RFID Security and Privacy: A Research Survey

Ari Juels
RSA Laboratories
ajuels@rsasecurity.com

28 September 2005

***Abstract*— This article surveys recent technical research on the problems of privacy and security for RFID (Radio Frequency IDentification).**

RFID tags are small, wireless devices that help identify objects and people. Thanks to dropping cost, they are likely to proliferate into the billions in the next several years – and eventually into the trillions. RFID tags track objects in supply chains, and are working their way into the pockets, belongings and even the bodies of consumers. This survey examines approaches proposed by scientists for privacy protection and integrity assurance in RFID systems, and treats the social and technical context of their work. While geared toward the non-specialist, the survey may also serve as a reference for specialist readers.

A condensed version of this survey will appear in the *IEEE Journal on Selected Areas in Communication* (J-SAC) in 2006.

Keywords: authentication, cloning, counterfeiting, EPC, privacy, security, RFID

I. Introduction

RFID (Radio-Frequency IDentification) is a technology for automated identification of objects and people. Human beings are skillful at identifying objects under a variety of challenge circumstances. A bleary-eyed person can easily pick out a cup of coffee on a cluttered breakfast table in the morning, for example. Computer vision, though, performs such tasks poorly. RFID may be viewed as a means of explicitly labeling objects to facilitate their "perception" by computing devices.

An RFID device – frequently just called an RFID *tag* – is a small microchip designed for wireless data transmission. It is generally attached to an antenna in a package that resembles an ordinary adhesive sticker. The microchip itself can be as small as a grain of sand, some 0.4mm^2 [82]. An RFID tag transmits data over the air in response to interrogation by an RFID reader.

In both the popular press and academic circles, RFID has seen a swirl of attention in the past few years. One important reason for this is the effort of large organizations, such as Wal-Mart, Procter and Gamble, and the United States Department of Defense, to deploy RFID as a tool for automated oversight of their supply chains. Thanks to a combination of dropping tag costs and vigorous RFID standardization, we are on the brink of an explosion in RFID use.

Advocates of RFID see it as a successor to the optical barcode familiarly printed on consumer products, with two distinct advantages:

1) *Unique identification:* A barcode indicates the type of object on which it is printed, e.g., "This is a 100g bar of ABC brand 70% chocolate." An RFID tag goes a step further. It emits a unique serial number that distinguishes among many millions of identically manufactured objects; it might indicate, e.g., that "This is 100g bar of ABC brand 70% chocolate, serial no. 897348738."[1] The unique identifiers in RFID tags can act as pointers to a database entries containing rich transaction histories for individual items.
2) *Automation:* Barcodes, being optically scanned, require line-of-sight contact with readers, and thus careful physical positioning of scanned objects. Except in the most rigorously controlled environments, barcode scanning requires human intervention. In contrast, RFID tags are readable without line-of-sight contact and without precise positioning. RFID readers can scan tags at rates of hundreds per second. For example, an RFID reader by a warehouse dock door can today scan stacks of passing crates with high accuracy. In the future, point-of-sale terminals may be able to scan all of the items in passing shopping carts [90].

Due to tag cost and a hodgepodge of logistical complications – like the ubiquity of metal shelving, which interferes with RFID scanning – RFID tags are unlikely to appear regularly on consumer items for some years. Retailers have expressed interest, though, in ultimately tagging individual items. Such tagging would, for instance, address the perennial problem of item depletion on retail shelves, which is costly in terms of lost sales.

Today, RFID is seeing fruition in the tagging of crates and pallets, that is, discrete bulk quantities of items. RFID tagging improves the accuracy and timeliness of information about the movement of goods in supply chains.

The main form of barcode-type RFID device is known as an EPC (Electronic Product Code) tag. An organization known as EPCglobal Inc. [25] oversees the development of the standards for these tags. Not surprisingly, EPCglobal is a joint venture

[1] In principle, barcodes can uniquely identify objects, of course; two-dimensional barcodes on shipped packages do so, for instance. In practice – particularly in retail environments – unique barcoding has proven impractical.

of the UCC and EAN, the bodies that regulate barcode use in the United States and the rest of the world respectively.

EPC tags cost less than thirteen U.S. cents apiece in large quantities at present [2]. Manufacturers and users hope to see per-tag costs drop to five cents in the next few years [75]. RFID readers cost several thousand dollars each, but it is likely that their cost will soon drop dramatically.

In the quest for low cost, EPC tags adhere to a minimalist design. They carry little data in on-board memory. The unique index of an EPC tag, known as an EPC code, includes information like that in an ordinary barcode, but serves also as a pointer to database records for the tag. An EPC code today can be up to 96 bits in length [47].[2] Database entries for tags, of course, can have effectively unlimited size, so that the recorded history of a tag and its associated object can be quite rich. EPCglobal has developed a public lookup system for EPC tags called the ONS (Object Name Service), analogous in name and operation with the DNS (Domain Name System). The purpose of the ONS is to route general tag queries to the databases of tag owners and managers.

In general, small and inexpensive RFID tags are *passive*. They have no on-board power source; they derive their transmission power from the signal of an interrogating reader. Passive tags can operate in any of a number of different frequency bands. LF (Low-Frequency) tags, which operate in the 124 kHz – 135 kHz range, have nominal read ranges of up to half a meter. HF (High-Frequency) tags, operating at 13.56 Mhz, have ranges up to a meter or more (but typically on the order of tens of centimeters). UHF tags (Ultra High-Frequency), which operate at frequencies of 860 MHz – 960 MHz (and sometimes 2.45GHz), have the longest range – up to tens of meters. UHF tags, though, are subject to more ambient interference than lower-frequency types. Later in this survey, we enumerate the major standards for passive RFID devices.

Some RFID tags contain batteries. There are two such types: *semi-passive* tags, whose batteries power their circuitry when they are interrogated, and *active* tags, whose batteries power their transmissions. Active tags can initiate communication, and have read ranges of 100m or more. Naturally, they are expensive, costing some $20 or more.

A. RFID today and tomorrow

Many of us already use RFID tags routinely. Examples include:

- Proximity cards, that is, the contactless cards used for building access.
- Automated toll-payment transponders – the small plaques mounted in automobile windshields. (These are usually semi-passive.)
- The ignition keys of many millions of automobiles, which include RFID tags as a theft-deterrent.
- Payment tokens: In the United States, the SpeedPass^{TM} token for petrol station payments is an example. Contactless credit-cards, like American Express ExpressPay^{TM} and the Mastercard PayPass^{TM} use RFID.

Some fifty million house pets around the world have RFID tags implanted in their bodies, to facilitate return to their owners should they become lost.

In a world where everyday objects carried RFID tags – perhaps the world of the future – remarkable things would be possible. Here are a few possibilities (among the myriad that the reader might dream up):

- **Smart appliances:** By exploiting RFID tags in garments and packages of food, home appliances could operate more cleverly. Washing machines might select wash cycles automatically, for instance, to avoid damage to delicate fabrics. Your refrigerator might warn you when the milk has expired or you have only one remaining carton of yogurt – and could even transmit a shopping list automatically to a home delivery service.[3]
- **Shopping:** In retail shops, consumers could check out by rolling shopping carts past point-of-sale terminals. These terminals would automatically tally the items, compute the total cost, and perhaps even charge the consumers' RFID-enabled payment devices and transmit receipts to their mobile phones. Consumers could return items without receipts. RFID tags would act as indices into database payment records, and help retailers track the pedigrees of defective or contaminated items.
- **Interactive objects:** Consumers could interact with RFID-tagged objects through their mobile phones. (Some mobile phones already have RFID readers.) A consumer could scan a movie poster to display showtimes on her phone. She could obtain manufacturer information on a piece of furniture she likes by waving her phone over it.
- **Medication compliance:** Research at Intel and the University of Washington [32] exploits RFID to facilitate medication compliance and home navigation for the elderly and cognitively impaired. As researchers have demonstrated, for example, an RFID-enabled medicine cabinet could help verify that medications are taken in a timely fashion. More generally, RFID promises to bring tremendous benefits to hospitals [30].

B. But what, really, is "RFID"?

We have discussed the basics of RFID and laid out some evocative scenarios. Yet we have not formally defined the term "RFID." A wholly satisfying definition is elusive. But it is not a mere pedantic exercise: The definition of RFID can have an important impact on technical and policy discussions.[4]

In this article, we use "RFID" to denote any RF device whose main function is identification of an object or person. At the rudimentary end of the functional spectrum, this

[2]The expectation at the time of writing is that the EPC codes will soon expand to a minimum of 128 bits in length – with extensions for 256 bits or more.

[3]The company Merloni has built prototype RFID-enabled appliances [7].

[4]For example, in March 2005, Wired News published an article [16] highlighting privacy concerns raised by a Department of Homeland Security (DHS) project to issue RFID identification cards known as DAC cards ("DHS access cards"). While vigilant about privacy concerns, DHS responded that such concerns were largely misplaced, and resulted from a misunderstanding: DAC cards, the agency said, would not be RFID devices, but ISO 14443 devices. (ISO 14443 is an international standard for proximity cards.)

definition excludes simple devices like retail inventory tags, which merely indicate their presence and on/off status. It also excludes portable devices like mobile phones, which do more than merely identify themselves or their bearers. A broad definition for "RFID" is appropriate because the technical capabilities and distinctions among RF devices will drift over time, and the privacy and authentication concerns that we highlight in this paper apply broadly to RF identification devices great and small. Most importantly, though, the names of standards like 'ISO 14443" or "EPC Class-1 Gen-2" do not trip off the tongue or inhere well in the mind. The term "RFID" will unquestionably remain the popular one, and the term according to which most people frame debate and policies – a fact it behooves technologists to remember.

Of course, standards precisely define classes of RF devices. It is worth briefly mentioning the major ones. ISO 18000 is a multi-part standard that specifies protocols for a number of different frequencies, including LF, HF, and UHF bands. For UHF tags, the dominant standard will very likely be the recently ratified EPCglobal Class-1 Gen-2 standard. For HF tags, there are two main standards apart from ISO 18000. ISO 14443 (types A and B) is a standard for "proximity" RFID devices; it has a nominal 10cm operating range. ISO 15693 is a more recent HF standard for "vicinity" RFID devices; it can achieve longer nominal ranges – up to 1m for large antenna setups. (Mode 1 of ISO 18000 Part 3 is based on ISO 15693.)

Also of note is the NFC (Near-Field Consortium) standard (NFCIP-1/ECMA340, ISO 18092). Compatible with ISO 14443 and ISO 15693, this HF standard transcends the fixed tag-reader model, in that an NFC device can operate as either a reader or a tag, and thus either transmit or receive. Some mobile phones today support NFC; many portable devices may well in the future.

C. Security and Privacy Problems

1) Privacy: RFID raises two main privacy concerns for users: clandestine *tracking* and *inventorying*.

RFID tags respond to reader interrogation without alerting their owners or bearers. Thus, where read range permits, clandestine scanning of tags is a plausible threat. As discussed above, most RFID tags emit unique identifiers, even tags that protect data with cryptographic algorithms (as we discuss below). In consequence, a person carrying an RFID tag effectively broadcasts a fixed serial number to nearby readers, providing a ready vehicle for clandestine physical tracking. Such tracking is possible even if a fixed tag serial number is random and carries no intrinsic data.

The threat to privacy grows when a tag serial number is combined with personal information. For example, when a consumer makes a purchase with a credit card, a shop can establish a link between her identity and the serial numbers of the tags on her person. Marketers can then identify and profile the consumer using networks of RFID readers – both inside shops and without. The problem of clandestine tracking is not unique to RFID, of course. It affects many other wireless devices, such as Bluetooth-enabled ones [51].

In addition to their unique serial numbers, certain tags – EPC tags in particular – carry information about the items to which they are attached. EPC tags include a field for the "General Manager," typically the manufacturer of the object, and an "Object Class," typically a product code, known formally as a Stock Keeping Unit (SKU).[5] (See [47] for details.) Thus a person carrying EPC tags is subject to clandestine inventorying. A reader can silently determine what objects she has on her person, and harvest important personal information: What types of medications she is carrying, and therefore what illnesses she may suffer from; the RFID-enabled loyalty cards she carries, and therefore where she shops; her clothing sizes and accessory preferences, and so forth. This problem of inventorying is largely particular to RFID.

Today the problems of clandestine RFID tracking and inventorying are of limited concern, since RFID infrastructure is scarce and fragmentary. As explained above, the tagging of individual retail items is probably some years away. Once RFID becomes pervasive, however, as is almost inevitable, the privacy problem will assume more formidable dimensions. One harbinger of the emerging RFID infrastructure is Verisign's EPC Discovery Service [48]. It creates a unified view of sightings of individual EPC tags across organizations.

