RFID PRIVACY: A TECHNICAL PRIMER FOR THE NON-TECHNICAL READER

DRAFT: 23 FEBRUARY 2005

Ari Juels
RSA Laboratories
Bedford, MA, USA
ajuels@rsasecurity.com

Abstract RFID (Radio-Frequency IDentification) is a wireless identification technology poised to sweep over the commercial world. A basic RFID device, often known as an "RFID tag," consists of a tiny, inexpensive chip that transmits a uniquely identifying number over a short distance to a reading device, and thereby permits rapid, automated tracking of objects. In this article, we provide an overview of the privacy issues that RFID gives rise to. While technically slanted, our discussion aims primarily to educate the non-specialist.

We focus here on basic RFID tags of the type poised to supplant optical barcodes over the coming years, initially in industrial settings, and ultimately in consumer environments. We describe the challenges involved in simultaneously protecting the privacy of users and supporting the many beneficial functions of RFID. In particular, we suggest that straightforward approaches like "killing" and encryption will likely prove inadequate. We advance instead the notion of a "privacy bit," effectively an on/off data-privacy switch that supports several technical approaches to RFID privacy enforcement.

Keywords: blocker, encryption, EPC, kill command, privacy, RFID

1. Introduction

RFID (Radio-Frequency IDentification) is a technology that facilitates the automated identification of objects. While people are generally skillful at visual identification of a range of objects, computers are not. The task of identifying a coffee mug as a coffee mug is one that many bleary-eyed people perform naturally and effectively every morning in a variety of contexts. For computing systems, this same task can pose a challenging exercise in artificial intelligence.

The simplest way to ease the process of automated identification is to equip objects with computer-readable tags. This is essentially what happens in a typical supermarket. Through a printed barcode on its packaging, a can of tomato soup identifies itself automatically to a checkout register. While a checkout clerk must manually position items to render them readable by a scanner, printed barcodes alleviate the overhead of human categorization and data entry. Over the course of well more than two decades, they have proven indispensable timesavers and productivity boosters.

An RFID chip, also referred to as an RFID tag, is in effect a wireless barcode. It comprises a silicon microprocessor and an antenna in a package that is generally in size and form like an ordinary adhesive label. An RFID tag can be as small, though, as a grain of sand, and can even be embedded in paper [8]. An RFID tag carries no internal source of power; rather, it is simultaneously powered and read by a radio-emitting scanner. Under ideal circumstances, an RFID tag is readable through obstructions at a distance of up to several meters.

RFID confers a powerful advantage lacking in the optical barcode: It largely eliminates the need for human positioning of objects during the scanning process. This feature promises a new order of automated object identification. For example, it could eventually render checkout clerks in supermarkets obsolete. Once RFID-tagging is universal, a customer might be able to roll a shopping cart full of items by a point-of-sale scanner that would ring them up without human intervention – and automatically mediate payment as well. This vision extends to the factory and warehouse as well, where RFID could enable automated inventory-taking and ultimately even robot-guided item selection and assembly.

RFID tags have another advantage over optical barcodes. Today, every product of a given type - every 150-count box of Kleenex® tissues, for example - carries an identical barcode. With existing printing processes and scanning standards, it is impractical for individual boxes to bear unique serial numbers. In contrast, RFID tags do actually transmit unique serial numbers in addition to product information. An RFID scanner can distinguish one box of tissues from the many other millions of exactly the same type. RFID therefore permits much finer-grained data collection than optical barcodes do.

RFID in some sense endows computing systems with the ability to "see" objects. By merit of their unique serial numbers and wireless transmission, RFID tags enable computing systems in certain respects to outstrip human beings. An RFID system can "see" visually obstructed objects, and can distinguish automatically between objects that are otherwise physically identical. The implications of such power for industrial automation and productivity are tremendous. Thanks to their role in streamlining inventory operations and thereby cutting costs, billions of RFID tags are likely to see use in the commercial world over the next few years. To name just a few examples: Wal-mart® and the United

States Department of Defense, among others, are mandating that their major suppliers apply RFID tags to pallettes of items by 2005 [22] (although there has been some lag in compliance); the U.S. FDA is advocating use of RFID to secure pharmaceutical supplies [7]; tens of millions of pets have RFID tags implanted under their skin so that they can be traced to their owners in case of loss [1]; a company called VeriChip is extending this concept to human beings by selling a human-implantable RFID tag [20].

