Uniting Legislation with RFID Privacy-Enhancing Technologies

Melanie Rieback, Bruno Crispo, Andrew S. Tanenbaum

Dept. of Computer Science
Vrije Universiteit
Amsterdam, The Netherlands

Abstract

RFID is a popular identification and automation technology with serious security and privacy threats. Legislation expounds upon the actual security and privacy needs of people in RFID-enabled environments, while technology helps to ensure legal compliance. This paper examines the main aims of RFID privacy legislation, and explains how to achieve them using RFID privacy-enhancing technologies. The discussion reveals that multiple RFID privacy-enhancing technologies must be combined and coordinated to achieve the protection of an individual. People currently do not have a tool that allows them to do this, so we suggest a unified platform called the RFID Guardian. The RFID Guardian is a mobile personal privacy platform that manages, utilizes, and integrates RFID privacy-enhancing technologies.

Keywords: Radio frequency identification, security, privacy, data protection legislation, privacy-enhancing technologies, RFID Guardian.

1 Introduction

Radio Frequency Identification (RFID) technology faces security problems that originate from a combination of technological and social factors. Therefore, in order to protect citizens' privacy in an RFID-enabled world, a potential solution needs to address both sides of the problem. Legislation is useful because it formally determines the security and privacy needs of people, and RFID privacy-enhancing technologies are useful because they confound illegal activity. The ideal solution is logically one that leverages the available technologies with an explicit focus upon fulfilling legislative requirements. Unfortunately, most current RFID security work tends to adopt either a purely technological or purely legislative point of view. This strict dichotomy of RFID security and privacy approaches is not sufficient to enforce the protection of personal civil rights in an RFID-tagged society.

This paper examines the main aims of RFID privacy legislation, and explains how we can achieve them using RFID privacy-enhancing technologies. In the process, we will closely examine the new European Union RFID Privacy and Data Protection working document, alongside many

of the most prominent RFID security and privacy technological solutions. We then suggest a new approach, called the RFID Guardian, in which RFID privacy-enhancing technologies are explicitly leveraged to achieve legislative privacy and data protection goals.

2 Introduction to RFID

Radio Frequency Identification (RFID) is a popular inductively-powered identification technology, that is used everywhere from credit cards to cow rumens. Passive RFID transponders are tiny resource-limited computers that are inductively powered by the energy of the request signal sent from RFID readers. Once the RFID tag receives enough energy to "power up" its internal electronics, the tag can decode the incoming query and produce an appropriate response by modulating the request signal using one or more subcarrier frequencies. These RFID tags can do a limited amount of processing, and have a small amount ($<$1024 bits) of storage. Semi-passive and active RFID tags require a battery for their operation, and have accordingly more functionality. RFID is useful for a variety of applications including: supply chain management, automated payment, physical access control, counterfeit prevention, smart homes and offices, animal tracking, and subdermal medical data storage.

Despite the utility of RFID automation, not everyone is happy with the proliferation of RFID tags. Privacy activists warn that pervasive RFID technology might bring unintended social consequences, much in the same way as the automobile and the television. As people start to rely on RFID technology, it will become easy to infer information about their behavior and personal tastes, by observing their use of the technology. To make matters worse, RFID transponders are also too computationally limited to support traditional security and privacy enhancing technologies. This lack of information regulation between RFID tags and RFID readers may lead to undesirable situations. One such situation is unauthorized data collection, where attackers gather illicit information by either actively issuing queries to tags or passively eavesdropping on existing tag-reader communications. Other attacks include the unwanted location tracking of people and objects (by correlating RFID tag "sightings" from different RFID readers), and RFID tag traffic analysis.

3 Examining the Solutions

We will now examine how RFID privacy-enhancing technologies can be leveraged to achieve legislatively dictated security and privacy goals.