Figure 1 illustrates the threat of clandestine RFID inventorying as it might in principle emerge in the future.

Remark: Some people like to point out that mobile phones already permit wireless physical tracking, and are practically ubiquitous. Mobile phones, however, have on/off switches. More importantly, mobile phones transmit signals receivable only by specialized telecommunication equipment. The owner of a mobile phone mainly reposes trust in her service provider. By contrast, most RFID tags are scannable by commodity RFID readers, which will soon be everywhere. Of course, mobile handsets increasingly exploit new channels like Bluetooth and WiFi, so some of the privacy distinctions between RFID tags and mobile phones will erode. Mobile phones, though, have fairly considerable computing power, and can support sophisticated forms of access control.

There is already considerable political and media ferment around RFID privacy. Several consumer advocacy groups have mounted campaigns against RFID deployment in retail settings. In 2003, for example, a boycott [3] caused Benetton to disavow RFID-tagging plans for its garments (amid misconceptions about the company's plans [6]). In the same year, a group of privacy organizations signed a position statement on the use of RFID in consumer products [27].[6]

RFID privacy is already of concern in several areas of everyday life:

- **Toll-payment transponders:** Automated toll-payment transponders – small plaques positioned in windshield

[5]These fields are short numerical codes that are meaningful, like barcodes, only upon translation. Services like the ONS will publicly translate General-Manager codes into human-readable form. Manufacturers may or may not choose to make their Object-Class codes publicly available. These codes will be easy to determine, however, with or without reference to the manufacturer: Scanning one instance of a given product type will reveal its Object Class.

[6]Participation in this movement is varied and colorful. It includes well established civil liberties groups like the ACLU. It also includes at least one highly visible RFID opponent motivated by a fear that RFID may fulfill the prophesy of the Mark of the Beast from the Book of Revelation [15].

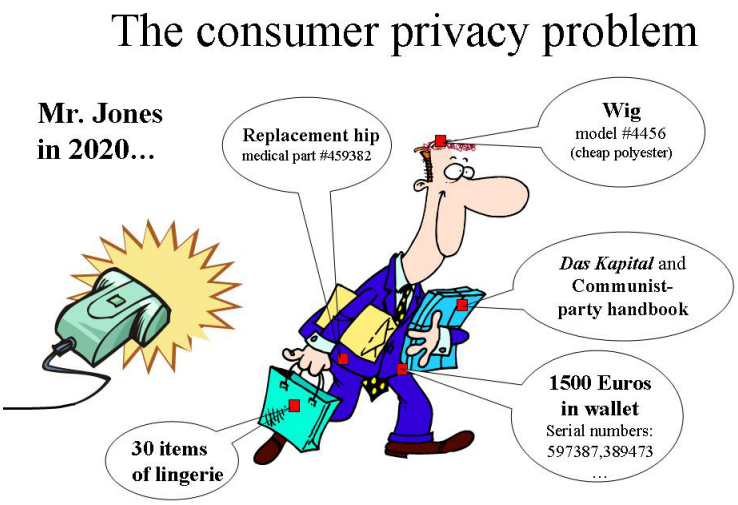

Fig. 1. An illustration of potential consumer privacy problems of RFID

corners – are commonplace worldwide. In at least one celebrated instance, a court subpoenaed the data gathered from such a transponder for use in a divorce case, undercutting the alibi of the defendant [81].

- **Euro banknotes**: As early as 2001 [85], the media reported plans by the European Central Bank to embed RFID tags in banknotes as an anti-counterfeiting measure. This project seems increasingly implausible given the attendant technical difficulties (not to mention the purported target date of 2005). It has served off and on, however, as a flashpoint for privacy concerns.[7]
- **Libraries:** Some libraries have implemented RFID systems to facilitate book check-out and inventory control and to reduce repetitive stress injuries in librarians. Concerns about monitoring of book selections, stimulated in part by the USA Patriot Act, have fueled privacy concerns around RFID [69].
- **Passports:** An international organization known as the International Civil Aviation Organization (ICAO) has promulgated guidelines for RFID-enabled passports and other travel documents [46], [57]. The United States has mandated the adoption of these standards by twenty-seven "Visa Waiver" countries as a condition of entry for their citizens. The mandate has seen delays due to its technical challenges and changes in its technical parameters, partly in response to lobbying by privacy advocates [91].[8]
- **Human implantation:** Few other RFID systems have inflamed the passions of privacy advocates like the VeriChip system [84]. VeriChip is a human-implantable RFID tag, much like the variety for house pets. One intended application is medical-record indexing; by scanning a patient's tag, a hospital can locate her medical record. Indeed, hospitals have begun experimentation with these devices [41]. Physical access control is another application in view for the VeriChip.

In the United States, several states have initiated RFID-privacy legislation, most notably California, where the state assembly considered (and rejected) bills in 2004 and 2005. Often overlooked in policy discussion is the REAL ID Act, recently passed by the U.S. legislature. This bill mandates the development of federal U.S. standards for drivers' licenses, and could stimulate wide deployment of RFID tags.

a) Read ranges: Tag read ranges are an important factor in discussions about privacy. Different operating frequencies for tags induce different ranges, thanks to their distinctive physical properties. Under ideal conditions, for instance, UHF tags have read ranges of over ten meters; for HF tags, the maximum effective read distance is just a couple of meters. Additionally, environmental conditions impact RFID efficacy. The proximity of radio-reflective materials, e.g., metals, and radio-absorbing materials, like liquids, as well as ambient radio noise, affect scanning distances. At least one manufacturer, Avery Dennison, has devised RFID tags specially for application to metal objects. Liquids – like beverages and liquid detergents – have hampered the scanning of UHF tags in industry RFID pilots. Protocol and hardware-design choices also affect read ranges.

The human body, consisting as it does primarily of liquid, impedes the scanning of UHF tags, a fact consequential to RFID privacy. If in the future you find yourself worried about clandestine scanning of the RFID tag in your sweater, the most effective countermeasure may be to wear it!

Sometimes RFID tags can foul systems by reason of excessively long range. In prototypes of automated supermarket-

[7]Rumors even circulated recently of RFID tags embedded in high-value U.S. notes, as demonstrated experimentally by the propensity of these notes to catch fire in microwave ovens.

[8]The U.S. State Department has recently indicated that: (1) U.S. passport covers will include metallic material to limit RF penetration, and thus prevent long-range scanning of closed passports; and (2) The U.S. may adopt a key ICAO privacy-protecting mechanism called Basic Access Control (BAC). Under BAC, passport contents are encrypted; optical scanning is required to obtain the decryption key from a passport.

checkout trials run by NCR Corporation, some (experimental) patrons found themselves paying for the groceries of the people behind them in line [90].

Certainly, the RFID industry will overcome many of these impediments, so it would be a mistake to extrapolate tag capabilities too far into the future. It is important, however, to keep the limitations of physics in mind.

For the study of RFID privacy in passive tags, it is more accurate to speak not of the read range of a tag, but of the read *ranges* of a tag. Loosely speaking, there are four different ranges to consider. In roughly increasing distance, they are:

- **Nominal read range:** RFID standards and product specifications generally indicate the read ranges at which they intend tags to operate. These ranges represent the maximum distances at which a normally operating reader, with an ordinary antenna and power output, can reliably scan tag data. ISO 14443, for example, specifies a nominal range of 10cm for contactless smartcards.
- **Rogue scanning range:** The range of a sensitive reader equipped with a powerful antenna – or antenna array – can exceed the nominal read range. High power output further amplifies read ranges. A rogue reader may even output power exceeding legal limits. For example, Kfir and Wool [65] suggest that a battery-powered reading device can potentially scan ISO 14443 tags at a range of as much as 50cm, i.e., five times the nominal range. The rogue scanning range is the maximum range at which a reader can power and read a tag.
- **Tag-to-reader eavesdropping range:** Read-range limitations for passive RFID result primarily from the requirement that the reader power the tag. Once a reader has powered a tag, a second reader can monitor resulting tag emissions without itself outputting a signal, i.e., it can eavesdrop. The maximum distance of such a second, eavesdropping reader may be larger than its rogue scanning range.
- **Reader-to-tag eavesdropping range:** In some RFID protocols, a reader transmits tag-specific information to the tag. Because readers transmit at much higher power than tags, they are subject to eavesdropping at much greater distances than tag-to-reader communications – perhaps even kilometers away.[9]

Also of concern in some special cases are *detection* ranges, that is, the distance at which an adversary can detect the presence of tags or readers. In military scenarios, for example, tag-detecting munitions or reader-seeking missiles pose a plausible threat.

Research question: There is scant published research on the feasible rogue-scanning and eavesdropping ranges for commercial RFID tags. Such research would benefit both RFID security analyses and public policy formulation. For example, rumors have circulated of RFID-enabled passports being vulnerable to eavesdropping at a distance of 30 feet [92] – perhaps a motivation for the recent U.S. State Department decision to consider encryption in such passports.

b) Privacy from cradle to grave: The importance of RFID privacy in military operations reinforces an oft-neglected point: Privacy is not just a consumer concern. The enhanced supply-chain visibility that makes RFID so attractive to industry can also, in another guise, betray competitive intelligence. Enemy forces monitoring or harvesting RFID communications in a military supply chain could learn about troop movements. In civilian applications, similar risks apply. For example, many retailers see item-level RFID tagging as a means to monitor stock levels on retail shelves, and avoid out-of-stock products. Individually tagged objects could also make it easier for competitors to learn about stock turnover rates; corporate spies could walk through shops surreptitiously scanning items [80]. Many of the privacy-enhancing techniques we discuss in this survey aim to protect consumers, or at least human bearers of RFID tags. It is useful to bear in mind the full scope of the privacy problem, though. In a recent survey article, Garkfinkel et al. [56] offer a taxonomy of threats across the different stages of a typical industrial supply chain.

2) Authentication: Privacy is a hobby-horse in media coverage of RFID. To some extent, it has overshadowed the equally significant problem of authentication.[10] Loosely speaking, RFID privacy concerns the problem of misbehaving readers harvesting information from well-behaving tags. RFID authentication, on the other hand, concerns the problem of well-behaving readers harvesting information from misbehaving tags, particularly counterfeit ones.

Asked what uses they foresee for RFID, ordinary U.S. consumers most frequently mention recovery of stolen goods [72]. In the popular imagination, RFID tags serve as a trustworthy label for the objects to which they are attached. Belief in tag authenticity will inevitably come to underpin many RFID applications. But it is in some measure an illusion.

Basic RFID tags are vulnerable to simple counterfeiting attacks. Scanning and replicating such tags requires little money or expertise. In [89], Jonathan Westhues, an undergraduate student, describes how he constructed what is effectively an RF tape-recorder. This device can read commercial proximity cards – even through walls – and simulate their signals to compromise building entry systems.

EPC tags will be vulnerable to similar attacks. An EPC, after all, is just a bitstring, copyable like any other. EPC tags offer no real access-control mechanisms. It is possible that "blank," i.e., fully field-programmable EPC tags, will be readily available on the market.[11] More importantly, elementary RFID simulation devices will be easy to come by or create. Such devices need not even resemble RFID tags in order to

[9]The EPC Class-1 Gen-2 standard exploits the gap between tag-to-reader and reader-to-tag eavesdropping ranges to achieve stronger data secrecy. When a reader is to transmit a sensitive value like a PIN P to a tag, the tag first transmits a random bit-string R to the reader. The reader transmits $P\,XOR\,R$, rather than P directly. Eavesdropping on the more vulnerable reader-to-tag channel alone, therefore, does not reveal P. A version of this idea first appeared in Weis et al. [87].

[10]In fact, RFID was first invented as a "friend-or-foe" authenticator for fighter planes during WWII.

[11]Field-programmable Class-1 Gen-2 EPC tags are available today [5]; they contain factory-programmed identifiers, however, in addition to user-programmable bits.

deceive RFID readers. As a result, EPC tags may carry no real guarantee of authenticity.

Yet plans are afoot for use of such tags as anti-counterfeiting devices. In the United States, the Food and Drug Administration (FDA) has called for the pharmaceutical industry to apply RFID tags to pallets and cases by 2007, with the aim of combatting counterfeit pharmaceuticals [35]. Two companies, Texas Instruments and VeriSign Inc., have proposed a "chain-of-custody" approach in support of this effort [50]. Their model involves digital signing of tag data to provide integrity assurance. Digital signatures do not confer cloning resistance to tags, however. They prevent *forging* of data, but not *copying* of data.

