vision

In a world saturated with RFID tags, protecting the privacy of individuals is technically difficult. Without a proper alignment of interests it may be impossible.

Historically, the development and deployment of RFID-based systems has been driven primarily by large manufacturers and retailers looking for ways to track their inventory and its location in the supply chain. It is therefore not surprising that RFID brings more benefits to them than to individual consumers. The benefits for consumers remain largely hypothetical, while the privacy-invading threats are real. RFID proponents wonder how they can make the public accept and use the technology. Long-term success for RFID requires the alignment of the interests of all the parties involved.

Let's pretend we believe that, as they proclaim, the proponents of RFID are genuinely interested in protecting consumer privacy, not just in reaping efficiency and functionality benefits. What are the risks? What should technology developers and researchers protect? After discussing these issues I shall cynically indicate why it is currently unlikely that consumers will enjoy the RFID privacy that some of them vociferously demand.

A problem for developers building "smart" environments is that, despite very significant advances over the past few years, computers still can't reliably recognize objects and people in a scene. A quick fix is to label any items of interest with special tags that might be, for example, optical or electronic. The machines now recognize the tagged items even if they are still unable to make out any other detail in the scene. However, compared to human vision, after this treatment the computers see both too little and too much.

They see too little because they still don't really see the items; if developers program the machines to do something (such as opening your door when you are in front of it) based on the presence or proximity of an item, they will actually do it based solely on the presence or proximity of the tag. At the same time, machines also see too much, because radio tags can be scanned even through opaque materials. Your smart home can now tell when you're back; but so can the burglar. If you dismiss this as an unlikely threat, because you believe tags would only be affixed to objects rather than to people, then think of the RFID serial number in your eyeglasses or watch. Even if there is no single object that you carry every day, you may still be tracked by a subset of, say, your watch, wallet, and home keys. Ubiquitous, inescapable Orwellian surveillance.

With RFID, machines suddenly go from seeing a lot less than human eyes to seeing a lot more. With normal human eyesight, you can't see inside my briefcase, my home, or under my clothes. And I expect you not to be able to. RFID is not merely giving machines an imperfect kind of sight; it's giving them X-ray vision. Imagine what might happen [3]:

LISA HANEY

- For cyber-pickpockets, augmented reality glasses will superimpose dollar signs on the richest victims. The suggestion that banknotes might soon be tagged for anticounterfeiting purposes sounds like RFID's killer app—in the literal sense of "your money or your life." Even if the game of "who's got the biggest wad of cash" is technically infeasible because banknotes cannot be scanned from a distance, there are no obstacles to playing "who's got the Rolex" or even just "who's got the iPod" or the trendy cell phone; and
- More than personal privacy is at risk; a retail store might not like its competitors posing as customers and conducting covert inventory-monitoring raids.

What can be done about this? Researchers have proposed a variety of solutions, ranging from access-control protocols to jamming countermeasures. Some consumer groups favor the definitive opt-out choice of permanently killing the tag after purchase, which regrettably negates any potentially beneficial ubiquitous computing applications of RFID in the home. It is true, however, that none of the end-user applications so far proposed (such as the cyber-fridge that reorders milk over the Net or the frozen food package that communicates the appropriate cooking time and power setting to the microwave oven) is particularly compelling. While for businesses there are clear advantages in instrumenting the supply and retail chains with RFID, for individuals the risks seem to outweigh the benefits. But still, if I knew I could retain control, even I would like my smart home to be able to tell me on, say, which shelf in which room or behind which sofa I might find a particular book out of the 10,000+ I have. Can we build privacy-protecting safeguards into RFID systems?

To become as ubiquitous as the barcode, the RFID tag must be extremely cheap—no more than a couple of cents per tag. Except for Garfinkel's fair use guidelines [1], most of the privacy-protecting contributions in the literature are technology-driven countermeasures that attempt to do something useful within stringent hardware limitations. Here, to encourage discussion, I take a different approach: If there were no limitation on the computational power of the tags, what would we want to happen? My answer is the "ownership-based RFID security policy model," originally presented in my invited talk at the International Workshop Series on RFID in Tokyo in 2004.

