Personal and Ubiquitous Computing manuscript No.
(will be inserted by the editor)

Marc Langheinrich

A Survey of RFID Privacy Approaches

Received: January 30, 2008 / Accepted: May 5, 2008

Abstract A bewildering number of proposals have offered solutions to the privacy problems inherent in RFID communication. This article tries to give an overview of the currently discussed approaches and their attributes.

Keywords RFID · privacy

1 Introduction

An April 2008 search for articles on RFID privacy and security in Google Scholar[1] yields over 700 titles, while Gildas Avoine's manually maintained *RFID Security & Privacy Bibliography* [2] still lists as many as 214 publications on this topic since 2003. There certainly seems to be no shortage of scholarly work in this area, yet a "solution" to these problems remains elusive. A June 2007 EU policy document [16] states that "effective action is needed so Europeans can trust that the various applications of RFID and related technologies are as safe, secure and privacy-friendly as they possibly can be."

Why is the seemingly simple problem of securing the readout of a relatively short numeric identification code still unsolved? What issues still need to be addressed before "safe, secure and privacy-friendly" RFID tags have become a reality? This article attempts to summarize the existing body of knowledge and identifies the issues and shortcomings of today's proposals.

2 Uses and Threats

One problem that prevents a silver-bullet solution to RFID privacy is certainly the wide range of applications and technologies that the generic term "RFID" comprises. Want [57] provides an excellent overview of the various uses and technologies; Juels [29] offers valuable insights into the security and privacy implications of these. For the purpose of this article, we will focus on low-cost, battery-less (passive) systems, as these will most likely have the biggest impact on consumer privacy, due to their potentially large numbers and low computational resources.

The basic feature of an RFID system is the automatic *identification* of items [38]. In its simplest form, such identification can be binary, e.g., paid or not paid, useful for *alerting*. Modern tags allow hundreds of bits to be used for such an ID, and standardization bodies such as EPCglobal have defined formats that allow for the automatic resolution of these IDs into product information. With multiple readers deployed, even unresolved IDs can still offer *monitoring* capabilities by tracking the movements of an item, e.g., goods in a manufacturing process. In contrast to bar codes, RFID tags can additionally offer on-chip computation, thus supporting cryptographic protocols for *authentication*. Especially relevant for privacy is the fact that these function can be accessed without a line-of-sight, i.e., both reader and tag can be completely hidden from view, making it difficult, if not impossible for the owners of scanned objects to be aware of such a process taking place.

All four of these RFID use cases – identification, alerting, monitoring, and authentication – can be subverted by a specific type of attack. These attacks will be described in the following subsections.

2.1 Authentication and Counterfeiting

RFID technology has its roots in the "identify friend or foe" (IFF) systems for fighter planes in the second world war [49], where non-forgeable identities were vital. Today, RFID-based smart-cards are already in widespread use as payment and travel systems (e.g., the Japanese SUICA card or the Octopus card in Hong Kong), access control systems (such as skipasses or car immobi-

M. Langheinrich
Faculty of Informatics, University of Lugano, USI
Via Guiseppe Buffi 13, 6904 Lugano, Switzerland
E-mail: langheinrich at acm dot org

[1] See `scholar.google.com`.

lizers), and most recently as national and international identification documents. Efforts are also underway to extend the identification functionality of RFID tags to fight product counterfeiting [53], in particular for medical drugs and luxury items such as watches. In all cases, it is imperative that the authenticity of RFID tags cannot be compromised.

While the mere use of RFID chips already complicates the process of creating forged items, the widespread availability of writable or even reprogrammable tags means that the use of RFID alone does not offer enough protection from determined counterfeiters. Westhues [59] built what is practically an "RFID tape recorder", which could record and play back replies from many commercial RFID-based access control systems. Consequently, tags and readers usually need to share a common secret and employ a challenge-response protocol to verify each other's knowledge of the secret. Challenge-response protocols are a well-known problem in security literature, and many strong solutions exist. The particular challenge of RFID lies both in the low computational power of the tags, as well as their susceptabilty to physical attacks, implying that RFID solutions must be both of low complexity and resistant to pyhsical memory analysis [58].

While forged RFID tags certainly represent a security problem, they are not in the focus of RFID privacy concerns. Forged *reader* authentications, however, are much more relevant, as the next section will show.

2.2 Identification and Sniffing

The core RFID privacy problem is that of unauthorized tag readout: with the help of wireless communication, third parties can in principle read the tags of personal items from large distances, and without any indication that such a readout is taking place. Controlling access to tag data is thus of prime importance.

By default, most RFID tags are indiscriminate: upon entering a sufficiently powered reader field, they will reply to any well-formed reader request with their full ID. With standardized ID formats, such as EPCglobal's tag data specification [15], this ID can be resolved into a particular application domain, a manufacturer, a product name, and even a serial number. A typical concern is thus that "chatty" RFID tags disclose the posession of personal items normally hidden from view, e.g., the brand of underwear one is wearing, the presence of a wig or hip replacement, or even a particular medicine one is carrying [38]. When in 2003 the European Central Bank considered the use of RFID tags in Banknotes [41], criminal scenarios quickly surfaced in which clever robbers would screen their victims first in order to assess the amount of cash carried. Similar concerns surround the use of RFID in travel documents, where a chatty passport might disclose the citizenship of its bearer and thus allow the construction of "smart bombs" that would only blow up if a worthwile target passes by.