Our concern in this article is the effect on individual privacy of RFID-enabled computing systems that can automatically "see" everyday objects - the clothing on your person, the medical implants in your body, the prescription drugs you are carrying, the payment devices in your pocket, and perhaps even individual pieces of paper, like banknotes and airline tickets.

Computer perception of everyday objects would confer undoubted benefits: If you are lost in an airport or parking lot, an RFID-based system that can guide you to your gate or car would be appealing. So too would be the ability to return items to shops without receipts, either for refunds or warranty servicing, and RFID-enhanced medicine cabinets that ensure that you have remembered to take your medications. (In fact, a group at Intel has created prototypes of this idea [6].) But RFID could engender many malicious activities and nuisances as well, including clandestine profiling and physical tracking. Articles in the popular press have tarred RFID with Orwellian catchwords and monikers like "spy-chips" [11]. Privacy advocates have even mounted boycotts against companies using RFID [14].

As we shall explain, both the utopian and dystopian visions surrounding RFID are largely hypothetical at this point. But privacy is and will be an important issue in RFID systems, one that we should take steps to address in the early stages of deployment, as standards and practices take shape that will persist for many years. This article will treat the question of RFID privacy from a technically focused perspective. In short, we shall consider the question: What technical options do we have for protecting privacy and simultaneously preserving the many benefits of RFID?

2. Four essential facts about RFID privacy

Any meaningful discussion of RFID privacy must proceed in view of four essential facts.

1 "RFID" often serves as a catch-all term. Wireless barcodes are one manifestation of RFID. Other wireless devices may also be viewed as forms of RFID. Among these are the SpeedPass^{TM} payment tokens now used by millions of consumers in the United States, as well as contactless building-access cards and toll-payment transponders in automobile windshields used worldwide. These different technologies have in-

commensurable technical properties. Toll-payment transponders, for instance, carry batteries to boost their transmission range, while SpeedPass^{TM} and wireless barcodes are "passive," meaning that they have no internal power sources. SpeedPass^{TM} executes a form of cryptographic challenge-response (anti-cloning) protocol, while wireless barcodes lack the circuitry to do so. Thus, while all of these wireless devices bear significantly on consumer privacy, they do not lend themselves to easy categorical discussion. Rather, "RFID" denotes a broad and fluid taxonomy of devices that share the characteristic of wireless transmission of identifying information. Loosely speaking, the term RFID may even apply to your mobile phone - a kind of hypertrophied RFID tag. In this article, we use the term "RFID tag" to refer to the very basic and cheap (ultimately perhaps five-cent/unit) wireless barcode. Tags of this kind have only barebones computing power, and are essential designed just to emit an identifier, i.e., a string of numbers.

The major standard for RFID tags is under development by an entity known as EPCglobal - a joint venture of the UCC and EAN, the bodies regulating barcode use in the U.S. and Europe respectively. Tags defined by this standard are often referred to as Electronic Product Code (EPC) tags. These are the type we concern ourselves with principally here - particularly the most basic types, known as Class 0 and 1 tags. Up-to-date details on EPC tags may be found on the EPCglobal Web site [3].

2 RFID tags – again, of the wireless-barcode variety – are unlikely to have a considerable presence in the hands of consumers for some years to come. The entities spearheading RFID-tag development now through EPCglobal - including large corporations such as Wal-mart ® and Proctor & Gamble® – are looking to RFID mainly to manage cases and pallets of items in the supply-chain, not to tag individual consumer products. There are exceptions, of course. The U.K. retailer Marks and Spencer, for example, has initiated RFID tagging of individual items of apparel [2]. For several reasons, however, most notably tag cost and the persistence of existing data-management infrastructure, RFID tags will in all probability supplant product barcodes only gradually. Any discussion of the topic of RFID and consumer privacy in the year 2005 is necessarily futuristic. EPC-tag privacy may be a topic of immediate import for the year 2015 or 2020. This is not to discount the value of the debate now: The persistence of data-management infrastructure will not mean gradual RFID deployment, but will also mean that once deployed, the RFID designs of 2005 - with all of their features and drawbacks - may be the predominant ones in 2020. Moreover, consumer use

of barcode-type RFID is happening in a limited way already, as libraries, for instance, begin tagging books with RFID [12].