To be fair, even in the absence of resistance to tag cloning, unique numbering of objects can be a powerful anti-counterfeiting tool. As a simple illustration, consider the forgery of paintings, an epidemic in the art world. The Victorian painter Alma-Tadema presciently evaded this problem with a simple expedient. To avoid new "discoveries," he not only signed his paintings, but wrote unique, sequential serial numbers on them and cataloged them. For this reason (among others), spurious Alda-Tademas do not turn up on the art market as do, say, spurious Van Goghs. RFID tags can help combat counterfeiting on the same principle. If two RFID-tagged crates turn up in a warehouse with identical serial numbers, a problem has clearly arisen. Such detection does not require tag authentication. The FDA has noted that simply by furnishing better data on item pedigrees in supply chains, RFID tags can help identify sources of counterfeit goods.

Nonetheless, scenarios abound in which counterfeiters can exploit the vulnerability of RFID tags to cloning. Detection of duplicates ultimately requires consistent and centralized data collection; where this is lacking, physical and digital anti-counterfeiting mechanisms become more important. Here are a couple of examples (from [54]):

Example: EXCON Corp., a shipping company, is plotting to steal prescription medications that it has been entrusted with transporting. These medications sit in tamper-proof cases with attached RFID tags. Rather than trying to defeat the tamper-proofing of the cases, EXCON creates bogus medications and cases, and clones the associated EPC tags. It swaps in the bogus cases while it has custody of the real ones.[12]

Example: Dupyu Stores, an unscrupulous retailer, wishes to introduce bogus pharmaceuticals into its stock. After skimming the tags on legitimate pharmaceutical packages, Dupyu staff attach cloned tags to counterfeit, look-alike packages. Even in a system in which tag pedigrees are publicly accessible, this activity can still deceive consumers. Cloned tags will appear to have the same pedigree as legitimate tags, namely a history of legitimate manufacture and ultimate delivery to Dupyu. See [78] for elaboration on this scenario.

[12]This *modus operandi* is not an uncommon one. Shamos [76] reports that corrupt officials have altered vote tallies in elections in this manner. Rather than tampering with ballot-boxes, they created fake ballot-boxes and ballots offsite, applied counterfeited seals, and substituted these for legitimate ballot boxes in transit from polling stations.

Some RFID devices, such as the American Express ExpressPay^{TM} and the Mastercard PayPass^{TM} credit cards, and the active RFID tags that will secure shipping containers, can perform cryptographic operations. Bar reverse-engineering (and side-channel attacks), these devices offer very good resistance to cloning. As we explain below, however, some popular RFID devices perform cryptographic operations that are too weak to afford protection against determined attackers.

What about RFID as an anti-theft mechanism? Certainly, RFID tags can help prevent theft in retail shops. They will serve as an alternative to the Electronic Article Surveillance (EAS) tags that today detect stolen articles of clothing and other, relatively high-value items. RFID tags will not, however, prove very effective against determined thieves. A thief wishing to steal and repurpose an RFID-tagged object can disable its existing tag and even, with enough sophistication, even replace it with a tag carrying data of her choice.[13]

There is another aspect of authentication that is specific to RFID, namely authentication of *distance*. Thanks to the relatively short range of some RFID devices, users can authorize commercial transactions with RFID devices by placing them explicitly in proximity to readers. RFID-enabled payment tokens like credit cards work this way. As we shall see, however, tag distance is difficult to authenticate. Researchers have already demonstrated spoofing attacks.

Remarks: (1) The problems of RFID security and privacy are to some extent interdependent. Generally, cloning a tag requires scanning that violates the privacy of its holder.

(2) Denial of service is an important security issue in RFID systems, but not an issue specific to RFID. All wireless devices are subject to radio jamming. Similarly electromagnetic impulses can permanently damage radio devices (and in fact, any type of electronic hardware).

D. Attack models

In order to define the notions of "secure" and "private" for RFID tags in a rigorous way, we must first ask: "Secure" and "private" against what? The best answer is a formal model that characterizes the capabilities of potential adversaries. In cryptography, such a model usually takes the form of an "experiment," a program that intermediates communications between a model adversary, characterized as a probabilistic algorithm (or Turing machine), and a model runtime environment containing system components (often called *oracles*). In the model for an RFID system, for example, the adversary would have access to system components representing tags and readers.

In most cryptographic models, the adversary is assumed to have more-or-less unfettered access to system components in the runtime environment. In security models for the Internet, this makes sense: An adversary can more or less access any networked computing device at any time. A server, for instance, is always on-line, and responds freely to queries

[13]Thieves today commonly bypass EAS systems by hiding items in foil-lined bags that prevent the penetration of radio waves needed to read inventory tags.

from around the world. For RFID systems, however, around-the-clock access by adversaries to tags is usally too strong an assumption. In order to scan a tag, an adversary must have physical proximity to it – a sporadic event in most environments. It is important to adapt RFID security models to such realities. Because low-cost RFID tags cannot execute standard cryptographic functions, they cannot provide meaningful security in models that are too strong.

An important research challenge, therefore, is the formulation of weakened security models that accurately reflect real-world threats and real-world tag capabilities. Juels [52], for example, proposes a so-called "minimalist" security model and accompanying protocols for low-cost tags. This model supposes that an adversary only comes into scanning range of a tag on a periodic basis (and also that tags release their data at a limited rate). More precisely, the minimalist model assumes a cap on the number of times that an adversary can scan a given tag or try to spoof a valid reader; once this cap is reached, it is assumed that the tag interacts in private with a valid reader. The minimalist model might assume, for example, that an adversary can scan a target proximity card or try to gain unauthorized entrance to a building only ten times before the legitimate owner of the card achieves valid building entry outside the eavesdropping range of the adversary.

Juels and Weis [61] consider a formal security model that they call a "detection" model. The underlying assumption is that the adversary's goal is to clone a tag without being detected in the attempt. This is weaker than a "prevention" model, which assumes that an adversary cannot clone a tag at all, irrespective of whether its attempts are detected.

In the vein of more standard cryptographic modeling, Molnar, Soppera, and Wagner [68] propose a formal model for privacy in tags with full cryptographic capabilities – pseudo-random functions, in particular. Of special interest is the fact that their definitions include extensions for delegation of tag secrets. They propose a scheme in which a tag owner can disclose just a selected portion of the tag's identifiers. Avoine likewise proposes some strong cryptographic models for tag privacy. He analyzes several schemes with respect to these models [11], and identifies a number of formal weaknesses.[14]

Many cryptographic models of security fail to express important features of RFID systems. A simple cryptographic model, for example, captures the top-layer communication protocol between a tag and reader. At the lower layers are anti-collision protocols and other basic RF protocols. Avoine and Oechslin (AO) [13] importantly enumerate the security issues present at multiple communication layers in RFID systems. Among other issues, they highlight the risks of inadequate random-number generation in RFID tags. (As remarked in a footnote above, for example, the EPC Class-1 Gen-2 standard relies on randomness to protect sensitive data transmitted from the reader to the tag.) They observe the tracking threats that can arise from many competing RFID standards: A tag's underlying standard could serve as a short, identifying piece of information. AO also note potential risks at the physical level in RFID systems. For example, due to manufacturing variations, it is conceivable that an adversary could identify tags based on physical quirks in the signals they emit. Even the best cryptographic privacy-preserving protocol may be of little avail if an RFID tag has a distinct "radio fingerprint"!

There is, however, a flip side to the presence of multiple communication layers in tags. If tags have distinct radio fingerprints that are sufficiently difficult to reproduce in convincing form factors, then these fingerprints could help strengthen device authentication [22]. Moreover, as we shall discuss, some proposed RFID protocols actually exploit the presence of multiple protocol layers to *improve* tag privacy.

E. Nomenclature and organization

For the remainder of this survey, we classify RFID tags according to their computational resources. In section II, we consider *basic* tags, meaning those that cannot execute standard cryptographic operations like encryption, strong pseudo-random number generation, and hashing. We turn our attention in section III to what we call *symmetric-key* tags. This category includes tags that cost more than basic RFID tags, and can perform symmetric-key cryptographic operations.

Our categorization is a rough one, of course, as it neglects many other tag features and resources, like memory, communication speed, random-number generation, power, and so forth. It serves our purposes, however, in demarcating available security tools. We separately consider the problems of privacy and authentication protocols within each of the two categories.

Devices like RFID tags for shipping-container security, high-security contactless smartcards, and RFID-enabled passports[15] can often perform public-key operations. While our general points in this survey apply to such tags, we do not treat them explicitly. The majority of RFID tags – certainly passive ones – do not have public-key functionality. Moreover, existing cryptographic literature already offers much more abundant treatment of the problems of privacy and security for computationally powerful devices than for the weak devices that typify RFID.

II. Basic RFID Tags

Basic RFID tags, as we have defined them, lack the resources to perform true cryptographic operations. Low-cost tags, such as EPC tags, possess at most a couple of thousand gates, devoted mainly to basic operations [88]. Few gates – on the order of hundreds – remain for security functionality. It is tempting to dismiss this computational poverty as a temporary state of affairs, in the hope that Moore's Law will soon render inexpensive tags more computationally powerful. But pricing pressure is a strong countervailing force. RFID tags will come to be used in vast numbers; if and when they replace barcodes on individual items, they will contribute substantially to the cost of those items. Thus, given the choice between, say, a ten-cent RFID tag that can do cryptography, and a five-cent tag that cannot, it seems inevitable that most retailers

[14] Avoine identifies the scheme of Ohkubo, Suzuki, and Kinoshita (OSK) alone as possessing the formal properties he defines. As we note below, however, OSK is in fact vulnerable to privacy compromise.

[15] Most such passports will probably not perform public-key cryptography in their first generation. But the ICAO guidelines provide for public-key challenge-response protocols.

and manufacturers will plump for the five-cent tag. They will address security and privacy concerns using other, cheaper measures. (The barebones security features of the EPC Class-1 Gen-2 standard reinforce this point.)

The lack of cryptography in basic RFID is a big impediment to security design; cryptography, after all, is one of the lynchpins of data security. On the other hand, the lack of cryptography in basic tags poses intriguing research challenges. As we shall see, researchers have devised a farrago of lightweight technical approaches to the problems of privacy and authentication.

A. Privacy

Most privacy-protecting schemes for basic tags have focused on the consumer privacy problems discussed above. (Industrial privacy, i.e., data secrecy, is important too, but less frequently considered.) We now enumerate the various proposed approaches to the consumer privacy problem.

1) "Killing" and "Sleeping": EPC tags address consumer privacy with a simple and draconian provision: Tag "killing." When an EPC tag receives a "kill" command from a reader, it renders itself permanently inoperative. To prevent wanton deactivation of tags, this kill command is PIN protected. To kill a tag, a reader must also transmit a tag-specific PIN (32 bits long in the EPC Class-1 Gen-2 standard). As "dead tags tell no tales," killing is a highly effective privacy measure. It is envisioned that once RFID tags become prevalent on retail items, point-of-sale devices will kill the RFID tags on purchased items to protect consumer privacy. For example, after you roll your supermarket cart through an automated checkout kiosk and pay the resulting total, all of the associated RFID tags will be killed on the spot.

Removable RFID tags support a similar approach. Marks and Spencer, for example, include RFID tags on garments in their shops [20]. These RFID tags, however, reside in price tags, and are therefore easily removed and discarded.

Killing or discarding tags enforces consumer privacy effectively, but it *eliminates all of the post-purchase benefits of RFID for the consumer*. The receiptless item returns, smart appliances, aids for the elderly, and other beneficial systems described earlier in this article will not work with deactivated tags. And in some cases, such as libraries and rental shops, RFID tags cannot be killed because they must survive over the lifetime of the objects they track. For these reasons, it is imperative to look beyond killing for more balanced approaches to consumer privacy.[16]

Rather than killing tags at the point of sale, then, why not put them to "sleep," i.e., render them only temporarily inactive? This concept is simple, but would be difficult to manage in practice. Clearly, sleeping tags would confer no real privacy protection if any reader at all could "wake" them. Therefore, some form of access control would be needed for the waking of tags. This access control might take the form of tag specific PINs, much like those used for tag killing. To wake a sleeping tag, a reader could transmit this PIN.

The sticking point in such a system is that the consumer would have to manage the PINs for her tags. Tags could bear their PINs in printed form, but then the consumer would need to key in or optically scan PINs in order to use them. PINs could be transmitted to the mobile phones or smartcards of consumers – or even over the Internet to their home PCs. Consumers have enough difficulty just managing passwords today, however. The nitty-gritty management of PINs for RFID tags could prove much more difficult, as could the burden of managing sleep/wake patterns for individual tags.

A physical trigger, like the direct touch of a reader probe, might serve as an alternative means of waking tags [79]. Such approaches, however, would negate the very benefit of RFID, namely convenient wireless management.