Clearly, this act of *sniffing out* the data on an RFID tag can only be prevented if tags disclose their identitiy only to authorized readers, i.e., those that are under the control of the item owner or another authorized party. Authenticating readers, or more generally speaking, the interrogating party, is thus the primary technical issue for RFID privacy. Furthermore, care must be taken that an unauthorized party could not simply listen in to an unsecured communication between a tag and a legitimate reader.

2.3 Monitoring and Tracking

It is important to realize that privacy can also be violated without actually identifying individual items. Once a specific tag or a set of tags can be associated with a particular person, the mere presence of this tag in a particular reader field already implies a (most likely unwanted) location disclosure. Combining several such sightings across multiple logs can easily *track* a person over longer periods of time. The fact that RFID tags are typically unique excerbates the problem, yet Weis [58] already noted that even non-unique IDs can uniquely identify a person by virtue of the particular *constellation* they are carried in.

To prevent such tracking, it is not sufficient to simply scramble an ID to prevent the identification of an item – tags must either frequently update their ID in a non-predictable (and preferably non-traceable) manner, or remain completely silent upon inquiries from illegitimate readers. The latter approach, while intuitively appealing, is difficult in practice: in order to prove its authenticity to a particular tag, a reader would need to know which tag to prove it to (i.e., which secret to use in the authentication algorithm). Without some sort of initial reply from the tag, this is difficult.[2]

2.4 Alerting and Denial of Service

In its simplest form, an RFID tag simply announces its presence, e.g., to an anti-theft gate in a bookstore. Sold items get their embedded RFID tag killed at checkout so that only unpaid items will be detected.

To completely alleviate privacy concerns of RFID tags, an irreversible tag deactivation is necessary. Current industry protocols like EPCglobal's Class-1 Gen-2 [14] already require compliant tags to offer a *Kill-command* that completely silences the tag once issued. As post-sales benefits of tagged items increase (e.g., smart washing machines or RFID-enabled returns), however, permanently disabling tags might force the consumer to choose between privacy and the convenience offered by

[2] The alternative of using the same secret for all of its tags typically lowers the strength of the authentication algorithm significantly.

novel RFID-based services. Temporary silencing a tag (e.g., only between the supermarket to the home, where it can be reactivated) might improve this, yet incurs high password management costs [27], as reactivation must necessarily be restricted to authorized readers only. Such credentials would need to be passed on from vendor to consumer, and potentially further on to other family members or friends, for whom a certain item might have been bought – a technical feat that would require practically all point-of-sale-systems to seamlessly exchange such data with just about any personal electronic device (e.g., a mobile phone or wireless smart card), and in turn with the plethora of home-installed RFID systems and readers out there. This assumes, of course, that all consumers would carry and use such an electronic device in the first place.

The act of tag deactivation is typically in direct conflict with commercial security concerns. If tags could be silenced too easily, entire supply chains could be severely disrupted by an attacker mounting a *denial-of-service* attack, i.e., sending kill commands to passing trucks or while strolling though supermarket aisles. A simple aluminium-foil lined bag is often enough to hide tagged items in there in order to prevent an automated sales terminal from picking up stolen goods; a personal jamming device that would prevent readers from "coming through" might work equally well.

3 Technical Approaches to RFID Privacy

Westin defines privacy as "the claim of individuals . . . to determine for themselves when, how, and to what extend information about them is communicated to others" [60]. Sniffing and tracking RFID tags violates this control, whether it involves actual data disclosure (in the form of meaningful IDs) or simply presence indication (through meaningless but trackable IDs).

There are certainly many ways of categorizing the various RFID privacy proposals under discussion today. Short of killing tags at checkout, we can broadly distinguish between two technical options:

- *Hiding, Blocking:* Tags are effectively silenced, either by jamming the radio channel or by having them reply only to readers that present proper credentials.
- *Encrypting, Rewriting:* Tag data is rendered meaningless to unauthorized readers. In order to prevent tracking, even meaningless data must be updated periodically.

The following sections will discuss the various solutions discussed in the literature, with a particular focus on deployment: If a solution requires costly rewritable tags, or even the implementation of special crypto circuitry, the odds of a large scale deployment of this approach diminish rapidly. Solutions that can be readily implemented on standard EPCglobal-conformant tags are particularly appealing. Also the operational costs, i.e., the required infrastructure for both vendors and consumers, and the individual effort for using the system, must be taken into account. Section 4 will then describe some further deployment issues in more detail.

3.1 Hiding and Blocking

Karjoth and Moskowitz [34] propose to physically clip tags at checkout, using perforated tear-off antennas. Tags remain functional, yet their range is effectively reduced to few centimeters. While the technology has been commercially licensed [54], its applicability is limited to items with non-embedded tags. A proposal by Inoue and Yasuura [25] suggests the use of two tags, with one tag holding the unique serial number being peeled away at purchase time, effectively reducing the granularity of the identification.[3] A number of vendors such as Emvelope Inc.[4] have begun selling aluminimum lined wallets and pouches for keeping RFID-enabled credit cards and passports safe from unwanted readouts.

