An Overview of Approaches to Privacy Protection in RFID

Jimmy Kjällman
Helsinki University of Technology
Jimmy.Kjallman@tkk.fi

Abstract

Radio Frequency Identification (RFID) is a common term for technologies using micro chips that are able to communicate over short-range radio and that can be used for identifying physical objects. RFID technology already has several application areas, and more are being envisioned all the time. While it has the potential of becoming a really ubiquitous part of the information society over time, there are many security and privacy concerns related to RFID that need to be solved. These issues have been addressed quite extensively by researchers in this field, and as a result, several protection mechanisms have been developed for different types and uses of this technology. This paper examines some of these proposed technical approaches to privacy protection in order to find out their suitability in terms of security versus utility in their proposed domains of application.

KEYWORDS: RFID, privacy

1 Introduction

Radio Frequency Identification (RFID) technology is gaining a foothold as an advanced barcode replacement, a wireless smartcard and a generic system for attaching automatically readable data to objects. Currently RFID is being used for tracking goods in supply chains, identifying vehicles in toll collection, tracking animals and storing biometric data in electronic passports – just to name a few examples. In the near future RFID tags might be commonly found on all items sold in stores and even as implants in human bodies.

Two major factors in the fast adoption of this technology that recently has taken place have been the decreasing cost and shrinking size of RFID-capable devices. Another factor that has contributed to the success of RFID is its suitability to a vast number of applications.

However, while at a glance RFID might seem like a simple technical issue, it brings about surprisingly complex problems at closer look. These problems include security and privacy concerns for corporations, consumers or other users of this technology. This paper studies some technical solutions proposed for tackling these issues, and evaluates their effectiveness as privacy protection methods compared to their impact on the usefulness of RFID, especially in a personal use context.

But first, we will give a brief primer [1] on RFID technology in section 2.1 and discuss its privacy issues in section 2.2.

[1] For more information on RFID technology, see e.g. [4] or [14].

2 Background

2.1 RFID Technology in Brief

The essential building blocks in an RFID system are called *tags* and *readers*. A tag is a very small microchip which can be used to store and wirelessly transmit identification information, such as a serial number, of the object or person that it is attached to. A reader, on the other hand, is a device that interrogates information stored in tags. In contrast to a tag, which is usually quite simple and cheap, a reader may be more complex and is often part of a larger computer system that also includes a database holding information related to tag IDs.

The general goal of RFID is to be able to automatically and uniquely identify objects using radio transmission technology. However, there are numerous different RFID implementations available that provide the means to achieve this aim. The variety of standards in this field is to some extent a natural consequence of the fact that there are so many possible domains were this kind of identification can be used, and each domain has its own constraints and requirements regarding for example cost, size, radio capabilities and data storage – as well as its own privacy issues.

One common way to categorize these different types of RFID tags is to make a distinction between *active* and *passive* tags. The latter do not have a power source of their own, but derive their energy for computing and responding from the electromagnetic signal sent by a reader. Thus they are usually smaller and cheaper than the former which do have access to battery power, that is used to enable active transmission of data.

Another method of grouping tags is to look at their cryptographic abilities. In this case, cheaper tags are usually unable to perform necessary computations for cryptographic operations, such as encryption, on their own while more expensive ones might support this kind of functionality. Naturally, this is particularly interesting in security and privacy contexts, where we aim at protecting information against illicit exploitation.

2.2 RFID Privacy Issues

A problem with RFID tags is that the identification information they hold can be used for purposes that violate a user's privacy. A person might be carrying tags for instance in clothes, medicines, books, bank notes, passports and other belongings, and if no protection mechanisms are employed, the data in these tags can be interrogated (or eavesdropped) by any reader, legitimate or not, in the physical proximity of

that person. Furthermore, the data is read in clandestine way, so that the user isn't necessarily aware of when and where it happens. This information can then be used, for example, for unauthorized tracking or inventorying purposes [7].

In tracking, static data held and transmitted by a tag (or a set of tags) can be used for keeping a record of the tag's location. If this data can be linked to the identity of a person in any way, it also makes it possible to track that person as long as the data does not change. In fact, this privacy threat can be realized even if the tag data itself does not reveal any other useful information than the ID.