3 RFID tags are unreliable – at least at present. The hypothetical scanning range of a passive RFID tag is on the order of some tens of meters. In practice, it is at best a few meters. RFID signals do propagate through obstructions. In practice, however, metals - such as the foil lining of a can of potato chips - can play havoc with RFID signals. Additionally, the type of passive RFID tag with the longest range, known as an ultra-high frequency (UHF) tag, is subject to interference in the presence of liquids. This factors significantly into the issue of consumer privacy, because human beings consist largely of water [15]. If you're worried about your RFID-tagged sweater being scanned, your best course of action may be to wear it!

   Even when RFID systems scan effectively, they do not achieve omniscient perception of their surroundings. The company NCR conducted a pilot involving automated shopping-cart inventorying at an RFID-based check-out register [23]. This exercise revealed that *good* scanning range could pose problems: Customers sometimes ended up paying for the purchases of those behind them in line!

   Of course, these are the technical obstacles of today. Improvements in reader and RFID-tag antenna technology, changes in packaging, different use of radio spectrum, and techniques yet to be conceived will no doubt lead to improved effectiveness. One should not wholly credit either the view of RFID systems as unerring nor the view that they are too shoddy to pose a threat to consumer privacy. It is hard to say exactly how they will evolve.

4 A final point: RFID privacy is not just a consumer issue. RFID tags on products could facilitate corporate espionage by offering an easy and clandestine avenue for harvesting inventory information [19]. Among leaders in the deployment of RFID is the United States Department of Defense. Battery-powered RFID tags played a significant role in management of materiel in the second Gulf War, for example [16]. (It is recounted that prior to this campaign, the supply chain was so poor that the only reliable way to procure a helmet, for example, was to order three helmets. RFID has purportedly remedied this situation to some extent.) RFID could create infringements of privacy that are uncomfortable or even dangerous for consumers. For the military, infringements of privacy could be lethal. The idea of RFID-sniffing munitions is illustration enough.

In its increasingly prevalent practice of using off-the-shelf technologies, the Department of Defense may use EPC tags - the same RFID tags serving the needs of industry. This places an extra burden of privacy enforcement on the developers of EPC tags.

Nor is it RFID tags alone that pose a threat of data compromise in an RFID system. RFID readers and their associated computing facilities in warehouses will harvest valuable business intelligence - valuable to its legitimate consumer as well as to industrial spies. Broadly speaking, RFID stretches the security perimeter of computing networks into the physical world.

3. The nature of the threat

EPC tags will include several pieces of information, most notably a product-type identifier, a manufacturer identifier, and a unique serial number. Thus, the RFID tag on a sneaker might indicate that it is a "year 2005 tennis shoe" that is "manufactured by Adidas ®," and that it has been assigned the unique serial number "38976478623." (These pieces of information will be represented in the form of numerical codes.)

The threat of privacy infringement from RFID is twofold. First, the presence of a unique serial number in an RFID tag opens up the possibility of clandestine physical tracking. Suppose that Alice pays for her sneakers using a credit card. The shop she has patronized can make an association between the name "Alice" and the serial number "38976478623." Whenever Alice returns to the shop, her identity can be established automatically - a situation valuable for marketing. If this information is sold, then Alice's sneaker might betray her identity more widely. By further linking the sneaker serial number with Alice's credit history, shops might make decisions about the level of service that Alice should receive. And so forth.

In fact, the threat of physical tracking does not require a direct binding between names and serial numbers. If Alice participates in a political rally, for example, law enforcement officers might note her sneaker as belonging to a suspect individual. By using RFID readers deployed strategically around a city, officers might track and/or apprehend Alice.

A second threat arises from the presence of product information in RFID tags. This information in principle permits clandestine scanning of the objects on Alice's person. If Alice is carrying a painkilling drug with a high street value, she could be more vulnerable to mugging. The European Central Bank purportedly considered a plan a few years ago to embed RFID tags in banknotes [5]. These would probably have been very short-range tags designed for combating counterfeiting, but who knows what unanticipated abuses they might have engendered? Alice could also be subject to profiling of various

types. If she is wearing a Rolex, she might receive preferential treatment in jewelry shops - and poor service if she is wearing a cheap digital watch. If she is carrying a book on anarchism, she might trigger a law-enforcement watch when she walks by a police station. If she walks by a video screen carrying a bottle of Pepsi®, she might see a Coca-Cola® advertisement, and soon and so forth.