For items that do not fit in pouches nor have detachable labels, Juels, Rivest, and Szydlo [32] proposed the so-called *blocker-tag*, a simple RFID tag that overloads a reader's anti-collission protocol by answering to every single read request with a jammed signal. While the blocker-tag could be manufactured cheaply (as it is more or less a particularly programmed RFID tag), its operation depends greatly on its orientation: if misaligned, it could cease operating due to lack of power from a reader's field and thus expose all of its blocked tags.

Rieback, Crispo, and Tanenbaum [48] also point out that differential signal analysis could differentiate between blocker-tag-only jamming signals and those were both a blocker-tag and a real tag reply. They instead propose a battery powered device, the *RFID Guardian* [47], which not only produces a randomly modulated jamming signal, but also allows the user to upload access control lists indicating which party can perform what operation on which tags.[5] Sanjay Sarma, co-founder of MIT's Auto-ID center, has proposed a similar device called the *Vindictive Sentinel*, albeit with a simpler configuration: all valid readers would be registered and all others would be blocked completely.[6] Spiekermann [51] (in this volume) calls this approach the "Agent Scheme" (see also section 4.2 on the issue of "ownership transfer" below).

[3] Note that such items could still be traceable as particular *constellations* [58].

[4] See `www.emvelope.com`

[5] To allow for selective jamming, the RFID Guardian requires the use of a deterministic protocol like ISO-15693, where tags reply in a pre-defined timeslot (based on their ID) to reader requests.

[6] See slides of his invited talk at `events.iaik.tugraz.at/RFIDSec06/Program/`

3.2 Rewriting and Encryption

Encryption is often seen as the obvious solution for securely controlling access to one's tags. Juels rightly refers to this as "siren song of encryption" [27]: This is because many proposals ignore the practical problems of key management, i.e., how the required keys for hundreds of mundane objects such as underwear, DVD-cases, chewing gum packs, or soft drinks could possibly be securely and reliably exchanged between stores and their customers, as well as consumers and their friends and families. Consequently, encryption might only work well in controlled systems such as payment cards and identification systems, not with cheap everyday artifacts.

In its simplest form, cryptographically controlled access was first proposed by Weis et al. [58] in the form of *hash locks*: tag data is only released if the correct key is given, which is stored in hashed form directly on the tag. This hash value can be read out by any reader, yet only authorized ones would be able to look up the tag's key in a database of key-hash pairs. Tags would be able to verify a key using an integrated hash function that comparse the key hash with the stored hash value. While this protects the actual data on the tag, Weis at al. realized that a static hash value would still be traceable, and thus proposed an extension using random values: Instead of simply sending their static hash value, tags choose a random value r and send the pair $(r, h(ID||r))$ to the reader, prompting the reader to brute-force its inventory for any ID that matches the given hash if concatenated with r [58].

Using randomized hash locks prevents readers from tracking an unknown item, yet it also complicates the reader's search for the correct key. In practice, Weis et al.'s scheme requires readers to lineraly search through its list of tags. Many proposals exist to avoid such brute-force searches, while keeping the untraceability property of seemingly random tag replies. The general idea is to keep a counter on both the tag and the reader loosely synchronized, and include this value in tag replies. The reader can then keep a few possible tag values for each tag, and update its database whenever it successfully identified a tag. One of the first such proposals was by Ohkubo, Suzuki, and Kinoshita [45], who proposed to use *hash-chains* and precompute m such tag outputs in a look-up table. By limiting the length of hash-chains to m, readers could store those efficiently. While this scheme provides *forward security*,[7] it is vulnerable to replay attacks [3]. Henrici and Müller [23] use a Δc in each tag that counts the read attempts since the last successful reader authentication. Sending Δc to readers eliminates the vulnerability of the Ohkubo scheme to replay attacks, without hampering quick authentication. Malicious readers may artificially inflate Δc and thus be able to track a tag. Dimitriou [10] uses *mutual* authentication of both tags and readers to limit ID updating, thus keeping both readers and tags always in perfect synchronization. If no authorized reader updates the tag value, however, its value stays constant and can thus be tracked again.

A different approach again is followed by Molnar and Wagner [44], who propose a tree-based key-space: Tags do not hold a single key, but a set of keys arranged in a tree. Each tag stores all keys of a single particular path in the tree, with authorized readers knowing all keys in the tree. The reader can then use a challenge-response protocol to step through the tree from its root to the leaves, checking whether the tag in question contains a key, e.g., in the left or the right part of the tree (in case of a binary tree). In contrast to approaches using brute-force key spaces searches, this scheme offers logarithmic lookup properties. This, however, comes at the expense of security, as tags share large parts of the keyspace: if one or more tag-secrets are compromised, the security of the remaining tags is affected. This general idea has since been extended by Buttyan et al. [6], Dimitriou [11], and Lu et al. [40], yet tree-based approaches typically lack key-updating capabilities due to their shared keyspace.

[7] Forward security means that a compromised tag does not disclose the entire history of tag sightings, even if these were under different pseudonym IDs.

4 Practical Issues for Deployment

Hiding or encrypting a tag seems simple enough, yet when implemented for hundreds of millions of tags, on a global scale, and involving complex flows of goods between manufacturers, vendors, customers, and even the customers' friends and families, simplicity in both implementation and operation is of paramount importance. The following sections will describe the current work in both hardware optimization (to minimize tag costs) and process optimization (to simplify use of privacy mechanisms), in particular the process of changing the ownership of a tagged item. Last but not least, we will also report on policy solutions that are meant to complement any deployed technical protection.