Inventorying, on the other hand, requires that the tag either holds explicit information of the object it belongs to, i.e. what the object is, or that similar data can be looked up somewhere else using the tag's ID. In this way, it is possible to make an inventory of RFID-tagged items that a person carries.

In addition to the two basic threats described above, many more threats to personal privacy can be imagined based on how tags are associated with objects, individuals and the behavior of individuals (see e.g.[5]). These threats often also depend on certain social contexts. It can, for instance, be possible for sellers to use RFID information to determine a customer's product preferences, or for thieves to find out what valuable items a person is possessing. In other situations the information could perhaps be used to determine if a transaction of a product occurs between individuals, or to find out the exact location of an individual or tagged item. Drawing even further conclusions based upon item data and movement patterns provided by RFID systems, it might be possible to conclude higher level actions that a person has taken. For example, this kind of data could reveal that someone has taken possession of a number of many valuable objects in a store, or been present at a crime scene, thus hinting that the person might have committed a crime.

As a conclusion, privacy implications imposed by RFID should indeed be taken seriously, and preferably they should of course be addressed before the technology is deployed virtually everywhere. In this respect RFID has already caught some negative publicity when concerned privacy activists have expressed their objection to the use of RFID, and gone as far as to organize boycotts against companies planning to deploy it [3].

Consequently, as there is a real need to prevent future problems and to gain social and legal acceptance of this technology, many technical mechanisms have been developed in order to mitigate the privacy risks of RFID. Some of these solutions aim at restricting tag reading to be carried out only by authenticated and authorized readers or in situations where a user permits it. Others try to limit the usefulness of data read or from tags by encrypting the data on a tag or changing the identification information between interrogations.

Next, we continue to discuss privacy issues by describing how these means of privacy protection can be evaluated.

3 How to Evaluate Privacy Protection

In this paper we study and evaluate selected technical approaches to privacy protection in RFID by doing a literature review of research work in this domain. We briefly present the chosen approaches and analyze them by comparing them against defined evaluation criteria. In this way we aim at finding out information about the effectiveness and suitability for privacy protection of these methods in their central use contexts. The main evaluation criteria to be used are presented below.

3.1 Effectiveness

By effectiveness of a protection solution we mean the positive impact it has on the level of privacy when using RFID. That is, how well it actually helps in improving a user's privacy. This kind of effectiveness of course depends both on the kind of privacy the solution is intended to provide and on the situations where the solution is planned to be commonly used. In other words, a protective measure should be evaluated with regard to how well it is capable of preserving certain aspects of privacy in relation to relevant attacks in its possible contexts of use.

In this paper we do not use any formal attack model for evaluating privacy, but instead we examine privacy protection starting from the personal privacy threats, such as scanning and inventorying, presented earlier in section 2.2. In this way we explain how each examined solution affects privacy in practice when applied in its relevant social contexts. We discuss the privacy threats that a solution is successfully able to address and may point out some threats that are beyond its scope. When possible, we also give a statement on whether it is possible for an attacker to circumvent the offered protection.

3.2 Utility Impact

In addition to providing effective privacy protection, a solution might impose unwanted side-effects in the form of reduced utility compared to a situation where the solution is not employed. This implies a tradeoff between the benefits of RFID and the security and privacy offered by the solution. Thus, we have to think about the goals of RFID itself when applying this evaluation criteria. Again, those goals are highly dependent on the context where RFID is employed. We can, however, also distinguish some general characteristics that we want to preserve, like automatic, unique and wireless product identification, that we already mentioned earlier.

Properties that completely prevent taking advantage of an important RFID feature, or that complicate it, are obviously not wanted in most cases from RFID privacy protection solutions. Yet, as we shall present in section 4, some solutions are for example based on hindering all RFID functionality in tags. In this paper we examine whether such tradeoffs are reasonable or not.

One specific utility factor that often needs to be considered is the usability impact of a privacy enhancement system. For instance, if the system requires that a user has to manage passwords or cryptographic keys for a host of items, it might actually be too complex to be deployed in practice. Other factors include effects on the cost of an RFID tag and the needed support from other parts in an RFID system.