The core idea of the policy is that the tag can be read only by its owner, who must also be the owner of the tagged object. Ownership is transferrable, as it is for everyday objects, but the invariant (tags readable only by their owners) must be preserved. I do not for the moment worry about how to implement this policy within realistic hardware constraints, only about choosing a simple, consistent, and fair set of rules. This policy concisely defines a reasonable boundary among the usage patterns that should be allowed and the ones that should be forbidden—although some subtle problem cases may persist near the edges. It will be instructive for users and developers to compare any proposed technical solutions against this abstract, high-level specification.

Privacy solutions are appropriate only if privacy is an objective. In the case examined here, namely preserving consumer personal privacy in a world saturated with tags, the main problem is that RFID proponents have a strong incentive to violate customer privacy. This incentive is price discrimination—the lucrative practice, described with exemplary lucidity by Odlyzko [2], of charging each customer the maximum amount he or she is prepared to pay, instead of selling at the same price to all buyers. Consumers express outrage at price discrimination when they notice it; sellers therefore disguise it with marketing mechanisms that obfuscate the true pricing structure. Luxury goods retailers, once they are able to read the tags on their customers' clothes ("This guy is wearing only designer garments"), can easily recognize the brand-addicted, price-insensitive buyers and entice them with individually tuned "discounts" over the inflated list price.

There may also be other considerations. In a political climate in which Western democracies frequently erode the civil liberties of their citizens in the name of the fight against terrorism, some governmental agencies will view universal X-ray vision as desirable. Just imagine what is likely to happen in airports when RFID technology is pervasively deployed. The next

time you go through security, the full content of your suitcase, including the serial numbers of all items, will be scanned (and logged forever for future data mining). Moreover, the customs officers will see through your luggage just as easily and remember everything you carried each time you were scanned; when you're back on home soil they will be able to spot that you didn't have this expensive digital camera when you flew abroad two weeks ago, even if you are now nonchalantly wearing it round your neck.

This is a perfect example of intrusive behavior from the state that many of us nowadays would consider outrageous but which has a chance of becoming legal if technology makes it easy, thanks to the often-abused excuse that law-abiding citizens have nothing to fear from it. After all, don't airport security officers worldwide already use real X-rays? (Answer: Yes, but this doesn't let them detect, store, and data-mine the model and serial number of every item carried by every passenger; with RFID, they could even compile lists of passengers who carried specific books in their luggage in the past year.)

If, as we initially agreed to believe, privacy protection is a common goal of all the parties involved in the RFID debate, then the study of technical solutions serves a purpose. In that spirit, the ownership-based security policy model helps clarify the protection goals, understand the trade-offs, and assess the validity of any proposed implementation. If, however, the true interests of the parties involved are fundamentally opposed, then any technical discussion has little practical relevance until that tension is resolved. C

References

1. Garfinkel, S. Adopting fair information practices to low-cost RFID systems. Presented at the Workshop on Socially Informed Design of Privacy-Enhancing Solutions in Ubiquitous Computing of Ubicomp 2002 (Göteborg, Sweden, Sept. 29–Oct. 1, 2002).
2. Odlyzko, A. Privacy, economics, and price discrimination on the Internet. In *Proceedings of ICEC 2003: Fifth International Conference on Electronic Commerce* (Pittsburgh, PA, Sept. 30–Oct. 3). ACM Press, NY, 2003, 355–366.
3. Stajano, F. *Security for Ubiquitous Computing.* John Wiley and Sons, Chichester, U.K., 2002.

Frank Stajano (www.cl.cam.ac.uk/~fms27/) is a lecturer (associate professor) at the University of Cambridge, Cambridge, U.K.