Technical Report

UCAM-CL-TR-645
ISSN 1476-2986

Number 645

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

RFID is X-ray vision

Frank Stajano

August 2005

15 JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom
phone +44 1223 763500

http://www.cl.cam.ac.uk/

Technical reports published by the University of Cambridge
Computer Laboratory are freely available via the Internet:

http://www.cl.cam.ac.uk/TechReports/

ISSN 1476-2986

RFID is X-ray vision*

Frank Stajano
University of Cambridge Computer Laboratory
http://www.cl.cam.ac.uk/~fms27/

Abstract

Making RFID tags as ubiquitous as barcodes will enable machines to see and recognize any tagged object in their vicinity, better than they ever could with the smartest image processing algorithms. This opens many opportunities for "sentient computing" applications. However, in so far as this new capability has some of the properties of X-ray vision, it opens the door to abuses. To promote discussion, I won't elaborate on low level technological solutions; I shall instead discuss a simple security policy model that addresses most of the privacy issues. Playing devil's advocate, I shall also indicate why it is currently unlikely that consumers will enjoy the RFID privacy that some of them vociferously demand.

1 Sentient machines

Writing is everywhere: wherever you may be right now, there is probably some object near you with some writing on it, even discounting the recursive circumstance that you are currently reading this sentence. As Tantau remarks, "Whenever you wear clothing, even a swim suit, there is a lot of text right next to your body." In the justly famous paper [12] that introduced "ubiquitous computing", Weiser envisaged a world in which computing and communication capabilities embed themselves into everyday objects as pervasively and unobtrusively as writing.

RFID appears likely to become the first wave in the actual deployment of the ubiquitous computing scenario: computing and communication functionality, albeit very primitive and specialized, embedded into billions of everyday objects. To a first approximation, once the price is right, there will be an RFID tag anywhere you now see a barcode.

There are indeed many similarities between barcodes and RFID tags—so many that it's easier just to focus on the differences. Conceptually, only two are significant: the code space cardinality and the transmission mechanism.

As for **code space cardinality**, the international EAN barcode standard consists of 13 decimal digits and is therefore limited to a million manufacturers, each allowed to define up to 100,000 products[1]. (The UPC barcode popular in the US has one less digit and hence can only encode 100,000 manufacturers.) The Auto-ID standard, in contrast, defines a 96 bit code and a

*Keynote talk at Workshop 1 of the International Workshop Series on RFID, 10 November 2004, Tokyo, Japan. Organized by Joint Forum for Strategic Software Research (SSR) and System LSI Research Center of Kyushu University.

[1]The first and last of the 13 digits are a type selector and a checksum.

partitioning scheme that allows for 256 million manufacturers and 16 million products per manufacturer. More importantly, there are still enough bits left to provide 64 billion serial numbers *for each individual product model*. While all the beer cans in the 24-pack look the same to the barcode scanner, with RFID each razor blade cartridge in the warehouse will respond with its own unique name when queried.

As for **transmission mechanism**, the barcode must be acquired optically and therefore must be aligned with the reader, as supermarket checkout cashiers know all too well. The RFID tag, instead, as its name indicates, uses radio frequency; it can therefore be read without requiring line of sight, so long as it is within range of the reader.

These two differences greatly enhance the possibilities of the new tagging technology compared to the old. Because the code embeds a unique serial number, you can prove with your till receipt that this defective item was sold to you in this store[2]; the manufacturer, in turn, when receiving the defective return from the retailer, knows exactly on what day and on which assembly line of which plant the item was made and can check for similar defects in any other items of the same batch. Because the code can be read without a manual alignment operation, the reading may happen on a continuous basis rather than just at the checkout: smart shelves, both in the supermarket and in your own kitchen, can list the products they contain and go online to reorder when they are running low.