It is worth remarking that bold sallies into marketing-based exploitation of RFID as sketched above seem implausible. Corporations are too sensitive to their reputations among consumers. The threat in commercial settings probably stems more from gradual erosion of privacy. Clothing stores might, for instance, begin by offering discounts to customers wearing their garments. (They could even do so with customer permission by retaining only scanned information present in a specially designated database.) Shops might offer automated RFID-based payment and RFID-based warranty fulfillment and returns. Habituation is a slippery slope. More aggressive RFID-based marketing and other infringements might increasingly assume an air of innocuousness to consumers that would open the door to abuses. (As a useful analogy, witness changes in the ethos of the entertainment industry. These have gradually led to common production of content that would have seemed outrageously inappropriate but a few decades ago.)

Remark. In some circles there circulates a misconception that effective privacy protection may be achieved by storing the correspondence between EPC codes and their natural-language meanings in a "secure" database. Apart from the fact that such a database would need to be open to a large community to operate effectively, sophisticated resources are not required to ascertain that a number like "15872918" means "Coca-Cola Classic ®." It suffices to scan a single bottle of Coca-Cola Classic ® to learn this correspondence.

Why RFID privacy may matter

Irrespective of the contours that RFID technology ultimately assumes, it is the belief of this author that consumer privacy will be an important and psychologically evocative issue - more so than other technologies that permit tracking of human behavior, such as credit cards and browser cookies. RFID has several properties of particular psychological potency.

To begin with, RFID tags are palpable, and physically present with their owners. This is true of other devices like mobile phones, but there is a key difference. A mobile phone transmits information that is accessible (without specialist eavesdropping equipment) only by a well-regulated service provider. In contrast, RFID tags will be readable by any off-the-shelf scanning device. Additionally, it is likely that consumers will make use of RFID tags in ways that will render them conscious of the technology's presence and function.

When consumers perform item returns, when they are able to walk by scanners in clothing stores that read off their apparel sizes (for convenience), and so forth, they will perceive with strong immediacy that they are radiating personal information. Additionally, mobile phone models are available today that have (very short-range) RFID readers [13]. Thus consumers may come to scan RFID tags for their own purposes, such as comparison shopping and cataloging of personal possessions.

What could ultimately bring RFID privacy to the fore are a few stark, baleful, and well publicized incidents of privacy infringement: Muggings that involve use of RFID scanners to locate bottles of prescription information, for example. Passports are soon to be deployed with RFID tags [21]; these could cause an outcry if they betray personal information for use in identity theft. Privacy infringement through RFID has the potential to draw attention to itself in striking ways.

4. Proposed remedies to the RFID privacy problem

A form of very basic radio-frequency technology is already familiar in retail shops today. Electronic Article-Surveillance (EAS) systems rely on small plastic tags to detect article theft. Items that bear these tags trigger alarms at shop exits when improperly removed by customers. When EAS-tagged items are purchased, of course, their EAS tags are deactivated or removed. EAS systems have naturally pointed the way for RFID: Why not simply remove or deactivate RFID tags on purchased items to avoid privacy problems?

EPC tags support this approach by inclusion of a *kill* feature. When an EPC tag receives a special "kill" command from a reader (along with a tag-specific PIN for authorization), it permanently disables itself. Of course, "dead tags tell no tales." The presence of the kill command seems at first glance to kill the privacy debate.

Theft detection stops outside the shop door. The consumer benefits of RFID don't. We have mentioned the fact that consumers regularly carry RFID devices like SpeedPass^{TM} and contactless building-access cards already, and have also described some of the useful applications of ubiquitous RFID-tagging in the future, including "smart" medicine cabinets that monitor compliance with medication regimes [6], and receipt-free consumer item returns. Many more such applications are envisaged. These include "smart" appliances, like refrigerators than can draw up shopping lists, suggest meals based on available ingredients, and detect expired foodstuffs, washing machines that can detect garments that may be harmed by a given temperature setting, and clothing closets that can provide fashion advice. A company called Merloni has already prototyped a range of RFID-enabled appliances [1]). For recycling - namely accurate identification of plastic types - RFID would be a boon.

There are countless other proposed examples - and examples not yet imagined - how RFID can and undoubtedly will benefit ordinary people. The critical point here is that consumers will invariably want to have "live" RFID tags in their possession. Killing tags at the time of purchase will help address privacy problems in the short term, but in the long term will prove unworkable as it undercuts too many of the benefits of RFID. The same remark applies even to partial information "killing," e.g., the elimination of unique serial numbers at the point of sale, with the retention of item-type information.