4.1 Cryptographic Primitives

A large body of work in RFID privacy is concerned with lowering the requirements for cryptographic functions implemented on RFID hardware, such as the work by Feldhofer, Dominikus, and Wolkerstorfer [18] on using AES or the use of elliptic curve cryptography [4]. Some researchers target the limited hardware capabilities of standard EPCgloabl-tags, providing algorithms that only rely on simple XOR operations [35] or the presence of a random number generator [8, 55].

Juels [26] points out that typical attack models need to be significantly relaxed in real-world RFID environments, as adversaries typically do not have 24/7-access

to a tag, but rather minutes or seconds. Juels argues that a simple list of pseudonyms that cycles to a new ID upon every read request might be sufficient in many cases. By limiting the number of IDs that can be read out, an attacker has a much lower probability of re-encountering an ID, while at the same time not being able to resolve the (random) pseudonym. While certainly cheap to implement on a tag, Juels' scheme still requires the exchange of lookup tables to allow legitimate readers the resolving of pseudonyms.

An interesting avenue of research was initiated by Juels' and Weis' HB$^+$-protocol [33], which is a *probabilistic* algorithm that can be used to both authenticate a tag to a reader and to hide the real ID of a tag to an eavesdropper. In the HB$^+$-protocol, both reader and tag share a common k-bit secret $\boldsymbol{x}$, which allows the tag to compute the binary inner product $z = \boldsymbol{x} \cdot \boldsymbol{a}$ for a k-bit challenge $\boldsymbol{a}$ sent by the reader. However, instead of directly replying with the result z, the tag injects noise into its response with a constant probability $p \leq 0.5$. By repeating this challenge-response protocol for r rounds, the reader can identify/authenticate the tag if fewer than pr of its responses fit a particular secret $\boldsymbol{x}$. An attacker, on the other hand, is unable to learn the secret due to the presence of noise.[8] The HB$^+$-protocol only requires simple bitwise AND and XOR operations on the tag. In a similar fashion, Castelluccia and Soos [7] propose a probabilistic approach that has a tag reply with a random subset of L indexes from its key $\boldsymbol{x}$ (e.g., "`1,6,5,2`" for a 6-bit key), together with a bitstring $\boldsymbol{a}$ that complements this subset in such a way that the binary inner product $z = \boldsymbol{x} \cdot \boldsymbol{a} = L/2$. By repeatedly sending both indexes and complementing bitstrings, the reader can compute z for each of its known secrets and successively eliminate keys where $z \neq L/2$. As in the HB$^+$-protocol, an attacker needs to solve an NP-hard problem, while tags need only simple AND and XOR operations.

While work on cryptographic primitives is central to bringing strong cryptography to lower-powered and cheap RFID hardware, this generally does not change the central issues of pseudonym updates, key distribution, and ownership transfer, as described in the following subsection.

4.2 Supporting Ownership Transfer

Of particular interest to any real-world deployment of RFID encryption are approaches that specifically attempt to simplify *ownership transfer*, i.e., updating the key of an RFID tag in such a way that a prior owner of a tagged item (e.g., the supermarket) cannot read the tag after the item has been given to a new owner. Early suggestions by Inoue and Yasuura [25] simply replaced the original tag ID with a *Private ID* that allowed the new tag owner to look up the original value in a private database. As this approach does not take tracking or rewriting attacks into account, reader authentication and dynamic pseudonym changes were introduced, e.g., in the work Osaka et al. [46]. Common to this and other approaches is the need for a *Trusted Center* that holds the actual information about the tag (i.e., its ID or details about the tagged goods), which authenticated readers can query for an encountered tag pseudonym in order to receive the true tag ID. Molnar, Soppera, and Wagner [43] extended the tree-based approach by Molnar and Wagner [44] with a *delegation model* that allows a trusted center to store key-subtrees on a trusted reader, thus eliminating the need for reader online access. Each subtree supports a specific number of tag identifications, say, 1000 times. If tag ownership changes, the new owner needs to notify the trusted center that previous readers are not authorized to access tag data anymore. If the trusted center already delegated a key-subtree, the new owner can simply "fast forward" the tag's keyspace by reading it repeatedly until the set of delegated keys has been exhausted (thus rendering the delegated subtree useless).

Spiekermann, Günther, and Berthold [5,52] advocate the mandatory use of hash-locks at supermarket checkouts, using a consumer-chosen "RFID-password." To facilitate password management, the authors envision a smart consumer device ("data-protection card", e.g., a future mobile phone) that "takes over" the tags at checkout or at a separate deactivation station.[9] To simplify operations, only a single password for all items could be used, thus further alleviating the need for a consumer-maintained database. Given the often minimal value and short lifetime of supermarket items, the authors argue against burdening the process with strong security precautions. The main strength of this work lies in providing a roadmap for retail-based RFID use, yet it remains to be seen how realistic a comprehensive deployment of such "data-protection" devices is. The authors also focus primarily on supermarket environments, even though tagged chewing gums, soda cans, and ice cream cones might also be sold at small newsstands and through street hawkers – situations where no sophisticated point-of-sales terminals for tag reprogramming would be available.

4.3 Keyless Approaches

As an alternative to blocking and encryption approaches, Fishkin, Roy, and Jiang [19] proposed the use of signal strength-measurements directly on the tag, in order to assess the distance between a tag and its reader. Following the general principle of "distance implies distrust", the authors propose several disclosure levels: no replies

[8] This is known as the *Learning Parity in the Presence of Noise (LPN)* Problem.