2) The renaming approach: Even if the identifier emitted by an RFID tag has no intrinsic meaning, it can still enable tracking. For this reason, merely encrypting a tag identifier does not solve the problem of privacy. An encrypted identifier is itself just a meta-identifier. It is static, and therefore subject to tracking like any other serial number. To prevent RFID-tag tracking, it is necessary that tag identifiers be suppressed, or that they change over time.

a) Relabeling: Sarma, Weis, and Engels (SWE) propose the idea of effacing unique identifiers in tags at the point of sale [75] to address the tracking problem, but retaining product-type identifiers (traditional barcode data) for later use. Inoue and Yasuura (IY) [49] suggest that consumers be equipped to relabel tags with new identifiers, but that old tag identifiers remain subject to re-activation for later public uses, like recycling. As a physical mechanism for realizing the idea of SWE, IY also explore the idea of splitting product-type identifiers and unique identifiers across *two* RFID tags. By peeling off one of these two tags, a consumer can reduce the granularity of tag data. Karjoth and Moskowitz extend this idea [64], proposing ways that users can physically alter tags to limit their data emission and obtain physical confirmation of their changed state. As a remedy for clandestine scanning of library books, Good et al. [40] propose the idea of relabeling RFID tags with random identifiers on checkout.

The limitations of these approaches are clear. Effacement of unique identifiers does not eliminate the threat of clandestine inventorying. Nor does it quite eliminate the threat of tracking. Even if tags emit only product-type information, they may still be uniquely identifiable in constellations, i.e., fixed groups. Use of random identifiers in place of product codes addresses the problem of inventorying, but does not address the problem of tracking. To prevent tracking, identifiers must be refreshed on a frequent basis. This is precisely the idea in the approaches we now describe.

b) "Minimalist" cryptography: While high-powered devices like readers can relabel tags for privacy, tags can alternatively relabel themselves. Juels [52] proposes a "minimalist" system in which every tag contains a small collection of pseudonyms; it rotates these pseudonyms, releasing a different one on each reader query. An authorized reader can store the full pseudonym set for a tag in advance, and therefore identify

[16]There are some technical obstacles to effective killing of tags. For example, while a large retailer might have the infrastructure to accomplish it, what about mom-and-pop shops that do not have any RFID readers?

the tag consistently. An unauthorized reader, however, that is, one without knowledge of the full pseudonym set for a tag, is unable to correlate different appearances of the same tag. To protect against an adversarial reader harvesting all pseudonyms through rapid-fire interrogation, Juels proposes that tags "throttle" their data emissions, i.e., slow their responses when queried too quickly. As an enhancement to the basic system, valid readers can refresh tag pseudonyms.

The minimalist scheme can offer some resistance to corporate espionage, like clandestine scanning of product stocks in retail environments.

c) Re-encryption: Juels and Pappu (JP) [58] consider the special problem of consumer privacy-protection for RFID-enabled banknotes. Their scheme employs a public-key cryptosystem with a single key pair: A public key PK, and a private key SK held by an appropriate law enforcement agency. An RFID tag in the JP system carries a unique identifier S, the banknote serial number. S is encrypted under PK as a ciphertext C; the RFID tag emits C. Only the law enforcement agency, as possessor of the private key SK, can decrypt C and thus learn the serial number S.

To address the threat of tracking, JP propose that the ciphertext C be periodically *re-encrypted.* They envisage a system in which shops and banks possess re-encrypting readers programmed with PK. The algebraic properties of the El Gamal cryptosystem permit a ciphertext C to be transformed into a new, unlinkable ciphertext C' using the public key PK alone – and with no change to the underlying plaintext S. In order to prevent wanton re-encryption by, e.g., malicious passersby, JP propose that banknotes carry optical write-access keys; to re-encrypt a ciphertext, a reader must scan this key. (As we shall discuss, RFID-enabled passports may employ a similar mechanism.)

From several perspectives, like the need for re-encrypting readers, the JP system is very cumbersome. But it helpfully introduces the principle that cryptography can enhance RFID-tag privacy even when tags themselves cannot perform cryptographic operations.

In a critique in [10], Avoine explores limitations in the formal security model of JP. He observes, for instance, that eavesdropping on re-encrypting readers in the JP system can undermine privacy.

d) Universal re-encryption: The JP system relies on a single, universal key pair (SK, PK). While a single key pair might suffice for a unified monetary system, a general RFID system would certainly require multiple key pairs. Straightforward extension of JP to multiple key pairs $(SK_1, PK_1), (SK_2, PK_2), \ldots (SK_n, PK_n)$, however, would undermine system privacy. To re-encrypt a ciphertext C, it would be necessary to know under *which* public key PK_i it is encrypted, information that is potentially privacy-sensitive.

Golle et al. [39] address this limitation in JP by proposing a simple cryptosystem that permits re-encryption of a ciphertext *without knowledge of the corresponding public key*.[17] Their system, called *universal re-encryption*, involves an extension to the El Gamal cryptosystem that doubles ciphertext sizes.

The Golle et al. system has a serious security limitation: It does not preserve *integrity*. Instead of re-encrypting a ciphertext, an adversary can substitute an entirely new ciphertext, i.e., alter the underlying plaintext. Ateniese, Camenisch, and de Medeiros [9] furnish a solution to this problem predicated on bilinear pairings in elliptic curve cryptosystems. They propose a universal re-encryption scheme in which a ciphertext can be digitally signed by a central authority, thereby permitting anyone to verify the authenticity of the associated plaintext, namely the tag identifier. The Ateniese et al. scheme retains the full privacy-preserving features of ordinary universal re-encryption. It does not, however, defend against *swapping*, an attack in which an adversary exchanges two valid ciphertexts across RFID tags. Effective defense against swapping attacks remains an open research problem.

3) The proxying approach: Rather than relying on public RFID readers to enforce privacy protection, consumers might instead carry their own privacy-enforcing devices for RFID. As already noted, some mobile phones include RFID functionality. They might ultimately support privacy protection. Researchers have proposed several systems along these lines:

- Floerkemeier, Schneider, and Langheinrich [34] propose and briefly describe a prototype "Watchdog Tag," essentially an audit system for RFID privacy. The Watchdog Tag monitors ambient scanning of RFID tags, and collects information from readers, like their privacy policies.
- Rieback, Crispo, and Tanenbaum [73] and Juels, Syverson, and Bailey [60] propose very similar devices, respectively called an "RFID Guardian" and "RFID Enhancer Proxy" (REP). A Guardian (to use the first term) acts as a find of personal RFID firewall. It intermediates reader requests to tags; viewed another way, the Guardian selectively simulates tags under its control. As a high-powered device with substantive computing power, a Guardian can implement sophisticated privacy policies, and can use channels other than RFID (e.g., GPS or Internet connections) to supplement ambient data. For example, a Guardian might implement a policy like: "My tags should only be subject to scanning within 30m of my home (as determined by GPS), or in shops that compensate consumer tag-scanning with coupons for a 10% discount." The logistical questions of how a Guardian should acquire and release control of tags and their associated PINs or keys are tricky ones that merit further research.

4) Distance measurement: The barebones resources of basic RFID tags urge exploration of privacy schemes that shy away from expensive, high-level protocols and instead exploit lower protocol layers. Fishkin, Roy, and Jiang (FRJ) [31] demonstrate that the signal-to-noise ratio of the reader signal in an RFID system provides a rough metric of the distance between a reader and a tag. They postulate that with some additional, low-cost circuitry a tag might achieve rough measurement of the distance of an interrogating reader. FRJ propose that this distance serve as a metric for trust. A tag might, for example, release general information ("I am

[17] Golle et al. designed universal re-encryption for use in mix networks [19], a cryptographic, privacy-preserving tool for anonymous Web browsing, anonymous e-mail, elections, and so forth. They observe that a privacy-preserving RFID system involving relabeling is somewhat like a mix network.

attached to a bottle of water") when scanned at a distance, but release more specific information, like its unique identifier, only at close range.

5) Blocking: Juels, Rivest, and Szydlo (JRS) [59] propose a privacy-protecting scheme that they call *blocking*. Their scheme depends on the incorporation into tags of a modifiable bit called a *privacy bit*. A '0' privacy bit marks a tag as subject to unrestricted public scanning; a '1' bit marks a tag as "private." JRS refer to the space of identifiers with leading '1' bits as a *privacy zone*. A *blocker tag* is a special RFID tag that prevents unwanted scanning of tags mapped into the privacy zone.

Example: To illustrate how blocking might work in practice, consider a supermarket scenario. When first created, and at all times prior to purchase – in warehouses, on trucks, and on store shelves – tags have their privacy bits set to '0'. In other words, any reader may scan them. When a consumer purchases an RFID-tagged item, a point-of-sale device flips the privacy bit to a '1': It transfers the tag into the privacy zone. (This operation is much like the "kill" function in EPC tags, and may be similarly PIN-protected.) Once in the privacy zone, the tag enjoys the protection of the blocker. Supermarket bags might carry embedded blocker tags, to protect items from invasive scanning when shoppers leave the supermarket. When a shopper arrives home, she removes items from her shopping bags and puts them in the refrigerator. With no blocker tag inside, an RFID-enabled "smart" refrigerator can freely scan RFID-tagged items. The consumer gets privacy protection from the blocker when it is needed, but can still use RFID tags when desired!

How does a blocker actually prevent undesired scanning? It exploits the anti-collision protocol that RFID readers use to communicate with tags. This protocol is known as *singulation*. Singulation enables RFID readers to scan multiple tags simultaneously. To ensure that tag signals do not interfere with one another during the scanning process, the reader first ascertains what tags are present, and then addresses tags individually.

Blocking is of particular interest because, in exploiting singulation, it draws on the special operating characteristics of RFID. It is therefore worth giving a little detail.

One type of RFID singulation protocol is known as *tree-walking*. In this protocol, l-bit tag identifiers are treated as the leaves of a binary tree of depth l, labeled as follows. The root has a null label. For a node with binary label s, the left child has label $s \parallel$ '0'; the right child has has label $s \parallel$ '1'.

The reader effectively performs a depth first search of this tree to identify individual tags. Starting with the root of the tree, the reader interrogates all tags. Each tag responds with the first bit of its identifier. If the only response received by the reader is a '0' bit, then it concludes that all tag identifiers lie in the left half of the tree; in this case the reader recurses on the left half of the tree. Conversely, a concordant response of '1' causes the reader to recurse on the right half of the tree. If the tag signals collide, that is, some tags emit '0' bits and others emit '1' bits, then the reader recurses on both halves of the tree. The reader continues recursing in this manner on sub-trees; it restricts its interrogation to tags in the current sub-tree. This procedure eventually yields the leaves – and thus the l-bit identifiers – of responding tags.

A blocker impedes RFID scanning by simulating collisions in the singulation tree. For example, a naïvely designed blocker could block scanning of *all* tags simply by emitting both a '0' bit and '1' bit in response to every reader interrogation, and forcing the reader to traverse the whole tree. Given that a typical tag identifier is, say, 96 bits in length, such a tree has many, many billions of leaves. So such a blocker would always cause a reader to stall!

As we have explained, the aim of the blocker is not wanton disruption of tag scanning. Rather, the scheme is *selective*. Blocking here relies on designation of the *leading bit* of a tag identifier as the privacy bit. The blocker only disrupts the scanning process when a reader attempts to scan tags in the privacy zone, i.e., in the right half of the singulation tree. The blocker does not interfere with the normal scanning of tags with '0' privacy bits, i.e., those outside the privacy zone. Figure 2 shows how blocking might work in conjunction with tree-walking in the supermarket scenario we have sketched.

A blocker tag can be manufactured almost as cheaply as an ordinary tag. Blocking, moreover, may be adapted for use with ALOHA singulation protocols (the more common type). To prevent undesired reader stalling, JRS also propose mechanisms whereby a blocker tag can be "polite," that is, it can inform readers of its presence so that they do not attempt to scan the privacy zone.

Of course, the blocker concept has limitations. Given the unreliable transmission of RFID tags, even well-positioned blocker tags might fail. Readers might evolve, moreover, that can exploit characteristics like signal strength to filter blocker signals [74]. On the other hand, improvements and variations are possible: A blocker might be implemented as an active device in a mobile phone, for example. Given the notoriously unpredictable behavior of RFID devices in the real world, both attacks and defenses merit careful empirical evaluation.

a) Soft blocking: Juels and Brainard (JB) [55] propose a blocking variant that they call *soft* blocking. Rather than interfering with singulation, a soft blocker tag merely emits a compact policy statement, e.g., "Do not scan tags whose privacy bit is on." (Viewed another way, a soft blocker tag is always "polite.") JB propose that readers interpret such policies in software.[18] Soft blocking relies on auditing of reader configurations to enforce compliance. As reader emissions are subject to ambient monitoring, it is possible to construct an audit device that detects readers that violate tag policies. While lacking some of the technical assurances of JRS blocking, soft blocking has certain advantages. For example, while JRS blocking is "opt-out,", soft blocking supports "opt-in" policies.