The latter example points out how RFID technology can be helpful in implementing "Sentient Computing" [6]: computing systems with the ability to sense the world that surrounds them and to respond to stimuli in useful ways without the need for explicit prompting by their users. We emphasize that *sentient* is distinct from *intelligent*. This is not AI: in sentient computing, the link between stimulus and reaction must be simple, predictable and dependable. Accurate sensing of the real world is a hard problem. Despite great advances in machine vision and speech processing in recent years, further progress is still needed before such technologies can be integrated as dependable components of a sentient computing system. But RFID makes a big difference here.

2 Giving machines vision

Today's sentient computer has rather poor eyesight and it has difficulty seeing and recognizing the objects and people around it. We may view machine vision research as an attempt to give the computer good spectacles, or even laser surgery. A quicker if less elegant alternative, however, is simply to wrap any significant objects in a fluorescent yellow coat, so that they can be seen distinctly even by a very myopic computer. It's hard to make the machine see everything clearly, so we make it easier for the machine to see just those items we want it to see. By coating them yellow we make them stand out—we greatly increase the signal-to-noise ratio. Of course, here "seeing" is only meant in a primitive sense; the machine still can't make out any of the details in the scene, but at least it can now clearly recognize the items that we explicitly wrapped in fluorescent coats.

With RFID, therefore, we have given the sentient computer an imperfect but usable sense of sight. In what way is it imperfect? There are two diametrically opposite shortcomings: compared to human vision, the sentient computer now sees both too little and too much.

[2] An economics-literate cynic will ask why the store would ever print the RFID serial number on the till receipt, if the only consequence is to make the store more liable.

It sees **too little**, because it doesn't see actual objects but only their tags. If we tell the sentient computer to do something based on the presence, absence or proximity of an object, we must realize that it will only do it based on the presence, absence or proximity of the *tag*. The thief doesn't have to smuggle out the loot so long as he remembers to detach the tag before exiting the store. The spy doesn't have to hide from the camera before entering the restricted area, so long as she leaves her visitor badge outside. These are little more than jokes, of course, but they make a serious point.

Sentient computers now also see **too much**. If, in order for your machines to recognize and serve you, you put on a yellow coat, you now stand out. You can be immediately and reliably spotted from very far away, not just by your own electronic assistants but by anyone else too. And through walls. Your sentient home can now greet you when you come back and play your favourite music; but the burglar and the child molester, too, using their portable detectors, can check whether you are in or not. This is disturbing.

3 Giving machines X-ray vision

Sentient computers (and, through them, their masters) used to be able to see a lot less than human eyes. With RFID, they suddenly see a lot more. This may cause major privacy problems. With normal human eyesight, you can't see inside my backpack, inside my locked drawer, inside the boot of my car, or inside my home from the street. You can't see under my clothes. And I expect you not to be able to. So here is the crux of the privacy problem. RFID is not merely giving computers an imperfect kind of sight: it's giving them *X-ray vision*.

- Ladies too embarrassed to reveal their dress size to their best friend will be unwittingly broadcasting that and much more, including bra cup size and whether they are wearing Bridget Jones big pants or a sexy G-string, to any stalkers within radio range.

- Pickpockets won't have to guess which of these unattended bags is worth rummaging through during that short window of opportunity: augmented reality goggles will superimpose dollar signs on the bags that are worth the effort. And the suggestion that banknotes might soon be equipped with a sub-millimetre chip for anti-counterfeiting purposes sounds like RFID's *killer app*—but in the literal sense of "your money or your life!".

- The last example is admittedly a caricature, because it is unlikely that banknotes could be scanned from any great distance; but the more general point about the dangers of granting X-ray vision to cyber-pickpockets is not exaggerated. Even if the game of "who's got the biggest wad of cash" is technically infeasible, what would be the obstacle to playing "who's got the Rolex" or, at less exalted levels, "who's got the trendy cellphone"?

- Since readers do not require line of sight to work, you may be silently scanned as frequently as every few minutes during the course of your normal day—and you won't know who is scanning you. Someone might aggregate these sightings to track your whereabouts, keeping a log of everywhere you have been. The RFID serial number of your watch or eyeglasses becomes a pseudonym that always refers to you; and location privacy researchers [2, 5] have proved that it is usually easy to map this back to your real-world identity. Even if there is no single object that you carry every day, you may still be tracked by the intersection of what Weis *et al.* [11] describe as "constellations" of such objects: pen, comb, wallet, clothes etc.