[9] Until such devices are available, the authors propose that new random passwords would be assigned by the supermarket and printed on the receipt.

to far away readers, presence (e.g., a single bit) to closer ones, product IDs for close-by readers, and unique serial for near contact. While elegant in principle, both the problem of performing reliable measurements on low-cost RFID hardware, as well as the difficult predictability of the disclosure policy (how close is "very close"?) render the proposal difficult in practice.

Langheinrich and Marti [39] extend Juels "minimalist cryptography" described above with bit-throttling and shared secrets, effectively wrapping the tag data into several encryption layers that require continuous read access for significant amounts of time. Based on Adi Shamir's theory of shared secrets [50], the tag's real ID is encoded into several pieces ("shares"). The ID can only be reconstructed if enough of those pieces are known. While all pieces are stored on the same tag, readout is complicated by allowing only a random trickle of bits from the tag. Together with a short read range, this requires an attacker to spend a considerable amount of time in close proximity to the "target", making quick unnoticeable readouts difficult. At the same time, however, legitimate owners are able to use simple caching strategies to identify their items instantaneously, as an initial burst of disclosed bits is enough to probabilistically identify a tag from a known set. In order to prevent the repeated querying of such a larger initial subset, which would give an attacker faster access to the entire key, tags use random temporary IDs for tag singularization, thus making it more difficult for an attacker to correlate two such bitstrings across consecutive queries. Juels, Pappu, and Parno [31] have leveraged this approach to effectively distribute keys along the supply chain. As a side effect, they advocate that sold items remain locked with this password, in order to prevent unauthorized readouts (effectively prohibiting post-sales consumer services, except through the original merchant). However, they do not address how to prevent the unauthorized tracking of static identifiers described in section 3.2 above.

4.4 Policy Controls

Many authors have noted that RFID reading does not happen in a legal vacuum. Readers are physical devices that emit significant amounts of radiation – attacks on RFID tags are thus much more difficult to hide than, say, server attacks on the Internet.

Floerkemeier, Schneider, and Langheinrich [20] propose the use of "transparency protocols" directly within RFID standards, requiring readers to explicitly state their operators, data collectors, collection purpose, and data recipients. This would at the very least allow consumer interest groups and privacy commissioners to inspect and verify (audit) the proper operation of such systems. In addition, interested users might carry personal devices able to read such statements (so-called "watchdog tags") and keep personal data disclosure logs or even control access to personal tags. A similar approach is proposed by Juels and Brainard [30], who call this device a *tag privacy agent* (TaPA). Molnar, Soppera, and Wagner [42] propose to build reader devices around a trusted computing module and thus receive an auditable attestation about the proper functioning of each reader.

Kriplean et al. [37] focus on access to collected RFID data and propose the concept of *physical access control* (PAC) as an alternative to complex access policies. With PAC, the system distinguishes between *users* and *objects* and allows authenticated users access to all object and user sightings that were "visible" to them, i.e., RFID readouts that happened in the (visible) vicinity of where their personal *user* tag had been at the time (based on a map of installed readers). To prevent "misplacing" one's *user* tag among someone elses belongings (thus claiming to be always co-located with that person, which in PUC would grant an attacker access to all activities of that person), the authors propose a number of alert and feedback methods, such as an elevator that would announce the number of *user* tags present, in order to allow spotting such attacks. Note that Kriplean et al. assume a trusted infrastructure and do not address protection from unauthorized readers.

5 Summary and Outlook

Much work in RFID privacy is concerned with secure and efficient cryptographic algorithms. This, however, does only address a fraction of the issues encountered in real-world RFID system. As most of today's proposals require a shared secret between readers and tags, they are difficult to deploy in a general consumer setting. Given the gaping security holes [24] in many deployed RFID-based applications such as RFID-credit cards and ePassports, however, research in RFID security is nevertheless timely and highly relevant (also with regards to counterfeiting and cloning, e.g., see [28,56]).

In order to "solve" the privacy problem for the countless smart shopping scenarios, much more is needed than a cryptographic protocol. Unless key management is significantly simplified, only keyless approaches seem to stand a chance of success. Similarly, any such solution requires strong regulatory support, either in the form of active self-regulation [21] or effective legal enforcement of existing laws [9]. The current activities at the European policy level [12,13], including the public consultations during March and April 2008,[10] are expected to lead to additional legal instruments, requiring, e.g., operators to conduct privacy impact assessments (PIA) prior to deployment and ensuring the use of up-to-date information security measures in their systems.

Fabian, Günther, and Spiekermann [17] point out that much of the RFID privacy problem might actually lurk

[10] See `ec.europa.eu/information_society/policy/rfid/index_en.htm`

in the backend of the envisioned EPC information infrastructure: instead of bothering with localized attacks using deployed readers, smart attackers might simply eavesdrop on the generated (unsecured) traffic in backend systems to track unsuspecting consumers. Last but not least, the scope of the envisioned data collections will most certainly require equally large efforts in areas of privacy databases [1] and profile management [36] to be complete.

Acknowledgements The feedback of the anonymous reviewers, as well as the many helpful comments from my co-editor Sarah Spiekermann, helped tremendously in the writing of this article.