One scheme proposed by JB involves no explicit blocker tag at all, but relies on audit alone. This very simple approach

[18]RSA Laboratories demonstrated a conceptual soft blocking system at the RSA Conference in February 2004. They set up a mock pharmacy (called the R$_X$A Pharmacy), in which the bottles containing medications (jellybeans) bore RFID tags, and pharmacy bags carried soft blocker tags. This system was very simple. Both inventory tags and blockers were ordinary RFID tags. The system stored tags' privacy bits in software.

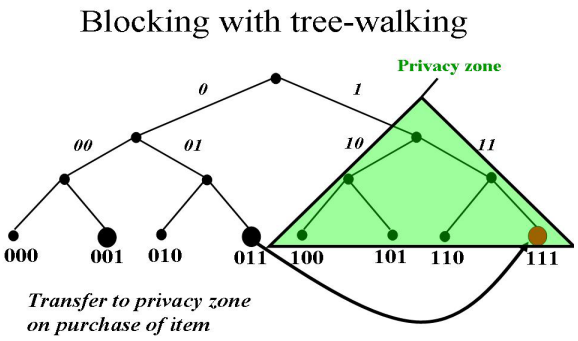

Fig. 2. Illustration of how a blocker tag might work

has obvious technical deficiencies, but is perhaps the most practical form of blocking!

b) Trusted computing: Molnar, Soppera, and Wagner (MSW) [67] briefly describe an alternative approach to enforcement of privacy policies, such as those that rely on "privacy bits." They describe how readers equipped with trusted platform modules (TPMs) can enforce tag privacy policies internally. Such readers can generate externally verifiable attestations as to their configuration in accordance with these policies. MSW note that the commercially available ThingMagic Mercury 4 reader includes an XScale 2 processor with a TPM. While the MSW approach does not of course address the problem of rogue readers, it can facilitate or complement other forms of privacy protection.

6) Legislation: Even at this early stage, RFID privacy has attracted the keen attention of policymakers and legislators. As noted above, RFID-privacy bills have arisen in several states in the U.S., although none has seen enactment at the time of writing. The U.S. Federal Trade Commission has issued a report that addresses the impact of RFID on consumers, with an emphasis on privacy [21], but has not yet expressed an intention to issue regulations. EPCglobal Inc. has published guidelines for its members on EPC privacy for consumer products [26]. These guidelines emphasize consumer education about the presence and functioning of EPC tags, and the provision of means of disablement or removal.

Good public policies for RFID are likely to prove hard to craft, because RFID tags, having essentially no form of access control, offer no obvious points of liability for information leakage. A healthcare provider, for instance, can issue a privacy policy describing the ways in which it grants or denies access to its customer databases; when a database is compromised, the target of liability is (more or less) clear. In contrast, a retailer cannot offer any guarantees about the tracking of RFID tags on items that leave its premises. RFID privacy is only fully meaningful if *all* entities with RFID readers subscribe to it – or if consumers do not carry live RFID tags. (It is of note that the EPCglobal guidelines do not really treat the problem of privacy in live RFID tags.)

Given the inevitable deficiencies of technology or policy acting in isolation, the cooperation of technologists and legislators seems essential to good RFID privacy enforcement. Some technologists have already turned their attention to RFID policy and legislation issues. Garfinkel published a five-point "RFID Bill of Rights" [36] with broad, pithy provisions for consumer notice and choice. Floerkemeier et al. [34] have considered ways of enforcing RFID compliance with the Fair Information Practices (FIP) of the Organization of Economic Cooperation and Development (OECD); their work aims particularly at informing consumers about the existence and purposes of RFID data collection.

B. Authentication

We have discussed the ways in which basic RFID tags can combat counterfeiting by offering enhanced supply-chain visibility. As we have noted, however, outside an environment of truly seamless information, counterfeiting of RFID tags can facilitate counterfeiting of consumer goods. Yet effective authentication of basic RFID tags – the type we consider here – is very difficult.

EPC tags of the Class-1 Gen-2 type have no explicit anti-counterfeiting features whatsoever. In principle, an attacker can simply skim the EPC from a target tag and program it into another, counterfeit tag – or simulate the target tag in another type of wireless device.

Juels [54] shows a simple way to repurpose the kill function in EPC tags to achieve limited counterfeiting resistance. Normally, the kill PIN authenticates a reader to a tag in order to authorize the deactivation of the tag. Instead, this authentication can be reversed, and the kill PIN can instead serve to authenticate the tag to the reader. The basic protocol proposed in [54] co-opts the ability of tags to distinguish between valid and spurious kill PINs.

In [53], Juels proposes an RFID protocol called *yoking*. It provides cryptographic proof that two tags have been scanned simultaneously – and evidence (although not proof) that the tags were scanned in physical proximity to one another. A yoking protocol might, for example, allow a pharmacy to demonstrate to a government agency that it scanned an RFID-tagged medication bottle at the same time that it scanned an RFID-tagged booklet of contraindications – and thus that it furnished legally required information to consumers. One variant of this protocol is suitable for basic tags in that it

requires virtually no computation, but it does require several hundred bits of storage per invocation.

Even if tags themselves do not have on-board anti-counterfeiting features, they can support physical anti-counterfeiting mechanisms. For example, physical one-way functions (POWFs) [71] are small plastic objects with reflective inclusions such as tiny glass beads. Laser scanning of POWFs reveals unique, random speckle-patterns that may be translated into bit-strings; a POWF as small as 1cm^2 can contain as many as 10^{12} static, random bits (effectively ROM). A POWF has two important anti-cloning properties: (1) Physical tampering destroys the information contained in a POWF, and (2) It is difficult to manufacture a POWF that emits a predetermined set of bits when scanned. Thus a POWF can help enforce unique identification of an object or container to which it is attached. While POWF data can be stored anywhere, an RFID tag may serve as a particularly useful carrier for POWF data. POWFs are just an attractive research concept at present. Many forms of packaging today contain special, proprietary (and secret) dyes and other physical markers of uniqueness. Basic RFID tags can equally well serve as carriers for their anti-counterfeiting data.

C. The problem of PIN distribution

As we have explained, both privacy and authentication features in basic tags can depend on tag-specific PINs. The kill function for Class-1 Gen-2 EPC-standard tags requires a PIN. There is also an option in the EPC standard for PIN-controlled write-access in tags. PIN distribution will almost certainly pose a major problem in the field, from the standpoints of both security and pure logistics. Once item-level tagging becomes prevalent, it will be necessary to provision point-of-sale terminals securely with the PINs for the RFID tags they are to kill. This problem, the perennial cryptographic one of *key management* in another guise, has seen only brief treatment in the RFID literature. Molnar, Wagner, and Soppera propose tree-based PIN distributions schemes akin to their ideas for privacy enforcement and delegation of secrets, which we summarize below; Juels [54] proposes an extended tag-authentication scheme in which readers prove their legitimacy through interaction with valid tags. The problem of secure PIN distribution merits much more investigation.

III. Symmetric-key tags

Let us now turn our attention to the class of RFID tags with richer security capabilities, those capable of computing *symmetric-key* (cryptographic one-way) functions.

For brevity, we use loose notation in this section, and assume very basic familiarity with cryptographic primitives. Recall that a cryptographic hash function h has the special property that for a random bitstring M of sufficient length, it is infeasible to compute M from knowledge of the hashed value $h(M)$ alone. Hashing involves no secret key (and is therefore only loosely called a symmetric-key function). In contrast, *symmetric-key encryption*, sometimes called *secret-key encryption*, relies upon a secret key k. With this key, a message or *plaintext* M can be encrypted as a *ciphertext* $C = e_k[M]$. Only with knowledge of k is it feasible to decrypt C and recover M.

In our discussions here we assume a centralized system, i.e., one in which readers are continuously on-line. We denote the number of tags in a system by n, and let T_i for $1 \leq i \leq n$ denote the identifier for the i^{th} tag in the system. We informally refer to this tag as T_i. We suppose that tag T_i contains in memory a distinct, random, and secret key k_i.

A. Cloning

In principle, symmetric-key cryptography can go far toward eliminating the problem of tag cloning. With a simple challenge-response protocol like the following, a tag T_i can authenticate itself to a reader with which it shares the key k_i:

1) The tag identifies itself by transmitting the value T_i.
2) The reader generates a random bitstring R (often called a *nonce*) and transmits it to the tag.
3) The tag computes $H = h(k_i, R)$, and transmits H.
4) The reader verifies that $H = h(k_i, R)$.

Alternatively, and more or less equivalently, the tag can return $e_{k_i}[R]$. (Note that for the moment here, we set aside privacy considerations, and suppose that tags identify themselves.)

Provided that the hash function h (or encryption function e) is well constructed and appropriately deployed, it is infeasible for an attacker to simulate T_i successfully without physically attacking the tag.

In practice, however, resource constraints in commercial RFID tags sometimes lead to the deployment of weak cryptographic primitives, and thus vulnerable authentication protocols, as our discussion now illustrates.

1) The Digital Signature Transponder (DST): Texas Instruments (TI) manufactures a low-frequency, cryptographically-enabled RFID device called a Digital Signature Transponder (DST). The DST serves as a theft-deterrent in millions of automobiles – many late-model Ford and Toyota vehicles, for example. Present as a tiny, concealed chip in the ignition key of the driver, the DST authenticates the key to a reader near the key slot as a precondition for starting the engine. (The metal portion of the ignition key in isolation will not start the vehicle.) The DST is also present in SpeedPass^{TM} wireless payment devices, used by millions of customers primarily at ExxonMobil petrol stations in North America.

The DST executes a simple challenge-response protocol essentially like that described above. It contains a secret key k_i. In response to a random challenge R from a reader, the DST executes an encryption function e and outputs $C = e_{k_i}[R]$. The challenge R is 40 bits in length, the response C is 24 bits in length. Of particular note is the length of the secret key k_i. It is only 40 bits. As cryptographers know, this is quite short by today's standards: A key of this length is vulnerable to brute-force computational attack. Perhaps recognizing the inadequate key-length of the DST, Texas Instruments has not published details of the encryption algorithm e, instead preferring the approach of "security through obscurity."

In late 2004, a team of researchers at Johns Hopkins University and RSA Laboratories set out to demonstrate the security vulnerability of the DST [17]. They succeeded in fully

cloning DST tokens, by which we mean cracking their keys and exactly simulating them in separate devices. Their effort involved three stages:

1) **Reverse-engineering:** The researchers determined the unpublished encryption algorithm e in the DST. They relied on three things: (1) A TI DST reader, available in an evaluation kit; (2) Some blank DSTs, meaning tokens with programmable secret keys; and (3) A loose schematic of the encryption algorithm e published on the Internet by a scientist at TI [63]. With the reader and blank tags, the researchers were able to determine the output value $e_k[R]$ for any key k and challenge R. Based on the published schematic, they carefully formulated and tested sequences of key/challenge pairs to derive operational details of the encryption algorithm e. They did not physically probe the DST in any way.
2) **Key cracking:** Having determined e, the researchers implemented a hardware "cracker" costing several thousand dollars. This cracker consisted of an array of 16 FPGA boards. Given two input-output pairs (R_1, C_1) and (R_2, C_2) skimmed from a target DST, it proved capable of recovering a secret key in about thirty minutes on average. The cracker operated by brute force, meaning that it searched the full space of 2^{40} possible DST keys.[19]
3) **Simulation:** The researchers constructed a programmable radio device that exactly simulates the output of any target DST.[20]

The JHU-RSA team demonstrated their attack in the field. Simulating the DST present in an ignition key (and using a copy of the metal portion), they "stole" their own car. They also purchased gasoline at a service station using a clone of their own SpeedPass^{TM} token!

As this work demonstrates, all that an attacker requires to clone a DST is a pair of challenge/response values. An attacker could, for example, set up a reader in a crowded area, such as a subway station, and harvest challenge/response pairs from DST in the pockets of passersby. Alternatively, the attacker could eavesdrop (at longer range) on the communications between a DST and valid reader.

2) Reverse-engineering and side channels: Most RFID tags are and may continue to be too inexpensive to include tamper-resistance mechanisms. Physically invasive attacks are mainly of concern for RFID tags that serve as authenticators, and of greatest concern when such attacks leave no physical traces or permit the construction of perfect physical replicas of target devices. For example, a reverse-engineered RFID-based payment device might be cloned to effect fraudulent payments (on-line controls serving as an important but limited countermeasure). Reverse-engineering of smartcards is an increasingly well studied area; even hardened devices have yielded to successful probing using modest resources [8].