- Since it is now fashionable to obsess about terrorist threats, observe that, if individuals can be identified by their RFID signatures, political targets might be ambushed with dormant bombs triggered to detonate when the right RFID signature is recognized.

- It is not only personal secrets that are at risk: a retail store might not like its competitors posing as customers and conducting covert inventory monitoring raids on a regular basis.

What can be done about this? Researchers have proposed a variety of solutions, from protocols that restrict the reading operation to certain principals [11] to hardware or software jamming countermeasures [7]. Some consumer groups favour 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.

Even hardened ubicomp proponents must admit 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 for a non-nerd. While for businesses there are clear advantages in instrumenting the supply and retail chain with RFID, for individuals the risks seem to outweigh the benefits. But still, even though as a security professional I have a natural inclination towards the paranoid standpoint, as a gadget lover I am reluctant to give up the technological possibility of rigging up a smart home able to tell me on which shelf in which room or behind which sofa[3] I might find a particular book out of the 10,000+ I have. Can we build privacy-protecting safeguards into RFID systems?

4 Ownership-based RFID security policy model

To become as ubiquitous as the barcode, the RFID tag must be very cheap: there are severe constraints on the gate budget and on the availability of special components such as non-volatile memory. Most of the privacy-protecting contributions in the literature, except perhaps for the fair use guidelines of Garfinkel's "RFID Charter" [4], are technology-driven countermeasures that attempt to achieve the best possible result within the stringent limitations of current and foreseeable hardware.

To encourage discussion I shall instead take a different approach: if anything were possible, technology-wise, what would we want? Can we draw up a security policy model, in the spirit of Bell-LaPadula [1] and Clark-Wilson [3], to indicate unambiguously the protection goals of the system? Here is a sketch of my proposal.

My aim in drafting such a policy is to define in a concise and self-consistent way the usage patterns that should be allowed and the ones that should be disallowed. I am not for the moment worried about how the policy could be implemented within realistic hardware constraints, at least until we agree that it is sound and fair. Ideally it should allow all the intended uses of the technology and stop all the objectionable ones (a laudable but unattainable goal).

The central idea of the policy is simply the Reading rule: the tag can only be read by its owner. The Binding rule, not present in the Tokyo draft of the policy, was introduced to eliminate the loophole through which I attach one of my tags to your shoe and then I "legitimately" track you because I am only just reading my own tag. The Ownership rule may seem obvious given the intuitive semantics of the term "owner" but it was originally introduced to eliminate

[3] Or, even better, in which of the too numerous overflow storage boxes...

Ownership-based RFID security policy model

Reading. A tag can only be read by its owner, unless the Delegating rule (q.v.) says otherwise. *(If the tag and associated object change owner, the right to read is transferred to the new owner and lost by the old owner.)*

Binding. Whenever a tag is attached to an object, the owner of the tag and the owner of the object must coincide. *(This implies that, if the object changes owner, the tag must be either transferred to the new owner or separated from the object.)*

Ownership. No tag and no tagged object may have more than one owner.

Lending. Whenever an object is lent, its ownership is temporarily transferred to the recipient. *(The lender no longer "owns" the object, and therefore has no right to read its tag, until it is returned.)*

Delegating. The owner of a tag may allow or disallow other principals to read the tag. *(This delegation does not transfer ownership, does not transfer the right to delegate any further, and does not remove the right to read from the owner. If the tag and associated object change owner, the right to delegate is transferred to the new owner and lost by the old owner.)*

similar loopholes, hidden but available if one abuses the definition: I nominate you joint owner of one of my tags and I affix the tag to your shoe, but I also remain owner of the tag myself; then I can track you legitimately, as above, because the tag on your shoe is also mine.