References

1. Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Hippocratic databases. In *Proceedings of the 28th International Conference on Very Large Databases (VLDB 2002)*, pages 143–154, Hong Kong, August 2002. Morgan Kaufmann. Available from World Wide Web: `www.vldb.org/conf/2002/S05P02.pdf`.
2. Gildas Avoine. Bibliography on security and privacy in RFID systems. Available online at `lasecwww.epfl.ch/~gavoine/rfid/`, 2006.
3. Gildas Avoine, Etienne Dysli, and Philippe Oechslin. Reducing time complexity in RFID systems. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography – SAC 2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 291–306, Kingston, Canada, August 2005. Springer.
4. Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. An elliptic curve processor suitable for RFID-tags. Cryptology ePrint Archive, Report 2006/227, 2006. Available from World Wide Web: `eprint.iacr.org/2006/227.pdf`.
5. Oliver Bertold, Oliver Günther, and Sarah Spiekermann. RFID: Verbraucherängste und Verbraucherschutz. *Wirtschaftsinformatik*, 47(6):422 – 430, 2005. Available from World Wide Web: `edoc.hu-berlin.de/docviews/abstract.php?id=26367`.
6. Levente Buttyán, Tamás Holczer, and István Vajda. Optimal key-trees for tree-based private authentication. In Gene Tsudik, Paul Syverson, and Elisa Bertino, editors, *Privacy Enhancing Technologies – 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, Revised Selected Papers*, volume 4258 of *LNCS*, pages 332–350, Berlin Heidelberg New York, 2006. Springer.
7. Claude Castelluccia and Mate Soos. Secret shuffling: A novel approach to RFID private identification. Conference on RFID Security, Malaga, July 11-13, 2007, July 2007. Available from World Wide Web: `rfidsec07.etsit.uma.es/slides/papers/paper-45.pdf`.
8. Hung-Yu Chien and Che-Hao Chen. Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards. *Computer Standars & Interfaces, Elsevier Science Publishers*, 29(2):254–259, February 2007.
9. Data Protection Commissioners. Resolution on radio frequency identification. 25th International Conference of Data Protection and Privacy Commissioners, November 2003. Available from World Wide Web: `www.privacyconference2003.org/commissioners.asp`.
10. Tassos Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm*, Athens, Greece, September 2005. IEEE.
11. Tassos Dimitriou. A secure and efficient RFID protocol that could make big brother (partially) obsolete. In *PERCOM '06: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06)*, pages 269–275, Washington, DC, USA, 2006. IEEE Computer Society.
12. EC – European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on radio frequency identification RFID in Europe: Steps towards a policy framework. COM/2007/0096 final, March 2007. Available from World Wide Web: `eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0096:EN:NOT`.
13. EDPS – European Data Protection Supervisor. Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on radio frequency identification (RFID) in Europe: steps towards a policy framework COM(2007)96, December 2007. Available from World Wide Web: `www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf`.
14. EPCglobal. Class-1 generation-2 UHF RFID protocol for communications at 860 MHz–960 MHz, version 1.0.9. EPC radio-frequency identity protocols, January 2005. Available from World Wide Web: `www.epcglobalinc.org/standards/Class_1_Generation_2_UHF_Air_Interface_Protocol_Standard_Version_1.0.9.pdf`. See `www.epcglobalinc.org/standards/Class_1_Generation_2_UHF_Air_Interface_Protocol_Standard_Version_1.0.9.pdf`.
15. EPCglobal. EPC tag data specification 1.3. EPCglobal Standard, March 2006. Available from World Wide Web: `www.epcglobalinc.org/standards/EPCglobal_Tag_Data_Standard_TDS_Version_1.3.pdf`. See `www.epcglobalinc.org/standards/EPCglobal_Tag_Data_Standard_TDS_Version_1.3.pdf`.
16. European Union. European policy outlook RFID (draft version). Working document, German Federal Ministry of Economics and Technology, June 2007. See `www.nextgenerationmedia.de/Nextgenerationmedia/Navigation/en/rfid-conference.html`.
17. Bastian Fabian, Oliver Günther, and Sarah Spiekermann. Security analysis of the object name service for RFID. In *Proceedings of the 1st International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, July 2005.
18. Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In Marc Joye and Jean-Jacques Quisquater, editors, *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370, Boston, Massachusetts, USA, August 2004. IACR, Springer.
19. Kenneth Fishkin, Sumit Roy, and Bing Jiang. Some methods for privacy in RFID communication. In Claude Castelluccia, Hannes Hartenstein, Christof Paar, and Dirk Westhoff, editors, *Security in Ad-hoc and Sensor Networks – First European Workshop, ESAS 2004, Heidelberg, Germany, August 6, 2004, Revised Selected Papers*, volume 3313 of *LNCS*, pages 42–53, Berlin Heidelberg New York, August 2005. Springer.
20. Christian Flörkemeier, Roland Schneider, and Marc Langheinrich. Scanning with a purpose – Supporting the

fair information principles in RFID protocols. In Hitomi Murakami, Hideyuki Nakashima, Hideyuki Tokuda, and Michiaki Yasumura, editors, *Ubiquitous Computing Systems – Second International Symposium, UCS Tokyo, Japan, November 8–9, 2004, Revised Selected Papers*, volume 3598 of *LNCS*, pages 214–231, Berlin Heidelberg New York, June 2005. Springer.