4 Approaches to Privacy Protection

Available RFID privacy protection mechanisms range from physical removal of tags to systems based public-key cryptography. Analyzing them all would be an overwhelming task, so in this paper we have chosen only three different categories to be studied and evaluated. The chosen solutions are all available for low-cost passive tags without cryptographic processing capabilities.

We begin by examining one of the most simple mechanisms, the tag deactivation approach. This method was chosen for evaluation because one particular manifestation of it, namely killing tags, is currently the most prevalent approach used in practice. We continue by studying the very different blocking approach, which shows that every RFID tag does not need to take care of its own privacy protection. Instead, separate tags can be dedicated to handle this task. Finally, we discuss tag pseudonyms, that represent yet another way of dealing with some privacy threats by making the identification data on a tag non-static.

We also present a summary of the results from the evaluation of these approaches in table 1.

4.1 Tag Deactivation

Permanent or temporary deactivation of RFID tags can be used as a very straightforward privacy protection mechanism. The basic principle behind this approach is, that when a tag is deactivated, it does not respond to any reader interrogations, thus not revealing any information of its identity or even its existence. In this subsection we examine two ways of tag deactivation: *killing* (permanent deactivation) and *sleeping* (temporary deactivation).

4.1.1 Killing

Killing is a solution to privacy issues that is employed in current Electronic Product Code (EPC) tags [1, 2]. These low-cost EPC tags are primarily used in supply chain management, but they also appear in consumer products. Killing of tags is suggested to occur at purchase time in order to protect consumer privacy [12].

Killing implies that a tag, when it receives a specified kill command, makes itself completely unusable for good. The kill command may be accompanied by a password that a tag verifies before terminating itself. This kind of deactivation is intended to be truly permanent, i.e. it must not be possible to take a killed tag back into use by any normal means.

Analysis: The killing approach is clearly very effective as a means of consumer privacy protection. It addresses both the tracking and inventorying threats presented in section 2.2, thus freeing a consumer from all concerns related to RFID after the product has been deactivated and acquired. Moreover, due to its simplicity, it is quite a cheap method as well. However, in terms of utility, matters are much worse. This is of course the case because killing RFID tags does not only eliminate the negative features of RFID, but it withdraws all the positive ones as well.

In some areas of use, such as in consumer product sales, the loss of benefits only eliminates some possible use cases, such as using RFID information when returning products or utilizing smart consumer appliances [5, 7].

In other areas, killing is not an option at all. An example where killing cannot be utilized is tagged library books, where identification is needed both at the time of borrowing and returning a book [11]. Another example is electronic passports [9], where the reading of biometric information stored on a passport is not possible unless the RFID tag is operational.

Conclusively, we state that killing tags is a rather simple and effective way of implementing post-purchase customer privacy protection while preserving pre-purchase benefits of RFID. But in many cases, this is not enough. After all, permanent deactivation of tags is of quite limited usefulness when we think about how widely RFID can be adopted.

4.1.2 Sleeping

As an attempt to overcome the problem of lost utility when a tag is killed, a simple solution would be to enable sleep and wake functionalities for RFID tags [7]. In this approach the state of being irresponsive to reader interrogation would be only temporary. First, a tag attached to, say, a consumer product could be put in to an inactive state when the product is purchased. Later, when RFID functionality is again needed at home or when returning the product, the tag could be activated. Thus, a customer's privacy would be ensured during the transport of the product.

The activation of tags should of course be allowed only to authorized readers. A tag could for example wake up only if it receives the correct passcode or key from a reader [7, 5].

Analysis: This solution offers as effective privacy protection than the killing approach, but is more flexible. The biggest problem with this solution is, that it requires the owner of an item to manage activation passwords for RFID devices [7, 5]. As a consequence, the user may have dozens of RFID tagged items in different states, in different places and possibly requiring different passwords for reading them. For an end user, this is clearly a severe usability problem.

Unless the management issues are solved, sleeping may not be an any more feasible option to use than killing. Furthermore, since a password transmitted from a reader to a tag might be caught by an eavesdropper, or even guessed by an attacker, we can see some uncertainty in the reliability of this protection scheme. Such security issues can, however, be tackled with proper countermeasures.