There is still another powerful attack: I could lend you an object without transferring ownership of it, say my pen, and track you through that for as long as you carry it. An isomorphic problem, pointed out during the workshop by Christian Floerkemeier, is that of the shopper filling up her trolley in the supermarket and who can still be tracked by the supermarket owner while on the shop floor because, until checkout, her shopping has not been paid for yet and therefore is still owned by the supermarket[4]. Someone suggested to define access rights in terms of who is *carrying* the tagged object; but this seems too fuzzy to act as a good foundation for a consistent security policy[5]. I believe that a better solution is to introduce a Lending rule, stipulating that lending an object has the same effects on access rights as temporarily trans-

[4] A more devious supermarket owner would track the shopper by following the trolley itself (which of course the supermarket owns), rather than the goods it contains. In fact this is just another instance of the attack described above, with the supermarket owner purposefully "lending" the trackable trolley to the unsuspecting customer. Even worse, the supermarket owner could link the partial profile of the customer built out of the current shop visit (what items s/he purchased this time and how long s/he spent in each aisle) to long-term identity inferred from payment information provided by the shopper on checkout.

[5] To show the ambiguity of the notion of "who is carrying it", think of "nested carriers": when you carry your groceries on a bus, are they being carried by you, by the bus driver or both? Does the answer temporarily change if you let go of the carrier bag? If you forget it on the bus? What about the collar worn by the pet carried by the little child you carry in your arms on the bus? And then think of goods in storage: who is carrying them? Who would be entitled to scan items that nobody is carrying?

ferring its ownership. The difficulty, however, then shifts to defining all the circumstances in which lending should be seen as taking place—the supermarket examples above and in footnote 4 show how subtle the issue may be.

The Delegating rule was added to provide a legitimate but controlled mechanism for the occasionally desirable functionality of multiple access. In its absence, a number of plausible applications could only be made acceptable through semantic perversions of the kind we chose to prevent by introducing the Ownership rule.

5 Incentives for and against privacy

As always in security, one of the best ways to assess threats is to follow the money. In the case of RFID, a problem is that businesses actually have a strong incentive to violate customer privacy. This incentive is *price discrimination*—the lucrative practice, described with exemplary lucidity by Odlyzko [8], 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, treat them with deference proportional to their expected expenditure and entice them with individually tuned "discounts" over the inflated list price.

A different way of using RFID tags for price discrimination, namely *regioning*, was pointed out by Ross Anderson during one of the discussions of the Computer Lab's security group at Cambridge in 2004. Just as DVD producers find it lucrative to charge Europeans more than Americans for the same movies, so makers of fashionable blue jeans like to extort higher prices from markets that can bear them, but don't mind a lower profit in poorer or more competitive areas where they would not otherwise sell much. Until now, the arbitrage made possible by grey imports has limited the price differential; with RFID, though, this safety valve would disappear, as individual garments would become fully traceable. (Do not be fooled by the fact that the introduction of RFID in fashion items is going to be marketed as an anti-counterfeiting measure: the purpose of regioning is blocking cheap imports of *authentic* goods—nothing to do with fakes.)

There may also be issues outside the economic sphere. 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 government agencies will view universal X-ray vision as a desirable surveillance tool. Just imagine what is likely to happen in airports when RFID technology is pervasively deployed. 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 [10], but that's a slightly different story). 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, and will automatically issue you with a hefty fine if you don't declare it. 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.)

6 Conclusions

Until now, the development and deployment of RFID 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 main privacy threat of RFID is that it enables a kind of X-ray vision. So far, the benefits for customers are few and hypothetical, while the privacy-invading threats are real. Still, this is a multi-party game and, as such, it requires an alignment of incentives in order to succeed.

If, as claimed, privacy protection is a common goal of all the parties involved in the RFID debate, and the problem is how to achieve it while reaping the envisaged efficiency and functionality benefits of the technology, then the study of technical solutions serves a purpose. In that spirit, discussing 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.