A kindred approach, advocated by EPCglobal [4], is to make RFID tags easily visible to the consumer and easily removable. Indeed, Marks and Spencer adopted this tack; they incorporated RFID into price tags rather than directly into the garments they were tagging. In general, however, this approach has the same drawback as the killing of tags: It undercuts the consumer benefits. And reliance on tag removal carries the additional drawback of inconvenience. It is difficult to imagine consumers assiduously poring through their shopping bags peeling off RFID tags. It is likewise difficult to imagine a valetudinarian carefully peeling RFID tags off her collection of medication bottles at the exit to a pharmacy. She could remove tags at home instead, but by then may already have walked the streets broadcasting the presence of a bottle of painkillers with a high street value.

A supplementary remedy advocated by EPCglobal and by some policymakers is consumer notification. Signage or product packaging would notify consumers of the presence of RFID tags on store items. While this may result in somewhat more vigorous peeling of labels (the exercise of a right to opt-out), it hardly offers consumers a convenient and effective avenue for privacy protection. It is indeed loosely analogous to signs that warn of video surveillance – except that RFID tags, unlike video cameras, will follow consumers home.

There is a simple physical means of enforcing RFID privacy protection. As mentioned above, metals interfere with RFID signals. It is possible to prevent radio signals from reaching an RFID device by enclosing it in a metal mesh or foil of an appropriate form, known as a Faraday cage. An agency of the State of California recently adopted this approach in offering mylar bags to shield toll-payment transponders from scanning when not in use. They bags offered a way to opt out of state-initiated programs that use such transponders to monitor traffic patterns. Faraday cages, however, are of limited utility. They not only prevent scanning of RFID tags on privately owned items, but also serve in evading EAS systems, i.e., abetting in-store theft. For this reason, retail shops are unlikely to support their widespread use. Faraday cages are also likely to be of little utility when and if RFID tags are embedded in a wide range of personal possessions, such as items of clothing.

The siren song of encryption

Encryption is a technique for shielding data from unauthorized access. Viewed in this light, its application to the problem of RFID privacy seems natural. But encryption does not provide a straightforward solution to the problems of privacy protection. If the product information and serial number on an RFID tag are encrypted, then they are readable only upon decryption under a valid secret key. This protects privacy, but introduces a new problem: How is the secret key to be managed?

A simple scenario is highly illustrative. Suppose that Alice purchases an RFID-tagged carton of milk at a supermarket. To protect her privacy as she walks home, the information on the carton is encrypted at the supermarket under some secret key k. Of course, Alice wants her refrigerator to be able to read the RFID tag on the carton of milk. Therefore her refrigerator must somehow be provisioned with the secret key k for use in decryption.

This key k might be printed on the milk carton, enabling Alice to enter it manually into her refrigerator by means of, e.g., a numeric keypad. This would be laborious, though. Alternatively, the key might be stored in a special portion of RFID tag memory, and Alice might release it by making physical contact with the tag, e.g., by touching it with a special-purpose wand. Physical intermediation of this kind would be still tedious.

A more convenient solution would be for Alice to make use of a supplementary device, a smartcard or a mobile phone, for instance, to manage the key k on her behalf. For example, Alice's mobile phone might furnish the key k to a supermarket point-of-sale device for encryption of her RFID tags at the time that she makes her purchase.

Suppose, however, that Alice is buying the carton of milk for her friend Bob. Alice would then either have to encrypt the milk information under a key belonging to Bob, or else transfer her secret key k to Bob. Yet Alice and Bob might not trust one another sufficiently to share keys.

As an alternative, the key k might be item-specific, i.e., the carton of milk might have its own associated encryption key k that is not shared with any other item. That way, Alice could freely transfer it to Bob without compromising her own secrets. But then Alice assumes the burden of managing the secret key for a single carton of milk.

The problem of enabling users to protect and distribute secret keys is known to data security experts as the "key management problem." Key management has proven historically to be one of the great challenges in securing computing systems of any kind, even when each user possesses just a single cryptographic key. (Think of the headaches that passwords cause today.) Requiring ordinary consumers to manage keys for individual items would make the problem even more difficult. Suppose that the carton of milk is leaky, and Alice would like

to return it to the supermarket, but her mobile phone battery is dead and she can't recover the key for the milk? When all of the natural scenarios involving Alice and her carton of milk are taken into account, encryption rapidly loses its appeal as a privacy-protection measure.