[19]An attacker scanning DSTs with a rogue reader could instead perform this key search using a Hellman table, as described below. This would reduce the key search effort to about two minutes on an ordinary PC.

[20]A DST cannot simply be programmed with a recovered key, as it outputs a static device identifier along with its cryptographic output.

Most interesting and potentially serious in the case of RFID are attacks involving *side channels*, meaning sources of information beyond the mere bit-values of protocol flows. RFID tags, far more than contact devices, leak information *over the air*, opening the prospect of wireless, non-invasive side-channel attacks. The two predominant forms of side-channel analysis studied by the security community are *timing attacks*, which extract information based on variations in the rate of computation of a target device, and *power analysis* attacks, which exploit measurable variations in power consumption. *Power interruption* and *fault induction* are related, more active forms of attack. Over-the-air timing attacks against RFID tags would appear to be eminently viable; their efficacy is an open research question. Similarly, measurements of electromagnetic emanations could pave the way for over-the-air power-analysis attacks. Carluccio, Lemke, and Paar have initiated early work in this area [18].

3) Relay attacks: No matter how well designed the cryptographic protocols in an RFID device, and no matter how strong the cryptographic primitives, one threat is ineluctable: *relay* or *man-in-the-middle* attacks.[21] These attacks can bypass any cryptographic protocol, even public-key ones. Given the limited read range of tags, many security applications of RFID involve a presumption of physical proximity between tags and readers. Basic security premises fail, for instance, if a proximity card can be caused to open a door or an RFID-based credit card can effect payment from a kilometer away.

A relay attack undermines proximity assumptions in an RFID system. To use the colorful nomenclature of Kfir and Wool [65], this type of attack involves two communicating devices, a *leech* and a *ghost*. The attacker situates the leech physically close to the target RFID device and the ghost close to a target reader. Intercommunication between the leech and ghost creates the appearance of physical proximity between the target RFID device and a target reader when they may in fact lie very far apart.

Kfir and Wool (KW) modeled the operational distance of a leech and ghost pair in an ISO 14443 system, for which the nominal read range is 10cm. They considered simple leech and ghost designs based on NFC devices. As noted above, some mobile phones are now NFC-enabled.

KW concluded that a leech can operate at a distance of at least 50cm from a target RFID device, while the ghost can operate at a distance of up to 50m from a target reader! The distance between the leech and ghost can in principle be almost unlimited – certainly on the order of kilometers. Recently, Hancke [43] actually implemented a relay attack against an ISO 14443A contactless smartcard, and achieved a 50m distance between the leech and ghost.

Simple countermeasures to RFID relay attacks exist, like pushbuttons or removable Faraday cages that confirm user intentionality, or user input of PINs into RFID readers. But these are inconvenient. RF shielding on readers can in principle limit the directionality of radio signals, and therefore the potential position of a ghost.

[21]*Wormhole* attacks, as explored in the *ad hoc* networking community, similarly involve deception around physical distance, often with the aim of tampering with routing tables.

Timing measurements are an oft contemplated but little studied countermeasure in the research community. A relay system induces a read time than simple device interrogation; Hancke has observed this in practice [43]. Hancke and Kuhn [42] have designed a protocol that bounds the distance between a reader and RF device, but requires special protocol design and use of ultra-wide-band communication. As mentioned above, Fishkin et al. have described a scheme in which a tag can estimate its distance from a reader [31]. This approach could limit the margin of maneuver for a leech. Another possible countermeasure to relay attacks is tag localization, i.e., loose determination of the position of the tag. Localization is technically challenging, however [33].

Ultimately, sensitive RF transactions may benefit from the aid of portable devices like mobile phones, which are capable of more sophisticated countermeasures than tags. A phone equipped with a GPS receiver, for example, can digitally sign its most recently observed location. In the meantime, relay attacks constitute a very important research area.

Research question: The RFID industry continues to manufacture cryptographically weak devices. Some tags employ strong cryptography, like the Philips Mifare^{TM} DESfire, which uses 3DES; there are weaker variants of this very popular product line, however. Many proximity cards and toll payment transponders use mere static identifiers, as does the VeriChip. Exploration of the vulnerabilities of these devices is an important research direction. The resulting lessons should benefit both the industry and consumers.

B. Privacy

At the heart of the privacy problem for symmetric-key-enabled RFID tags lies the challenge of *key management.*

As we have seen, cryptographically secure authentication (or even mere identification) of an RFID tag T_i relies on a symmetric key k_i shared between a tag and reader. The fact that this key is tag-specific leads to a paradox. Suppose that a tag identifies itself *prior* to authenticating an interrogating reader or without authenticating an interrogating reader at all, i.e., the tag emits its identifier T_i more or less promiscuously. Privacy, then, is unachievable, since any reader can learn the identity of the tag. On the other hand, a tag cannot easily identify itself *after* the reader authenticates to the tag. If the reader does not know which tag it is interrogating, it cannot determine which key k_i to use in protocol interactions with the tag!

There is a straightforward but heavyweight solution to this privacy conundrum. A reader can identify tags by means of *key search.* In loose schematic terms, the procedure is as follows.

Let $f_{k_i}[M]$ denote a keyed one-way function – either $h(k_i, M)$ or $e_{k_i}[M]$, for example. Let P be an input value, a random session-specific value, that is, a *nonce*, or a static bit-string. (Different proposed schemes involve different choices for P.) Reader identification of a tag encompasses the following two steps, often at the heart of a larger protocol:

1) Tag T_i emits $E = f_{k_{T_i}}[P]$. (For example, T_i might encrypt a nonce P under the key k_{T_i}.)
2) On receiving E from a tag, the reader searches the space of all tag keys $K = \{k_{T_j}\}_j$ for a key such that $f_{k_{T_j}}[P] = E$. (For example, the reader might try to decrypt E under every key in K until it obtains P.)

If the scheme is correctly parameterized, the reader will find only one key k_{T_j} that successfully yields E. This key uniquely identifies the tag as T_j. To ensure the privacy of the tag, clearly the value E emitted by the tag must vary from session to session, otherwise E is a static identifier. Thus, either k_{T_i} or P (or both) must vary over time; different schemes involve different ways of varying these values, as we shall see.

In our discussion of the literature, we focus on techniques for tag identification, rather than authentication. Of course, the two processes are interrelated. In a general symmetric-key system, however, tag identification is a pre-condition for tag authentication. As we have explained, a reader must determine which key k_i it shares with a tag in order to perform any mutually intelligible cryptographic operation.

C. The literature

Weis, Sarma, Rivest, and Engels [87] (WSRE) first advanced the general approach of key search for RFID-tag identification. Among other variants, they propose a basic scheme in which a tag emits $E = (h(k_i, R), R)$, where R is a random nonce generated by the tag. To identify a tag, a reader computes $h(k_j, R)$ for all keys in K until it finds k_i. (WSRE also describe how a reader, having identified a tag, can cryptographically "unlock" it so that it releases private data.)

WSRE noted the major sticking point with the key-search approach: The computational cost for the reader is linear in n. In practice, if the set of tags $\{T_i\}_{i=1}^n$ is large, then key search can be prohibitively costly. Subsequent literature in this area has largely aimed to reduce the cost of key search. Every such proposal, however, involves some kind of tradeoff, either the addition of a new architectural requirement or the suppression of a security or privacy property.

a) Tree approach: Molnar and Wagner (MW) [69] propose a scheme in which a tag contains not one symmetric key, but multiple keys. These keys are arranged in a hierarchical structure defined by a tree S. Every node in the tree, except the root, has a unique associated key. Each tag is assigned to a unique leaf; it contains the keys defined by the path from the root of S to this leaf. If the tree has depth d and branching degree b, then each tag contains d keys, and the scheme can accommodate up to d^b tags in total.

A tag in the MW scheme authenticates to a reader using each of its d secret keys – either in serial or in parallel – in order of their depth in the tree. The tag effectively runs several rounds of the two-step identification protocol sketched above, increasing the granularity of the key in each round, i.e., narrowing the set of tags to be searched. The result is a striking improvement in efficiency. A reader can identify a tag by means of a depth-first search of S, and therefore needs to search through at most db keys. In contrast, a brute-force key search, as we have explained above, would require that a reader search the space of all $n = d^b$ tag keys.

There is a price to be paid for this efficiency gain. The tree structure creates an overlap among the sets of keys in

tags. Compromise of the secrets in one tag, therefore, results in compromise of secrets in other tags. Compromise of a fraction of the tags in the system can lead to substantive privacy infringements, as analyzed in [12].

Molnar, Soppera, and Wagner (MSW) [68] explore ways in which the sub-trees in the MW scheme may be associated with individual tags. They introduce a new idea, that of *delegation* of the ability to identify tags. By transferring sub-tree data in the MSW system, the owner of a tag can enable another party to identify the tag over a limited window of time (i.e., number of read operations). Such tag delegation can be useful in a couple of ways:

1) A tag holder can transfer ownership of an RFID tag to another party while ensuring that past tag history remains private.
2) A centralized authority with full tag information can provision readers to scan particular tags over limited windows of time. Readers can thus download temporary scanning privileges, a useful feature in systems with intermittent connectivity.

b) Synchronization approach: Another approach to avoiding brute-force key search is for a reader to maintain synchronized state with tags.

Suppose that every tag T_i maintains a counter $P = c_i$ that is incremented with each reader query. On interrogation, the tag outputs $E = f_{k_i}[c_i]$. Provided that a valid reader knows the approximate current value of the counters of tags in the system, it can store a searchable table of tag output values. Suppose that for every tag T_i the reader maintains a counter value c'_i that does not lag behind c_i by more than d timesteps. Then if the reader maintains the output values $f_{k_i}[c'_i], f_{k_i}[c'_i + 1], \ldots, f_{k_i}[c'_i + d]$ in a table, it can at any time look up the output E of tag T_i. With a table of size dn, the reader can look up the output of any tag in the system.

The literature explores several variants of this principle:

- Ohkubo, Suzuki, and Kinoshita (OSK) [70] propose the conceptually simplest approach: They simply assume that a tag never emits more than m values over its lifetime. Therefore, a reader can construct a one-time lookup table on the first m outputs for all tags, i.e., on the values $\{f_{k_i}[j]\}_{i \in \{1 \ldots n\}, j \in \{1 \ldots m\}}$. (OSK do not investigate the issue of tag authentication, although a challenge-response protocol could be layered straightforwardly onto their basic system.)
- Henrici and Müller [45] propose to resolve the synchronization problem by having a tag emit the number of timesteps Δc since the last successful authentication with the reader. This approach, however, exposes a tag to adversarial tracking. By querying a tag repeatedly, for example, an attacker can inflate Δc artificially, to the point where Δc is distinctly large and therefore recognizable to the adversary. Avoine identifies this problem in [11].
- Juels [52] proposes a scheme that effectively caps the degree of desynchronization with a reader; it is a cryptographic variant on the "minimalist" approach described above. Rather than incrementing its counter indefinitely, a tag loops through a bounded sequence of d output values, $f_{k_i}[z], f_{k_i}[z + 1], \ldots, f_{k_i}[z + d - 1]$. Only upon successful mutual authentication with the reader does the tag advance to the next sequence of d output values. The reader maintains a dynamic lookup table of size $O(dn)$ for all tags. (Like the basic minimalist scheme, this one assumes "throttling" of tag data.)
- Dimitriou [24] proposes a scheme that eliminates the issue of desynchronization entirely. Here a tag alters its counter value, and thus its output value, only upon successful mutual authentication with a reader. This approach renders key search highly practical, and also helps defend against denial-of-service attacks. The drawback, of course, is that between identification sessions with a legitimate reader, the output value of a tag is static. Tags are therefore subject to tracking during such intervals of time. As Dimitriou notes, however, the resulting privacy properties may be sufficient from a practical standpoint.

c) Time-space tradeoff approach: In early work, Hellman [44] studied the problem of *breaking* symmetric keys. He considered the resource requirements of an attacker seeking to recover secret key k from a ciphertext $C = e_{k[M]}$ on a predetermined message M. The attacker might simply perform a brute-force key search, and invest computational effort $O(n)$, where n is the size of the total key space. Or she might pre-compute and store a table of size $O(n)$ consisting of $C = \{C_i = e_{k_i}[M]\}_{k_i \in K}$, and simply look up C in the table. Hellman demonstrated an intermediate choice. An attacker can pre-compute a table of size $O(N^{2/3})$ – commonly referred to as a Hellman table – that permits successful key search with computational effort only $O(N^{2/3})$. Loosely speaking, the idea is to group sequences of ciphertexts in C into deterministically traversable chains of size $O(N^{2/3})$. Within the Hellman table are stored only the first and last elements of these chains. Starting with a ciphertext C, the attacker can traverse the induced chain until she locates the last element. By consulting the Hellman table, she can then determine the first element in the chain; on traversing the chain from this point, she can determine k_i.