4.2 Blocking

Blocking is a way of forestalling a reader trying to interrogate RFID tags [10]. Blocking is implemented by specialized *blocker tags*, that prevent a reader from detecting any other nearby tags that need privacy protection. In this section, we will discuss two variations of blocking, namely "real" blocker tags and *soft blocking*.

Since blocking is in many ways a more complex subject than the other meachanisms we evaulate, we also discuss it more extensively than the other selected approaches.

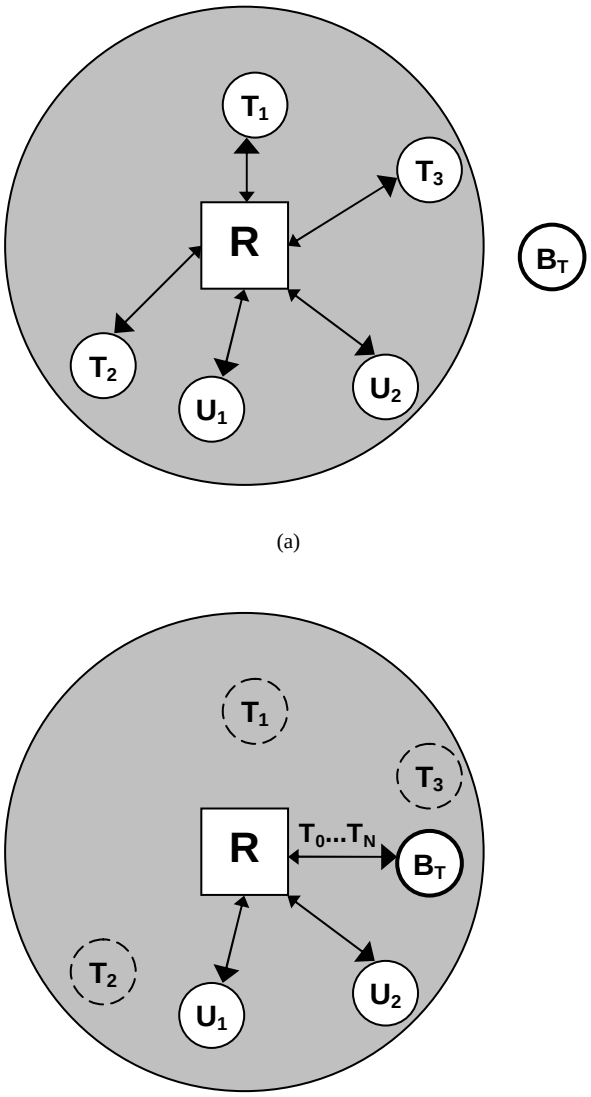

Figure 1: How the presence of a blocker tag affects the distinguishability of ordinary tags

4.2.1 Blocker Tags

A blocker tag [10] jams readers by appearing to be many tags at the same time. More precisely, it represents the IDs of all tags belonging a defined serial number spectrum. Thus, a blocker tag can be used to hide other nearby RFID tags, namely those whose IDs belong to the protected serial number space. In other words, a reader cannot distinguish real tags from the virtual IDs created by the blocker tag.

Strictly speaking, the above description does not tell how blocking usually is implemented in practice according to current proposals. Nevertheless, it suffices quite well for our privacy evaluation needs. However, we should mention that in practice, current blocker tag implementations rely on exploiting *anti-collision* protocols, also called *singulation* protocols. These protocols are normally used for allowing only one tag at a time to transmit its information to a reader. A blocker tag, on the other hand, does not follow this protocol in a standard manner. Instead, it causes a reader to see a welter of tags that are not present in reality.

In summary, we note that a blocker tag only blocks tags that are physically close to it and that belong to a specific range of IDs. The blocked ID range is called a *privacy zone*. The idea with privacy zones is that ordinary RFID tags can belong to different zones depending on their need for privacy protection. Furthermore, a tag's ID can be set to be part of a privacy zone when needed. This can be implemented by means of simple bit flipping. Such a zone change is preferably allowed only when a reader has supplied a correct password. A tag's ID could, for instance, be moved into a privacy zone reserved for consumer products at the time of purchase of a product. Then that tag could be protected by a blocker tag located on a shopping bag. In this example the blocker tag on the bag would only protect tags in the zone meant for groceries, but not necessarily other products belonging to other zones.