Moreover, straightforward encryption of tag data does not address the full range of basic privacy problems. Consider the problem of physical tracking. Suppose that the data D on the carton of milk are encrypted as a number E, and the RFID tag stores E instead of D. A malefactor that scans E may not know what data it represents, and therefore that he has scanned a carton of milk. Nonetheless, he can use E as a unique serial number for the purposes of physically tracking Alice. In other words, if D is a unique serial number for the carton of milk, then E is essentially a meta-serial-number!

Similar caveats vex related privacy-enhancing ideas, like that of putting tags to "sleep" upon purchase, and then "waking" them when they are ready for home use. If a tag can be awakened by just anyone, then the sleep function does not protect against surreptitious scanning of tags. Therefore, a sleeping tag must require a special accompanying key or PIN k to authorize waking. Management of the key k in this case presents many of the same challenges as those illustrated above in management of a decryption key k.

It is possible that as consumer devices like mobile phones evolve, reliable and convenient key-management systems will arise in support of RFID privacy. Prognostication on this score would be misguided. From today's perspective on RFID privacy, however, encryption does not adequately solve the most pressing problems.

Remark. In the scenarios we have just described, encryption of tag data is presumed to be performed by some external device, e.g., a point-of-sale device. More sophisticated approaches to privacy protection are possible if tags themselves can perform standard cryptographic operations like encryption. As noted above, however, due to the exigencies of cost, basic RFID tags do not contain a sufficient amount of circuitry to do so [17, 18]. Moore's Law - the long established trend toward a halving of circuitry costs every eighteen months or so - is sometimes viewed as an argument that tags will eventually be available to perform cryptographic operations. It is important to keep in mind, however, that cost is likely to trump functionality in RFID tags for quite some time. Given the choice between a five-cent cryptographically enabled tag and a rudimentary one-cent tag, a retailer or manufacturer is very likely to choose the latter, particularly given the volumes and slender margins on which their businesses depend. The situation could change with the development of more compact ciphers, but this is pure speculation. More importantly, even when RFID tags can perform cryptographic operations, it is still not immediately clear how to solve the vital privacy problems.

5. A technical proposal: The privacy bit

The remainder of this article will briefly explore the notion of an RFID *privacy bit* as suggested in [9, 10]. This is a simple, cost-effective technical proposal by the author for mitigating the problems of RFID privacy while preserving the consumer benefits of RFID. The aim is to strike a good balance between privacy and utility – to eat our cake and have it too.

A privacy bit is a single logical bit resident in the memory of an RFID tag. It indicates the privacy properties of the tag. A tag's privacy bit may be *off*, indicating that the tag is freely subject to scanning, as in a supermarket or warehouse; or it may be *on*, indicating that the tag is in the private possession of a consumer. To permit changes in the privacy properties of an RFID tag, its privacy bit should be writable by an RFID scanner. The operation of changing the privacy bit should naturally require authorization via an RFID-tag-specific PIN - just like the kill command described above.

As an accompaniment to the privacy bit, an additional tag feature is required. An RFID reader is able to scan tags in one of two modes, public or private. When a tag's privacy bit is on, the tag responds only to private-mode scanning. If the privacy bit is off, the tag responds to either scanning mode.

To illustrate how the privacy bit works, let us consider its use in a clothing store of the future - which we'll call ABC Fashions. The RFID tags on ABC Fashions garments initially have their privacy bits turned off. They remain off at the factories where the garments are manufactured, in the warehouses they pass through, and on the racks and shelves of the ABC Fashions shops. In any of these places, garments may be scanned normally and naturally: The presence of the privacy bit has no impact on the RFID operations of ABC Fashions.

The privacy bit comes into play when Alice purchases a garment at ABC Fashions - say a blouse. At this point, the privacy bit in the attached RFID tag is turned on.

Scanners in the ABC Fashions shops perform public-mode scanning. Thus, these scanners can perceive and inventory unpurchased items on racks and shelves. Likewise, theft-detection portals in ABC Fashions shops can detect unpurchased items. (Note in fact that the privacy bit serves not only to enforce privacy, but also supports electronic article surveillance!) To ensure privacy scanners in ABC Fashions and other shops do not perform private-mode scanning. Thus ABC Fashions scanners cannot scan purchased items, because their privacy bit is turned on. The same is true of the scanners in other shops and public locations that Alice might enter while carrying or wearing her blouse: They cannot scan it.