Acknowledgements

This article is the revised write-up of the keynote talk I gave at the first gathering in the "International Workshop Series on RFID" in Tokyo, Japan in November 2004, which had no formally published proceedings. It includes and extends some ideas from my 2002 book [9]. The Tokyo talk was my first public presentation of the ownership-based policy. I am grateful to Sozo Inoue of Kyushu University for inviting me and to the workshop attendees for interesting comments and discussions that have allowed me to improve this material.

A condensed version of this article also appears as a "Viewpoint" in the September 2005 issue of *Communications of the ACM*, a special issue dedicated to RFID. I am grateful to guest editor Gaetano Borriello for inviting me to contribute to that issue.

References

[1] D. Elliot Bell and Leonard J. LaPadula. "Secure Computer Systems: Mathematical Foundations". Mitre Report ESD-TR-73-278 (Vol. I–III), Mitre Corporation, Bedford, MA, Apr 1974.

[2] Alastair Beresford and Frank Stajano. "Location Privacy in Pervasive Computing". *IEEE Pervasive Computing*, **2**(1):46–55, Jan 2003. `http://www.cl.cam.ac.uk/~fms27/papers/2003-BeresfordSta-location.pdf`.

[3] David D. Clark and David R. Wilson. "A Comparison of Commercial and Military Computer Security Policies". In "Proceedings of the 1987 IEEE Symposium on Security and

Privacy", pp. 184–194. IEEE Technical Committee on Security and Privacy; and International Association for Cryptologic Research, IEEE Computer Society Press, Oakland, CA, 27–29 Apr 1987. ISBN 0-8186-0771-8.

[4] Simson Garfinkel. "Adopting Fair Information Practices to Low Cost RFID Systems". In "Ubicomp 2002 Privacy Workshop", Göteborg, Sweden, 29 Sep 2002. http://www.simson.net/clips/academic/2002_Ubicomp_RFID.pdf.

[5] Marco Gruteser and Dirk Grunwald. "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking". In "Proceedings of MobiSys 2003", pp. 31–42. The Usenix Association, San Francisco, CA, USA, 5–8 May 2003. http://systems.cs.colorado.edu/Papers/Generated/2003anonymousLbs.pdf.

[6] Andy Hopper. "The Clifford Paterson Lecture, 1999. Sentient Computing". *Phil. Trans. R. Soc. Lond. A*, **358**(1773):2349–2358, Aug 2000. http://www.cl.cam.ac.uk/Research/DTG/lce-pub/public/files/tr.1999.12.pdf.

[7] Ari Juels, Ronald L. Rivest and Michael Szydlo. "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy". In V. Atluri (ed.), "Proc. 8th ACM Conference on Computer and Communications Security", pp. 103–111. ACM Press, 2003. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf.

[8] Andrew M. Odlyzko. "Privacy, economics, and price discrimination on the Internet". In N. Sadeh (ed.), "ICEC2003: Fifth International Conference on Electronic Commerce", pp. 355–366. ACM, 2003. http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf.

[9] Frank Stajano. *Security for Ubiquitous Computing*. John Wiley and Sons, Feb 2002. ISBN 0-470-84493-0. http://www.cl.cam.ac.uk/~fms27/secubicomp/.

[10] Frank Stajano. "Will Your Digital Butlers Betray You?" In Paul Syverson and Sabrina De Capitani di Vimercati (eds.), "Proceedings of the 2004 Workshop on Privacy in the Electronic Society", pp. 37–38. ACM, Washington, DC, USA, 28 Oct 2004. ISBN 1-58113-968-3. http://www.cl.cam.ac.uk/~fms27/papers/2004-Stajano-butlers.pdf.

[11] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels. "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems". In "Security in Pervasive Computing", vol. 2802 of *Lecture Notes in Computer Science*, pp. 201–212. 2004. http://theory.lcs.mit.edu/~sweis/spc-rfid.pdf.

[12] Mark Weiser. "The Computer for the Twenty-First Century". *Scientific American*, **265**(3):94–104, Sep 1991. http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html.