To further illustrate the concept of blocker tags and privacy zones, we will now discuss figure 1, which outlines two simple, two-dimensional RFID environments. First, when we look at figure 1(a) we see that the reader R can freely scan the RFID tags T_1, T_2, T_3, U_1 and U_2. The blocker tag B_T is not seen by the reader, whose scanning range is drawn in grey. Then, when we move on to figure 1(b), we see that the blocker tag B_T is put inside the reader's range. This blocker tag protects a privacy zone that we call T. Tags $T_0 \dots T_N$ belong to this zone, while tags $U_0 \dots U_N$ do not. Thus, we see that the reader is capable of scanning tags U_1 and U_2 as in figure 1(a), but not tags T_1, T_2 and T_3. The blocker tag makes the reader think that *all* tags $T_0 \dots T_N$ are present, and thus it cannot determine which tags in zone T are present and which are not.

Finally, we note that blocking may also be polite, or reader-friendly, which means that it supports mechanisms that do not cause a reader to process a blocked serial number range in vain, which would normally be the case. This is often preferable, since blocking might otherwise unnecessarily cause legitimate readers to stall. Instead, a polite blocker tag can notify readers about its presence and indicate the privacy zones it blocks, so that a reader can avoid scanning them.

Analysis: By completely preventing unauthorized reading of RFID tags, blocker tags tackle both the threats of tracking and inventorying. In this view it is an effective privacy protection mechanism. Moreover, using dedicated tags for privacy protection also gives the benefit that the tags used for actual item identification can be kept very simple. On the other hand, the blocking technology itself should not be very expensive to implement, either [10].

However, there are some negative points related to blocker tags as well. On the technical side, RFID tags need to support a privacy zone division model. These privacy zones also need to be managed in order not to overlap each other. In practice this could imply that zones, i.e. ranges of serial numbers, are issued for specific areas of use according to common, global policies. Moreover, blocker tags of one user might possibly interfere accidentally with those of others. Blocker tags are also characterized as an opt-in solution [10], which implies that users need to be privacy-aware and

have to take care of having the right blocker tags for needed zones with them themselves.

Furthermore, the reliability of blocker tags' protection is slightly questionable. The placement of a blocker tag in relation to the tags it is protecting might under some circumstances cause the privacy protection to fail [7]. In such a case we might accidentally have the situation with no protection seen in figure 1(a), when we think we have privacy as in figure 1(b). Yet another issue is, that responses of blocker tags can possibly be analyzed and distinguished from responses of other tags [13]. Thus an attacker could be able to construct a reader that does not get fooled by a blocker tag. As a result, the security provided by blocker tags in their current forms are not necessarily as strong in the future, when attacks have evolved, as they are now.

Still, we can conclude that blocker tags offer an interesting approach to RFID privacy safeguarding. Despite its shortcomings we can assume that it can be used as an option to provide privacy at least in cases where tags are incapable of doing so themselves. Blocking can perhaps also be seen as an alternative to faraday cages or other physical means, that similarly let a user choose when and where privacy protection is applied.

4.2.2 Soft Blocking

In contrast to the blocking scheme described above, soft blocking [8] does not offer any technical protection like anti-collision exploitation for RFID tags. Instead, it relies solely on notifying readers about a request not to read tags which have their privacy bits set on. In this way, it only specifies and announces a security policy that it expects well-behaving readers to check and follow. Conformance to this privacy technology can be ensured by legislation, reader auditing or even active monitoring of readers.

With soft blocking, it is possible to follow more flexible policies compared to the use of real blocker tags. An illustration of this is, that a tag defining a policy can be a so called unblocker tag, which announces that, in addition to public tags, a reader may scan also tags that are set to be private.

Analysis: When we evaluate soft blocking as a privacy protection mechanism, we need to consider two things. On one hand, soft blocking obviously offers no real protection against any threats if the attacker is "breaking the rules" – as attackers very often do. On the other hand, if readers truly follow the given policies neatly, this approach is indeed quite effective, flexible and undoubtedly cheap and easy to implement.