In Alice's home, RFID scanners perform private-mode scanning. Therefore, Alice's RFID-enabled clothing closet can tell her when her blouse needs to be

cleaned, can search the Web for suggestions on colors of trousers to match her blouse, and so forth. Her RFID-enabled washing machine can warn her if she has placed her blouse in a wash cycle that might harm the fabric, or with colors that might stain it. If Alice gives the blouse as a gift, her friend Carol can equally well benefit from the presence of the RFID tag on the blouse.

Basic enforcement

This is all very well, but the privacy-bit concept is only effective if ABC Fashions and others are respectful of privacy-enhancing scanning policies. What is to prevent ABC Fashions from setting its RFID readers to perform private-mode scanning and harvesting information from the private tags of its customers? And then even if public entities behave responsibly, what is to prevent a thief or rogue law-enforcement officer from initiating private-mode scanning?

Thankfully, the privacy-bit concept need not depend on goodwill alone. There are some effective technical mechanisms for enforcing responsible privacy policies. The simplest is to place restrictions on the software (or firmware) capabilities of RFID readers according to their arena of deployment. This is effectively the approach used today for digital-rights management. A piece of software like Apple's iTunes, for instance, restricts the ways and extent to which users can download, share, and play pieces of music. In principle, by changing the underlying software, it is possible to bypass these restrictions. The effort and saavy required to do so, however, serve as barriers to abuse. Similarly, RFID readers might be equipped to perform private-mode scanning only when appropriate. The RFID reader in a refrigerator might perform private-mode scanning, while RFID readers of the type deployed on shop shelves might only be equipped to perform public-mode scanning. With sufficient expertise, someone might bypass restrictions on reader capabilities, but basic technical barriers might suppress the most common forms of abuse.

More importantly, it is possible to audit RFID scanners independently to verify that they comply with desired privacy policies. In order to execute private-mode scanning, an RFID reader must emit a private-mode scanning command. The emission of this command is readily detectable. It should be possible in the near future, for example, for a mobile phone to detect and alert its owner to the emission of an unexpected and possibly invasive private-mode RFID query. The possibility of simple public auditing would serve as a strong check on RFID privacy abuses.

Blocking

It is possible to achieve even stronger protection against inappropriate scanning by means of a device known as a blocker [10]. A blocker obstructs in-

appropriate private-mode scanning. It does not perform true signal jamming, which violates the regulations of most governments. Rather, a blocker disrupts the RFID scanning process by simulating the presence of many billions of RFID tags and thereby causing a reader to stall. (We gloss over the technical details here.) By carrying a blocker, a consumer can actively prevent the scanning of her private RFID tags.

A blocker can itself take the form of a cheap, passive RFID tag. Thus, it would be possible, for instance, for ABC Fashions to embed RFID blocker tags in its shopping bags. When carrying her blouse home, Alice would then be protected against unwanted scanning. When Alice places her blouse in her closet or washes it, however, its RFID tag would remain operative. (When she wears the blouse, she might rely on the water in her body to prevent unwanted scanning – or she might carry a blocker with her.)

For greater range and reliability, a blocker could alternatively be implemented in a portable device like a mobile phone. In this case, many nuanced technical mechanisms for policy enforcement are possible. For example, a mobile phone might block private-mode scanning by default, but refrain from blocking if a scanner presents a valid digital certificate authorizing it to perform private-mode scanning. Many other variant ideas are possible.

Remark. Blockers are sometimes objected to on the grounds that they can be crafted to interfere maliciously with public-mode scanning and mount denial-of-service attacks. This is true. But malicious blockers can readily be created whether or not privacy-preserving blockers exist. Malicious blockers are not a good reason for avoiding the use of privacy-preserving blockers.

Standards support

For the privacy bit concept to reach fruition, it would require support in technical standards, such as those of EPCglobal. Once the problems of consumer privacy become sufficiently apparent to the developers and deployers of RFID systems, this author hopes that EPCglobal and other standards bodies will support the idea.

6. Conclusion

We have presented an overview of some of the technical facets of RFID privacy. The most striking lesson here is that while RFID is a conceptually simple technology, it engenders technological questions and problems of formidable complexity.