Avoine, Dysli, and Oechslin (ADO) [12], [14] observe that the problem of symmetric-key search for readers in privacy-preserving RFID systems is nearly identical with that of breaking keys. For a reader to determine which tag it is communicating with, the reader can "crack" the ciphertext C_i to determine k_i and thus T_i. ADO apply a variant of the Hellman technique to the OSK system, yielding a scheme with considerably more practical lookup costs. Because of the need to pre-compute the Hellman table, the ADO variant, like the original OSK scheme, searches for keys over a pre-determined window of timesteps.

Remarks:

1) **Vulnerability in OSK and ADO:** A simple, practical attack against the privacy of the OSK and ADO schemes has been recently noted in [62]. Both schemes involve key search across a window of timesteps of predetermined size m. By probing the window boundary, i.e., exploiting the fact that the reader cannot identify tags with counter values greater than m, an attacker can

learn a tag's exact current counter value. Consider a tag T_i with current counter value c_i. The attacker queries the tag m times, obtaining outputs $E_1 = E_{c_i}$, $E_2 = E_{c_i+1}$, $\ldots E_m = E_{c_i+m}$. Then the attacker submits $E_m, E_{m-1}, \ldots, E_1$ to the reader in that order, until the reader accepts a value E_j. The attacker concludes that $c_i = j$ at the time of attack. For practical system parameterizations, e.g., $m = 128$ as proposed by ADO, this attack is problematic. (Other systems, e.g., MSW, are similarly vulnerable in theory [68], but practical parameterizations render such attacks infeasible.)

2) **Forward secrecy:** A main contribution of OSK is a technique for achieving forward secrecy in tags. This property means that if an attacker compromises a tag, i.e., learns its current state and its key, she is nonetheless unable to identify the previous outputs of the tag. The technique is simple: The tag and reader refresh k_i in every timestep by hashing it. Thus, in OSK, it is infeasible to compute previous keys and outputs from the current key. Dimitriou uses the same approach in his later scheme [24].

D. Implementing symmetric-key primitives

Just as important as the effective *use* of symmetric-key cryptographic primitives for privacy or authentication is the efficient design and *implementation* of these primitives. A few papers explore primitives geared specifically toward the very tightly constrained environments of RFID tags:

- Vajda and Buttyán [83] propose a medley of lightweight cryptographic primitives for RFID-tag authentication. (They do not provide formal analysis, however.)
- Feldhofer, Dominikus, and Wolkerstorfer [28] propose a lightweight hardware implementation of a symmetric-key cipher, namely a 128-bit version of the AES (Advanced Encryption Standard). Their design requires just over 3500 gate equivalents – considerably more than appropriate for basic RFID tags, but suitable for higher-cost RFID tags.
- Juels and Weis [61], [86] propose a lightweight authentication protocol called HB^+ that has security reducible to a problem called *Learning Parity with Noise*. To implement HB^+, tags need only generate random bits and compute binary dot products. The key lengths required for good security are as yet unknown, however, and the security model is limited [38].

ECRYPT (the European Network for Excellence in Cryptology) is currently evaluating 21 candidate stream ciphers [4], some of them geared toward resource-constrained hardware platforms. Successful candidates could prove suitable for RFID tags.

Research questions: The problems of key management and implementation of primitives are extremely important ones in this area. Other valuable research problems remain, however, of which we mention just a couple:

- Is it possible to construct a fully privacy-preserving, symmetric-key RFID identification scheme in which the reader performs computation $o(n)$, i.e., sub-linear in the number of tags? (Recall that use of Hellman tables undermines privacy.) Alternatively, is it possible to prove that such a scheme is impossible without the use of public-key cryptography?
- Nearly all of the schemes we have described presume a centralized model, namely that readers have continuous access to a centralized database. This feature provides resistance to replay and desynchronization attacks. What is the best way to engineer a system in which readers have only intermittent connectivity? Indeed, what is the best way to model such a system?

IV. Conclusion

It is astonishing how a modest device like an RFID tag, essentially just a wireless license plate, can give rise to the complex melange of security and privacy problems that we explore here. RFID privacy and security are stimulating research areas that involve rich interplay among many disciplines, like signal processing, hardware design, supply-chain logistics, privacy rights, and cryptography. There remain connections to be explored between the work surveyed here and other areas of study. We conclude by highlighting a few of these.

The majority of the articles treated in this survey explore security and privacy as a matter between RFID tags and readers. Of course, tags and readers lie at the fringes of a full-blown RFID system. At the heart will reside a massive infrastructure of servers and software. Many of the attendant data-security problems – like that of authenticating readers to servers – involve already familiar data-security protocols. But the very massive *scale*of RFID-related data flows and cross-organizational information sharing will introduce new data-security problems. We have mentioned key-management and PIN distribution for tags as one such potential problem. Other challenges will arise from the fluidity of changes in tag ownership. Today, domain names, for example, do not change hands very frequently; the DNS can involve human-intermediated access-control. The ONS – should it indeed see fruition – will need to accommodate many, many more objects that change hands with great frequency.

Sensors are small hardware devices similar in flavor to RFID tags. While RFID tags emit identifiers, sensors emit information about their environments, like ambient temperature or humidity. Sensors typically contain batteries, and are thus larger and more expensive than passive RFID tags. Between active RFID tags and sensors, however, there is little difference but nomenclature. For example, some commercially available active RFID devices are designed to secure port containers. They emit identifiers, but also sense whether or not a container has been opened. Given such examples, there is surprisingly little overlap between the literature on sensor security and that on RFID security. The boundaries between wireless-device types will inevitably blur, as evidenced by the dual role of reader and tag played by NFC devices.

Another important aspect of RFID security that of user *perception* of security and privacy in RFID systems. As users cannot see RF emissions, they form their impressions based

on physical cues and industry explanations. RFID will come to secure ever more varied forms of physical access and logical access. To engineer usable RFID systems and permit informed policy decisions, it is important to understand how RFID and people mix. This area sees some preliminary examiniation in [66], [77], [23].

Further reading: Finkenzeller [29] is the standard reference for general technical background on RFID. Shorter and more accessible are the on-line primer materials published by the *RFID Journal* [1], which is also a helpful source of current industry news.

The master's thesis of Steven Weis [88] describes early work in the area of RFID privacy, and provides good technical background. The recent U.S. Federal Trade Commission report in [21] provides a helpful regulatory perspective on RFID as it relates to consumers. An advisory committee known the Article 29 Working Party is in the process of developing European Commission privacy guidelines for RFID, which should be available soon. In 2003, a workshop on RFID Privacy took place at the MIT Media Lab. The workshop gave rise to a recently published book entitled *RFID: Applications, Security, and Privacy* [37]; the contributing authors offer a rainbow of backgrounds and perspectives.

Acknowledgements

The author would like to thank Farooq Anjum, Dan Bailey, David Molnar, Radha Poovendran, and Steve Weis for their comments on and suggestions for this work.

References

[1] RFID Journal. Online publication. Referenced 2005 at http://www.rfidjournal.com.

[2] Alien Technology Corporation achieves another step toward pervasive, economic RFID with announcement of 12.9 cent RFID labels, 13 September 2005. Alien Technology Press Release. Referenced 2005 at http://www.alientechnology.com.

[3] Boycott Benetton web site, 2005. Referenced 2005 at http://www.boycottbenetton.com.

[4] ECRYPT (European network for excellence in cryptology), stream cipher project Web page, 2005. Referenced 2005 at http://www.ecrypt.eu.org/stream/.

[5] Texas Instruments gen 2 inlay data sheet, 2005. Referenced 2005 at http://www.ti.com/rfid/docs/manuals/pdfSpecs/epc_inlay.pdf.

[6] Benetton explains RFID privacy flap. *RFID Journal*, 23 June 2004. Referenced 2005 at http://www.rfidjournal.com/article/articleview/471/1/1/.

[7] Merloni unveils RFID appliances. *RFID Journal*, 4 April 2003. Referenced 2005 at http://www.rfidjournal.com/article/articleview/369/1/1/.

[8] R. J. Anderson and M. G. Kuhn. Low cost attacks on tamper resistant devices. In B. Christianson, B. Crispo, T. M. A. Lomas, and M. Roe, editors, *Security Protocols Workshop*, volume 1361 of *Lecture Notes in Computer Science*, pages 125–136. Springer-Verlag, 1997.

[9] G. Ateniese, J. Camenisch, and B. de Madeiros. Untraceable RFID tags via insubvertible encryption. In *12th ACM Conference on Computer and Communication Security*, 2005. To appear.

[10] G. Avoine. Privacy issues in RFID banknote protection schemes. In J.-J. Quisquater, P. Paradinas, Y. Deswarte, and A. Abou El Kadam, editors, *The Sixth International Conference on Smart Card Research and Advanced Applications – CARDIS*, pages 33–48. Kluwer Academic Publishers, 2004.

[11] G. Avoine. Adversarial model for radio frequency identification, 2005. Cryptology ePrint Archive, Report 2005/049. Referenced 2005 at http://eprint.iacr.org.

[12] G. Avoine, E. Dysli, and P. Oechslin. Reducing time complexity in RFID systems. In B. Preneel and S. Tavares, editors, *Selected Areas in Cryptography – SAC 2005*, Lecture Notes in Computer Science. Springer-Verlag, 2005. To appear.

[13] G. Avoine and P. Oechslin. RFID traceability: A multilayer problem. In A. Patrick and M. Yung, editors, *Financial Cryptography – FC '05*, volume 3570 of *Lecture Notes in Computer Science*, pages 125–140. Springer-Verlag, 2005.

[14] G. Avoine and P. Oechslin. A scalable and provably secure hash based RFID protocol. In F. Stajano and R. Thomas, editors, *The 2nd IEEE International Workshop on Pervasive Computing and Communication Security – PerSec 2005*, pages 110–114. IEEE, IEEE Computer Society Press, 2005.

[15] M. Baard. RFID foes find righteous ally. *Wired News*, 14 July 2005. Referenced 2005 at http://wired.com/news/privacy/0,1848,68133,00.

[16] M. Baard. RFID invades the capital. *Wired News*, 7 March 2005. Referenced 2005 at http://www.wired.com/news/privacy/0,1848,66801,00.html.

[17] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security analysis of a cryptographically-enabled RFID device. In P. McDaniel, editor, *14th USENIX Security Symposium*, pages 1–16. USENIX, 2005. Dedicated Web site at www.rfidanalysis.org.

[18] D. Carluccio, K. Lemke, and C. Paar. Electromagnetic side channel analysis of a contactless smart card: first results. In *ECrypt Workshop on RFID and Lightweight Crypto*, Graz, Austria, 2005. Slide presentation. Referenced 2005 at http://www.iaik.tu-graz.ac.at/research/krypto/events/index.php.

[19] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.

[20] J. Collins. Marks & Spencer expands RFID retail trial. *RFID Journal*, 10 February 2004. Referenced 2005 at http://www.rfidjournal.com/article/articleview/791/1/1/.

[21] United States Federal Trade Commission. Radio frequency identification: Applications and implications for consumers, March 2005. Workshop report from FTC staff. Referenced 2005 at www.ftc.gov/os/2005/03/050308rfidrpt.pdf.

[22] T. Daniels, M. Mina, and S.Russell. A signal fingerprinting paradigm for physical layer security in conventional and sensor networks. In *IEEE/CreateNet SecureComm*. IEEE, 2005. To appear.

[23] P. de Jager. Experimenting on humans using Alien technology. In S. Garfinkel and B. Rosenberg, editors, *RFID: Applications, Security, and Privacy*, pages 439–448. Addison-Wesley, 2005.

[24] T. Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In *IEEE/CreateNet SecureComm*. IEEE, 2005. To appear. Referenced 2005 at http://www.ait.edu.gr/faculty/T_Dimitriou_files/RFID-securecomm05.pdf.

[25] EPCglobal Web site, 2005. Referenced 2005 at http://www.EPCglobalinc.org.

[26] Guidelines on EPC for consumer products, 2005. Referenced 2005 at http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html.

[27] American Civil Liberties Union (ACLU) et al. RFID position statement of consumer privacy and civil liberties organizations, 20 November 2003. Referenced 2005 at http://www.privacyrights.org/ar/RFIDposition.htm.