We can assume that most RFID readers, such as those that are found in stores, libraries, passport control points and mobile phones, will follow given regulations. Yet, it seems feasible to build customized readers that bypass the soft blocking mechanism.

Thus, while we agree that this approach seems practical due to its simplicity, we are also skeptical of whether legislators and law-enforcement authorities in reality can take the burden of actively ensuring that the privacy protection policies are not violated by illegitimate readers. Legislation can certainly support technical solutions in ensuring the privacy of users, but we suggest that for effective protection we should use mechanisms that are able to provide some level of guaranteed technical security by themselves as well. As we have mentioned, this is a property that soft blocking is lacking if applied as the only privacy solution.

4.3 Tag Pseudonyms

Tag pseudonyms [5] represent a *renaming* approach [7] to RFID privacy protection. In renaming, the identification information in a tag is made non-static mainly in order to protect against tracking. Here we have chosen to look more deeply into tag pseudonyms implemented by *minimalist cryptography*.

4.3.1 Minimalist Cryptography

In minimalist cryptography [6], a limited set of tag pseudonyms are stored on an RFID chip. These pseudo-IDs may possibly be programmable by an authorized reader, which allows IDs to be changed. When a reader interrogates a tag, that tag changes its identification information to the next pseudonym in its list, and responds with this ID. The idea here is, that an authorized reader will know all the alternative IDs and thus be able to uniquely identify the tagged item, while an adversarial reader will see different, seemingly random and unrelated IDs on every interrogation. As a security measure, the tag does not respond to consecutive interrogations immediately in order not to reveal all its pseudonyms at once to an attacker.

Minimalist cryptography was designed to be secure against a specific, quite limited adversarial model. In this model, as in the real world, an adversary has to be physically near the tag in order to get information out of it. The adversary also has to be able to track a physical item under a long period of time or during several occasions to be able to link together the tag pseudonyms belonging to that item.

An essential feature of minimalist cryptography is that as long as an adversary does not get to know the list of pseudonyms belonging to a tagged item, the protection mechanism remains reliable. This means that the list needs to be long enough and preferably it should be updated with new pseudonyms quite frequently.

Analysis: Because minimalist cryptography was designed to be secure in relation to the defined adversary model, it can of course be considered effective in real use contexts where the model is applicable. A warehouse, where a company's products are stored and transported, is an example of such a context [6]. In a warehouse RFID is also employed in a limited and controlled environment, where readers can easily share the most fresh pseudonym data between each other. Therefore, pseudonym management is not likely to present a problem in that context.

However, the adversary model can be applied to some personal use cases as well [7]. An attacker might have the opportunity to scan information on a person's tags only on occasional spots. If a tag interacts with a legitimate reader and renews its pseudonyms before the attacker sees an ID twice, then minimalist cryptography can protect the user

Table 1: Summary of evaluation results

Protection mechanism	Most important benefits	Major Disadvantages
Killing	Guaranteed protection against all threats	Loss of all RFID benefits
Sleeping	More flexible than killing	Password management problem
Blocker tags	Privacy protection in user-defined situations	Policy management, risk of unreliability
Soft blocking	More simple and flexible than real blocking	No technically enforced privacy
Minimalist cryptography	Sufficient protection against tracking	Pseudonym management, inventorying threat

against tracking. But because pseudonyms normally represent items belonging to a certain group of products that the attacker can find out [6], a user can still be the target of an inventory attack. Moreover, it seems that the distribution of pseudonyms to readers might be difficult to manage in a scenario where tags are read in various locations for different purposes, which is the case with consumer products, for instance.

In the form that the author of the minimalist cryptography originally has intended, this approach might be best suitable for protection against corporate espionage [6].

5 Conclusions

By merely scratching the surface of the wide research area of RFID privacy protection in this paper, we see that the issues to deal with are not simple. RFID technology is also in many other respects a challenging area of work, so difficulties in finding viable means to ensure privacy are understandable.

Many good solutions addressing privacy and security problems have been proposed, however. But when looking at the offered level of protection and preserved usefulness of RFID features, we cannot name one single, universal method that would clearly be the most recommended approach.