For this reason, it is unwise to view RFID privacy as a technological issue alone. Policymaking and legislation will also have a vital role to play in the realm of RFID privacy. They must not only supplement the protections that

technology affords, but must prove sensitive to its novelties and nuances. Regulating RFID is not like regulating the Internet or the transmission of credit-card information or the use of mobile phones; each technology has distinctive characteristics. Moreover, RFID is simultaneously an embryonic and rapidly changing technology, resistant to prognostication. RFID will bring to policy-makers the opportunity to enjoy a camaraderie with technologists in grappling with a difficult and stimulating set of problems. Let us hope that they can together achieve the delicate balance between privacy and utility needed to bring RFID to its high pitch of promise.

References

[1] C. Booth-Thomas. The see-it-all chip. *Time*, 22 September 2003. Available at http://www.time.com/time/globalbusiness/article/0,9171,1101030922-485764,00.html.

[2] J. Collins. Marks & Spencer expands RFID retail trial. *RFID Journal*, 10 February 2004. Available at http://www.rfidjournal.com/article/articleview/791/1/1/.

[3] EPCglobal Web site. www.epcglobalinc.org, 2004.

[4] Guidelines on EPC for consumer products, 2004. Available at http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html.

[5] Security technology: Where's the smart money? *The Economist*, pages 69–70, 9 February 2002.

[6] K. P. Fishkin, M. Wang, and G. Borriello. A ubiquitous system for medication monitoring. In *Pervasive 2004*, 2004. Available as 'A Flexible, Low-Overhead Ubiquitous System for Medication Monitoring,' Intel Research Seattle Technical Memo IRS-TR-03-011, Oct. 25, 2003.

[7] United States Food and Drug Administration. Combatting counterfeit drugs: A report of the Food and Drug Administration, 18 February 2004. Available at http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html.

[8] Hitachi unveils smallest RFID chip. *RFID Journal*, 14 March 2003. Available at http://www.rfidjournal.com/article/articleview/337/1/1/.

[9] A. Juels and J. Brainard. Soft blocking: Flexible blocker tags on the cheap. In S. De Capitani di Vimercati and P. Syverson, eds., *Wireless Privacy in the Electronic Society (WPES '04)*, pp. 1-8. ACM Press, 2004.

[10] A. Juels, R.L. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In V. Atluri, editor, *8th ACM Conference on Computer and Communications Security*, pages 103–111. ACM Press, 2003.

[11] D. McCullagh. Are spy chips set to go commercial? *ZDNet*, 13 January 2003. Available at http://news.zdnet.com/2100-9595_22-980345.html.

[12] D. Molnar and D. Wagner. Privacy and security in library RFID : Issues, practices, and architectures. In B. Pfitzmann and P. McDaniel, editors, *ACM Conference on Communications and Computer Security*, pages 210 – 219. ACM Press, 2004.

[13] Nokia unveils RFID phone reader. *RFID Journal*, 17 March 2004. Available at http://www.rfidjournal.com/article/view/834.

[14] Benetton to Tag 15 Million Items. *RFID Journal*, 12 March 2003. Available at http://www.rfidjournal.com/article/articleview/344/1/1/.

[15] M. Reynolds, 15 November 2003. Invited talk at MIT RFID Privacy Workshop. Slides available at http://www.rfidprivacy.org/2003/papers/physicsofrfid.ppt.

[16] M. Roberti. RFID Upgrade Gets Goods to Iraq. *RFID Journal*, 23 July 2004. Available at http://www.rfidjournal.com/article/articleview/1061/1/1/.

[17] S. E. Sarma, S. A. Weis, and D.W. Engels. Radio-frequency identification systems. In Burton S. Kaliski Jr., Cetin Kaya Koc, and Christof Paar, editors, *CHES '02*, pages 454–469. Springer-Verlag, 2002. LNCS no. 2523.

[18] S.E. Sarma. Towards the five-cent tag. Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001. Available from http://www.epcglobalinc.org.

[19] R. Stapleton-Gray. Would Macy's scan Gimbels? competitive intelligence and RFID, 2003. Available at www.stapleton-gray.com.

[20] Verichip corporation web site, 2004. http://www.4verichip.com/.

[21] M. L. Wald. New High-Tech Passports Raise Concerns of Snooping. *New York Times*, 26 November 2004. p. 28.

[22] Wal-Mart, DOD forcing RFID. *Wired News*, 3 November 2003.

[23] D. White, 15 November 2003. Video Presentation at MIT RFID Privacy Workshop.