21. Simson Garfinkel. RFID rights. *Technology Review*, 107(9), November 2004. Available from World Wide Web: `www.technologyreview.com/articles/04/11/wo_garfinkel110304.asp?p=1`.
22. Simson Garfinkel and Beth Rosenberg, editors. *RFID: Applications, Security, and Privacy*. Addison-Wesley, July 2005.
23. Dirk Henrici and Paul Müller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In Francis Lau and Hui Lei, editors, *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pages 149–153, Orlando, FL, USA, March 2004. IEEE Computer Society. Available from World Wide Web: `ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=28557&page=2`.
24. Thomas S. Heydt-Benjamin, Dan V. Bailey, Kevin Fu, Ari Juels, and Tom OHare. Vulnerabilities in first-generation RFID-enabled credit cards. In Sven Dietrich and Rachna Dhamija, editors, *Financial Cryptography and Data Security. 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago, February 12-16, 2007. Revised Selected Papers*, volume 4886 of *LNCS*, pages 2–14, Berlin Heidelberg New York, 2007. Springer. Available from World Wide Web: `www.springerlink.com/content/e7324164535up092/`. The full version of this paper appears as UMass Amherst CS TR-2006-055. See `www.rfid-cusp.org` for the latest version.
25. Sozo Inoue and Hiroto Yasuura. RFID privacy using user-controllable uniqueness. Proceedings of the RFID Privacy Workshop, MIT, November 2003. Available from World Wide Web: `www.rfidprivacy.us/2003/papers/sozo_inoue.pdf`.
26. Ari Juels. Minimalist cryptography for RFID tags. In Carlo Blundo, editor, *Security of Communication Networks (SCN)*, Amalfi, Italy, September 2004. Available from World Wide Web: `www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/minimalist/Minimalist.pdf`.
27. Ari Juels. RFID privacy: A tecnical primer for the non-technical reader. In Katherine Strandburg and Daniela Stan Raicu, editors, *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*. Springer, Berlin Heidelberg New York, 2005. Available from World Wide Web: `www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/rfid_privacy/DePaul23Feb05Draft.pdf`.
28. Ari Juels. Strengthening EPC tags against cloning. In *WiSe '05: Proceedings of the 4th ACM workshop on Wireless security*, pages 67–76, New York, NY, USA, 2005. ACM Press.
29. Ari Juels. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, February 2006. Available from World Wide Web: `www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf`.
30. Ari Juels and John Brainard. Soft blocking: Flexible blocker tags on the cheap. In Sabrina De Capitani di Vimercati and Paul Syverson, editors, *Workshop on Privacy in the Electronic Society – WPES*, pages 1–7, Washington, DC, USA, October 2004. ACM, ACM Press.
31. Ari Juels, Ravikanth Pappu, and Bryan Parno. Unidirectional key distribution across time and space with applications to RFID security. Cryptology ePrint Archive, Report 2008/044, 2008. Available from World Wide Web: `eprint.iacr.org/cgi-bin/cite.pl?entry=2008/044`.
32. Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In Sushil Jajodia, Vijay Atluri, and Trent Jaeger, editors, *Proceedings of the 10th ACM Conference on Computer and Communication Security*, pages 103–111, Washington, D.C., USA, 2003. ACM Press. Available from World Wide Web: `portal.acm.org/citation.cfm?id=948126&coll=Portal`.
33. Ari Juels and Stephen Weis. Authenticating pervasive devices with human protocols. In Victor Shoup, editor, *Advances in Cryptology – CRYPTO'05*, volume 3126 of *Lecture Notes in Computer Science*, pages 293–308, Santa Barbara, California, USA, August 2005. IACR, Springer.
34. Günter Karjoth and Paul A. Moskowitz. Disabling RFID tags with visible confirmation: clipped tags are silenced. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES 2005)*, pages 27–30, Alexandria, VA, USA, 2005. ACM Press.
35. Sindhu Karthikeyan and Mikhail Nesterenko. RFID security without extensive cryptography. In *Workshop on Security of Ad Hoc and Sensor Networks – SASN'05*, pages 63–67, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.
36. Alfred Kobsa and Jörg Schreck. Privacy through pseudonymity in user-adaptive systems. *ACM Transactions on Internet Technology*, 3(2):149–183, 2003.
37. Travis Kriplean, Evan Welbourne, Nodira Khoussainova, Vibhor Rastogi, Magdalena Balazinska, Gaetano Borriello, Tadayoshi Kohno, and Dan Suciu. Physical access control for captured RFID data. *Pervasive Computing, IEEE*, 6(4):48–55, Oct.-Dec. 2007.
38. Marc Langheinrich. RFID and privacy. In Milan Petkovic and Willem Jonker, editors, *Security, Privacy, and Trust in Modern Data Management*, pages 433–450. Springer, Berlin Heidelberg New York, July 2007.
39. Marc Langheinrich and Remo Marti. Practical minimalist cryptography for RFID privacy. *IEEE Systems Journal*, 1(2):115–128, December 2007. Available from World Wide Web: `www.vs.inf.ethz.ch/publ/papers/shamirtags07.pdf`.
40. Li Lu, Jinsong Han, Lei Hu, Yunhao Liu, and Lionel M. Ni. Dynamic key-updating: Privacy-preserving authentication for RFID systems. In Tom La Porta, Matt Mutka, Claudio Pinhanez, and Peter Steenkiste, editors, *Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom '07), March 19-23, 2007, White Plains, NY, USA*, pages 13–22. IEEE Press, 2007.
41. Janis Mara. Euro scheme makes money talk. *Wired News*, July 9, 2003. Available from World Wide Web: `www.wired.com/news/privacy/0,1848,59565,00.html`.
42. David Molnar, Andrea Soppera, and David Wagner. Privacy for RFID through trusted computing. In *WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 31–34, New York, NY, USA, 2005. ACM Press.
43. David Molnar, Andrea Soppera, and David Wagner. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography – SAC 2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 276–290, Kingston, Canada, August 2005. Springer.