[28] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In M. Joye and J.-J. Quisquater, editors, *Workshop on Cryptographic Hardware and Embedded Systems CHES 04*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370. Springer-Verlag, 2004.

[29] K. Finkenzeller. *RFID Handbook*. John Wiley & Sons, 1999.

[30] K. Fishkin and J. Lundell. RFID in healthcare. In S. Garfinkel and B. Rosenberg, editors, *RFID: Applications, Security, and Privacy*, pages 211–228. Addison-Wesley, 2005.

[31] K. P. Fishkin, S. Roy, and B. Jiang. Some methods for privacy in RFID communication. In *1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, 2004.

[32] 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-03-011,25 October 2003.

[33] K.P. Fishkin, B. Jiang, M. Philipose, and S. Roy. I sense a disturbance in the force: Unobtrusive detection of interactions with RFID-tagged objects. In *Sixth International Conference on Ubiquitous Computing*, pages 268–282, 2004.

[34] C. Floerkemeier, R. Schneider, and M. Langheinrich. Scanning with a purpose - supporting the fair information principles in RFID protocols, 2004. Referenced 2005 at citeseer.ist.psu.edu/floerkemeier04scanning.html.

[35] United States Food and Drug Administration. Combatting counterfeit drugs: A report of the Food and Drug

Administration, 18 February 2004. Referenced 2005 at http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html.

[36] S. Garfinkel. An RFID Bill of Rights. *Technology Review*, page 35, October 2002.

[37] S. Garfinkel and B. Rosenberg, editors. *RFID Applications, Security, and Privacy*. Addison-Wesley, 2005.

[38] H. Gilbert, M. Robshaw, and H. Sibert. An active attack against HB^+ – a provably secure lightweight authentication protocol. Manuscript, July 2005.

[39] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets. In T. Okamoto, editor, *RSA Conference - Cryptographers' Track (CT-RSA)*, volume 2964 of *Lecture Notes in Computer Science*, pages 163–178, 2004.

[40] N. Good, J. Han, E. Miles, D. Molnar, D. Mulligan, L. Quilter, J. Urban, and D. Wagner. Radio frequency identification and privacy with information goods. In S. De Capitani di Vimercati and P. Syverson, editors, *Workshop on Privacy in the Electronic Society – WPES*, pages 41–42. ACM, ACM Press, 2004.

[41] J. Halamka. Straight from the shoulder. *The New England Journal of Medicine*, 353:331–333, 28 July 2005.

[42] G. P. Hancke and M. G. Kuhn. An RFID distance bounding protocol. In *IEEE/CreateNet SecureComm*. IEEE, 2005. To appear. Referenced 2005 at http://www.cl.cam.ac.uk/ gh275/distance.pdf.

[43] G.P. Hancke. A practical relay attack on ISO 14443 proximity cards. Manuscript. Referenced 2005 at http://www.cl.cam.ac.uk/ gh275/relay.pdf.

[44] M. Hellman. A cryptanalytic time-memory tradeoff. *IEEE Transactions on Information Theory*, IT-26:401–406, 1980.

[45] D. Henrici and P. Müller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In R. Sandhu and R. Thomas, editors, *Workshop on Pervasive Computing and Communications Security – PerSec 2004*, pages 149–153. IEEE, IEEE Computer Society, 2004.

[46] International Civil Aviation Organization ICAO. Document 9303, machine readable travel documents (MRTD), part I: Machine readable passports, 2005.

[47] EPCglobal Inc. EPC^{TM} generation 1 tag data standards version 1.1 rev. 1.27, 10 May 2005. Referenced 2005 at http://www.epcglobalinc.org.

[48] VeriSign Inc. VeriSign EPC starter service^{TM} data sheet, 2005. Referenced 2005 at http://www.verisign.com/static/015884.pdf.

[49] S. Inoue and H. Yasuura. RFID privacy using user-controllable uniqueness. In *RFID Privacy Workshop*, MIT, Massachusetts, USA, November 2003.

[50] Texas Instruments and VeriSign, Inc. Securing the pharmaceutical supply chain with RFID and public-key infrastructure technologies. Whitepaper. Referenced 2005 at http://www.ti.com/rfid/docs/customer/eped-form.shtml.

[51] M. Jakobsson and S. Wetzel. Security weaknesses in Bluetooth. In D. Naccache, editor, *The Cryptographers Track at RSA*, volume 2020 of *Lecture Notes in Computer Science*, pages 176–191. Springer-Verlag, 2001.

[52] A. Juels. Minimalist cryptography for low-cost RFID tags. In C. Blundo and S. Cimato, editors, *The Fourth International Conference on Security in Communication Networks – SCN 2004* , volume 3352 of *Lecture Notes in Computer Science*, pages 149–164. Springer-Verlag, 2004.

[53] A. Juels. 'Yoking-proofs' for RFID tags. In R. Sandhu and R. Thomas, editors, *Workshop on Pervasive Computing and Communications Security – PerSec 2004*, pages 138–143. IEEE Computer Society, 2004.

[54] A. Juels. Strengthing EPC tags against cloning. In *ACM Workshop on Wireless Security (WiSe)*. ACM Press, 2005. To appear.

[55] A. Juels and J. Brainard. Soft blocking: Flexible blocker tags on the cheap. In S. De Capitani di Vimercati and P. Syverson, editors, *Workshop on Privacy in the Electronic Society – WPES*, pages 1–7. ACM, ACM Press, 2004.

[56] A. Juels, S. Garfinkel, and R. Pappu. RFID privacy: An overview of problems and proposed solutions. *IEEE Security and Privacy*, 3(3):34–43, May/June 2005.

[57] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. In D. Gollman, G. Li, and G. Tsudik, editors, *IEEE/CreateNet SecureComm*. IEEE, 2005. To appear. Referenced 2005 at http://www.cs.berkeley.edu/ dmolnar/papers/papers.html.

[58] A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFID-enabled banknotes. In R. Wright, editor, *Financial Cryptography '03*, volume 2742 of *Lecture Notes in Computer Science*, pages 103–121. Springer-Verlag, 2003.

[59] 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.

[60] A. Juels, P. Syverson, and D. Bailey. High-power proxies for enhancing RFID privacy and utility. In G. Danezis and D. Martin, editors, *Privacy Enhancing Technologies (PET)*, 2005. To appear.

[61] A. Juels and S. Weis. Authenticating pervasive devices with human protocols. In *Advances in Cryptology – CRYPTO 2005*, pages 293–308. Springer-Verlag, 2005. Lecture Notes in Computer Science, Volume 3621.

[62] A. Juels and S. Weis. Defining strong privacy for RFID, 2005. Manuscript.

[63] U. Kaiser. Universal immobilizer crypto engine. In *Fourth Conference on the Advanced Encryption Standard (AES)*, 2004. Slide presentation. Referenced 2004 at http://www.aes4.org/english/events/aes4/. Subsequently removed.

[64] G. Karjoth and P. Moskowitz. Disabling RFID tags with visible confirmation: Clipped tags are silenced (short paper). In S. De Capitani di Vimercati and R. Dingledine, editors, *Workshop on Privacy in the Electronic Society (WPES)*, 2005. To appear.

[65] Z. Kfir and A. Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. In *IEEE/CreateNet SecureComm*. IEEE, 2005. To appear. Referenced 2005 at http://eprint.iacr.org/2005/052.

[66] T. Kindberg, A. Sellen, and E. Geelhoed. Security and trust in mobile interactions: A study of users' perceptions and reasoning. In N. Davies, E. D. Mynatt, and I. Siio, editors, *Ubiquitous Computing: 6th International Conference (Ubicomp)* , volume 3205 of *Lecture Notes in Computer Science*, pages 196–213. Springer-Verlag, 2004.

[67] D. Molnar, A. Soppera, and D. Wagner. Privacy for RFID through trusted computing (short paper). In S. De Capitani di Vimercati and R. Dingledine, editors, *Workshop on Privacy in the Electronic Society (WPES)*, 2005. To appear.

[68] D. Molnar, A. Soppera, and D. Wagner. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In B. Preneel and S. Tavares, editors, *Selected Areas in Cryptography – SAC 2005*, Lecture Notes in Computer Science. Springer-Verlag, 2005. To appear.

[69] 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.

[70] M. Ohkubo, K. Suzuki, and S. Kinoshita. Efficient hash-chain based RFID privacy protection scheme. In *International Conference on Ubiquitous Computing – Ubicomp, Workshop Privacy: Current Status and Future Directions*, 2004.

[71] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. Physical one-way functions. *Science*, 297:2026–2030, 20 Sept. 2002.

[72] J. Parkinson. RFID: U.S. consumer research findings, 21 June 2004. Presentation from National Retail Federation at U.S. Federal Trade Commission RFID Workshop. Referenced 2005 at http://www.ftc.gov/bcp/workshops/rfid/parkinson.pdf.

[73] M. Rieback, B. Crispo, and A. Tanenbaum. RFID Guardian: A battery-powered mobile device for RFID privacy management. In Colin Boyd and Juan Manuel González Nieto, editors, *Australasian Conference on Information Security and Privacy – ACISP 2005*, volume 3574 of *Lecture Notes in Computer Science*, pages 184–194. Springer-Verlag, 2005.

[74] M. R. Rieback, B. Crispo, and A. S. Tanenbaum. Keep on blockin' in the free world: Personal access control for low-cost RFID tags. In *Proc. 13th International Workshop on Security Protocols*, Lecture Notes in Computer Science. Springer-Verlag, 2005. To appear.

[75] S. E. Sarma, S. A. Weis, and D.W. Engels. RFID systems, security and privacy implications. Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT, 2002.

[76] M.I. Shamos. Paper v. electronic voting records - an assessment, 2004. Paper written to accompany panel presentation at Computers, Freedom, and Privacy Conference '04. Referenced 2005 at http://euro.ecom.cmu.edu/people/faculty/mshamos/paper.htm.

[77] S. Spiekermann. Perceived control: Scales for privacy in ubiquitous computing environments. In L. Ardissono and T. Mitrovic, editors, *Conference on User Modeling – UM'05*, 2005. To appear.

[78] T. Staake, F. Thiesse, and E. Fleisch. Extending the EPC network – the potential of RFID in anti-counterfeiting. In *ACM Symposium on Applied Computing*, pages 1607–1612. ACM Press, 2005.

[79] F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *7th International Workshop on Security*

Protocols, volume 1796 of *Lecture Notes in Computer Science*, pages 172–194. Springer-Verlag, 1999.

[80] R. Stapleton-Gray. Would Macys scan Gimbels? competitive intelligence and RFID. In S. Garfinkel and B. Rosenberg, editors, *RFID: Applications, Security, and Privacy*, pages 283–290. Addison-Wesley, 2005.

[81] S. Stern. Security trumps privacy. *Christian Science Monitor*, 20 December 2001.

[82] K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh. An ultra small individual recognition security chip. *IEEE Micro*, 21(6):43–49, 2001.

[83] I. Vajda and L. Buttyán. Lightweight authentication protocols for low-cost RFID tags. In *Second Workshop on Security in Ubiquitous Computing – Ubicomp 2003*, 2003.

[84] VeriChip corporation web site, 2005. Referenced 2005 at http://www.4verichip.com/.

[85] C.P. Wallace. The color of money. *Time Europe*, 158(11). 10 September 2001.

[86] S. Weis. Security parallels between people and pervasive devices. In F. Stajano and R. Thomas, editors, *The 2nd IEEE International Workshop on Pervasive Computing and Communication Security – PerSec 2005*, pages 105–109. IEEE, IEEE Computer Society Press, 2005.

[87] S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In D. Hutter, G. Müller, W. Stephan, and M. Ullmann, editors, *International Conference on Security in Pervasive Computing – SPC 2003*, volume 2802 of *Lecture Notes in Computer Science*, pages 454–469. Springer-Verlag, 2003.

[88] S.A. Weis. Radio-frequency identification security and privacy. Master's thesis, M.I.T., June 2003.

[89] J. Westhues. Hacking the prox card. In S. Garfinkel and B. Rosenberg, editors, *RFID: Applications, Security, and Privacy*, pages 291–300. Addison-Wesley, 2005.

[90] D. White. NCR: RFID in retail. In S. Garfinkel and B. Rosenberg, editors, *RFID: Applications, Security, and Privacy*, pages 381–395. Addison-Wesley, 2005.

[91] R. Yu. Electronic passports set to thwart forgers. *USA Today*, 8 August 2005. Referenced 2005 at http://www.usatoday.com/travel/news/2005-08-08-electronic-passports_x.htm.

[92] K. Zetter. Feds rethinking RFID passport. *Wired News*, 26 Apr. 2005. Referenced 2005 at http://www.wired.com/news/privacy/0,1848,67333,00.html.