Nonetheless, we can state that the currently most widespread mechanism for protecting consumer privacy, tag killing, will not be sufficient as the only option in the future. Due to the need of preserving advantages of RFID tags over longer time periods, we need to look at alternative approaches. In this paper we studied blocking and tag pseudonyms. We suggest that blocking could be suitable for ensuring privacy in public situations, such as when carrying tagged items through a city. Tag pseudonyms, on the other hand, appear to be more at home in limited corporate environments and in cases where tracking of individual items needs to be prevented.

We conclude that the research work done in this domain has been valuable, but in order to find truly feasible and widely acceptable privacy protection schemes, further development is required. In cases where the theoretical basis is solid it is crucial to pay more attention to reliability and ease of use when the solutions are deployed in practice.

References

[1] Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag. EPCglobal, 2003. Referenced Nov 2006 at `http://www.epcglobalinc.org/standards/specs/`

[2] EPC Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID Conformance Requirements, Version 1.0.2. EPCglobal, 2004. Referenced Nov 2006 at `http://www.epcglobalinc.org/standards/specs/`

[3] EPIC RFID Privacy Page. Electronic Privacy Information Center, 2006. Referenced Nov 2006 at `http://www.epic.org/privacy/rfid/`

[4] Klaus Finkenzeller. *RFID-Handbook, 2nd edition*. Wiley & Sons, 2003.

[5] Simson Garfinkel, Ari Juels and Ravi Pappu. RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Security and Privacy*, 3(3):34–43, May-June 2005. Referenced Nov 2006 at `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1439500`

[6] Ari Juels. Minimalist Cryptography for Low-Cost RFID Tags. In *4th International Conference on Security in Communication Networks – SCN 2004*. Referenced Nov 2006 at `http://www.rsasecurity.com/rsalabs/node.asp?id=2033`

[7] Ari Juels. RFID Security and Privacy: A Research Survey. RSA Laboratories. Septemper 2005. Referenced Nov 2006 at `http://www.rsasecurity.com/rsalabs/node.asp?id=2937`

[8] Ari Juels and John Brainard. Soft Blocking: Flexible Blocker Tags on the Cheap. In *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society*, p. 1–7, ACM Press, 2004. Referenced Nov 2006 at `http://doi.acm.org/10.1145/1029179.1029181`

[9] Ari Juels, David Molnar and David Wagner. Security and Privacy Issues in E-passports. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks – SecureComm 2005*, p. 74–88, IEEE, 2005. Referenced Nov 2006 at `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1607561`

[10] Ari Juels, Ronald L. Rivest and Michael Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In *Proceedings of the 10th ACM Conference on Computer and Communications Security*, p. 103–111, ACM Press, 2003. Referenced Nov 2006 at `http://doi.acm.org/10.1145/948109.948126`

[11] David Molnar and David Wagner. Privacy and Security in Library RFID: Issues, Practices, and Architectures. In *Proceedings of the 11th ACM conference on Computer and communications security*, p. 210–219, ACM Press, 2004. Referenced Nov 2006 at `http://doi.acm.org/10.1145/1030083.1030112`

[12] Damith C. Ranasinghe, Daniel W. Engels and Peter H. Cole. Low-Cost RFID Systems: Confronting Security and Privacy. In *Auto-ID Labs Research Workshop, September 2004*. Referenced Nov 2006 at `http://www.m-lab.ch/auto-id/SwissReWorkshop/papers/LowCostRFID%2DConfrontingSecurityAndPrivacy.pdf`

[13] Melanie R. Rieback, Bruno Crispo and Andrew S. Tanenbaum. Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags In *13th International Workshop on Security Protocols, April 2005*. Referenced Nov 2006 at `http://www.rfidguardian.org/papers/sec_prot.05.pdf`

[14] Sanjay E. Sarma, Stephen A. Weis and Daniel W. Engels. RFID Systems and Security and Privacy Implications. In *4th International Workshop on Cryptographic Hardware and Embedded Systems – CHES 2002*, 2523:454–469 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 2003. Referenced Nov 2006 at `http://www.springerlink.com/content/7mdkkqvgwva88qxq/`