44. David Molnar and David Wagner. Privacy and security in library RFID: Issues, practices, and architectures. In Birgit Pfitzmann and Peng Liu, editors, *Conference on Computer and Communications Security – ACM CCS*, pages 210–219, Washington, DC, USA, October 2004. ACM, ACM Press.
45. Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Cryptographic approach to "privacy-friendly" tags. In Garfinkel and Rosenberg [22]. Available from World Wide Web: `www.rfidprivacy.us/2003/papers/ohkubo.pdf`.
46. K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi. An efficient and secure RFID security method with ownership transfer. In Yiu ming Cheung, Yuping Wang, and Hailin Liu, editors, *Computational Intelligence and Security, 2006 International Conference on (CIS'06)*, volume 2, pages 1090–1095, Piscataway, NJ, November 2006. IEEE Press. Available from World Wide Web: `ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4076126`.
47. Melanie Rieback, Bruno Crispo, and Andrew 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'05*, volume 3574 of *Lecture Notes in Computer Science*, pages 184–194, Brisbane, Australia, July 2005. Springer.
48. Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. Keep on blockin' in the free world: Personal access control for low-cost RFID tags. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, *Security Protocols, 13th International Workshop, Cambridge, UK, April 20-22, 2005. Revised Selected Papers*, volume 4631 of *LNCS*, pages 51–59, Berlin Heidelberg New York, 2007. Springer. Available from World Wide Web: `www.springerlink.com/content/92407245x4432q17/`.
49. Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. The evolution of RFID security. *IEEE Pervasive Computing*, 05(1):62–69, January-March 2006.
50. Adi Shamir. How to share a secret. *Comm. of the ACM*, 22(11):612–613, 1979.
51. Sarah Spiekermann. RFID and privacy – what consumers really want and fear. *Personal and Ubiquitous Computing*, 2008. Special issue on Privacy in Ubiquitous Computing (forthcoming).
52. Sarah Spiekermann and Oliver Berthold. Maintaining privacy in RFID enabled environments – proposal for a disable-model. In Philip Robinson, Harald Vogt, and Waleed Wagealla, editors, *Privacy, Security and Trust within the Context of Pervasive Computing*, volume 780 of *Springer International Series in Engineering and Computer Science*, pages 137–146, New York, September 2005. Springer Science and Business Meida, Inc. Available from World Wide Web: `www.springerlink.com/content/w8w447l70541w075/`.
53. Thorsten Staake, Frédéric Thiesse, and Elgar Fleisch. Extending the EPC network – the potential of RFID in anti-counterfeiting. In *Proceedings of the 2005 ACM Symposium on Applied Computing*, pages 1607–1612, New York, NY, USA, 2005. ACM Press.
54. Claire Swedberg. Marnlen makes privacy-friendly tags for retail items. *RFID Journal*, November 2006. See `www.rfidjournal.com/article/articleprint/2803/-1/1/`.
55. Gene Tsudik. A family of dunces: Trivial RFID identification and authentication protocols. In Nikita Borisov and Philippe Golle, editors, *Privacy Enhancing Technologies. 7th International Symposium, PET 2007 Ottawa, Canada, June 20-22, 2007 Revised Selected Papers*, volume 4776 of *LNCS*, pages 45–61, Berlin Heidelberg New York, July 2007. Springer. Available from World Wide Web: `www.springerlink.com/content/d67454h576847p42/`.
56. Pim Tuyls and Lejla Batina. RFID-tags for anti-counterfeiting. In David Pointcheval, editor, *Topics in Cryptology – CT-RSA 2006 - The Cryptographers' Track at the RSA Conference 2006, San Jose, USA, February 13-17, 2005, Proceedings*, volume 3860 of *LNCS*, pages 115–131, Berlin Heidelberg New York, 2006. Springer. Available from World Wide Web: `www.cosic.esat.kuleuven.be/publications/article-621.pdf`.
57. Roy Want. An introduction to RFID technology. *IEEE Pervasive Computing*, 5(1):25–33, January-March 2006.
58. Stephen A. Weis, Sanjay E. Sarma, Ron L. Rivest, and Daniel W. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In Dieter Hutter, Günter Müller, Werner Stephan, and Markus Ullmann, editors, *Security in Pervasive Computing – First International Conference, Boppard, Germany, March 12–14, 2003, Revised Papers*, volume 2802 of *LNCS*, pages 201–212, Berlin Heidelberg New York, 2004. Springer. Available from World Wide Web: `www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2802`.
59. Jonathan Westhues. Hacking the prox card. In Garfinkel and Rosenberg [22], pages 291–300.
60. Alan F. Westin. *Privacy and Freedom*. Atheneum, New York, USA, 1967.