3.1 The Contribution of Legislation

Legislation addresses the security and privacy needs of people in RFID-enabled environments. People have created informal "codes of conduct" that take inspiration from sources as varied as the

Bill of Rights[6] and the Ten Commandments[11]. There have also been formal attempts to create RFID privacy legislation in locations from the USA (California/New Mexico/Utah/Massachussets), to Japan, to the European Union. A recent example of this proposed legislation has originated from the European Union, where an advisory body called the Data Protection Working Party, issued the "Working document on data protection issues related to RFID technology"[12]. The following principles, summarized from the EU Working document, represent a typical legislative approach to RFID privacy:

1. **Visibility of RFID tags and RFID readers**

   Data subjects must be notified about the presence and usage of RFID tags and RFID readers by data controllers. (Data controllers are parties that process the back-end data collected by the RFID tags). According to Sections 4.2 and 5.2:

   > *Data controllers processing information through RFID technology must provide the following information to data subjects .. (i) the presence of RFID tags on their products or their packaging and the presence of readers* (Section 4.2) *The real time activation of RFIDs is also a piece of information to be provided to individuals that derive from the data protection Directive. So, simple techniques enabling visual indications of activation or activability states are also necessary.* (Section 5.2)

2. **Access and modification of RFID tag data**

   People have the right to access and change data on their RFID tags. According to Section 4.2:

   > *If RFID tags contain personal information as described under 3.2, individuals should be entitled to know the information contained in the tag and to make corrections using means easily accessible.*

3. **Usage of Privacy-Enhancing Technologies**

   Key information for RFID tags must be transferred to the user. This includes deactivation keys, sleep/wake keys, and cryptographic keys. Additionally, the user needs access to a nearby device that can utilize this information. According to Sections 4.2, 5.2, and 5.4:

   > *The data controller will also have to inform individuals about: (v) how to discard, disable, or remove tags from the products .. and (vi) how to exercise the right*

of access to information (Section 4.2) *The presence and nature of PET technology ... should be part of the information easily available.* (Section 5.2) *If no device enabling the individual to disable the tag is available, an individual who does not wish the tag to continue providing information on him/her will be prevented from exercising this right ... Both manufacturers and deployers of RFID technology should ensure that such operation of disabling the tag is easy to carry out.*(Section 5.4)

4. **Visibility of High-Level Query Details**

RFID deployments must provide high-level information to the user, such as the identity of the RFID data controller or why the data is collected. According to Section 4.2:

> *Data controllers processing information through RFID technology must provide the following information to data subjects: identity of the controller, the purposes of the processing as well as, among others information on the recipients of the data ...*

5. **Consent Withdrawal**

A user may choose to withdraw consent for RFID-based data collection. Considerations for withdrawal may include data collection purposes, the identity of the data controller, or any other arbitrary personal context. In order to revoke consent, people need the technological means to access the PETs on their RFID tags at will. According to Section 5.4:

> *Individuals can always withdraw their consent to the processing of personal data (ex. Article 7 a).*

6. **Confidentiality of Personal Data**

Personal data on RFID tags should reside in encrypted form on an RFID tag. This encryption can be performed by on-tag or off-tag cryptographic mechanisms. According to Section 5.5:

> *When RFID tags contain personal data, pursuant to Article 17 of the data protection Directive, they must have embedded technical measures to prevent unauthorised disclosure of the data ... Such measures are also necessary ex Art. 6.1.d of the data protection Directive to ensure the integrity of the data stored in the tag,*

thus avoiding unauthorised changes.

3.2 The Contribution of Technology

Even lawmakers emphasize that technological solutions are essential to uphold people's RFID privacy rights. Sections 4.2 and 5 of the European Union "Working document on data protection issues related to RFID technology"[12] state:

> *Technology may play a key role in ensuring compliance with the data protection principles ...* (Section 5) *Manufacturers have a direct responsibility in ensuring that privacy compliant technology exists to help data controllers carry out their obligations under the data protection Directive and to facilitate the exercise of an individual's rights* (Section 4.2).

Using technology to uphold the principles dictated by privacy legislation requires a mixed toolkit of general RFID technology, general security techniques, and RFID-specific privacy-enhancing technologies. The following discussion examines the technological tools necessary to implement each of the EU privacy principles:

1. **Visibility of RFID tags and RFID readers**

   Compliant RFID deployments might use signposting to convey the presence of RFID tags and RFID readers to the public. However, this "privacy mechanism" is very easy to thwart, so people would profit from having their own technological means of discovering the RFID tags and RFID readers around them. RFID tags can be discovered and managed using a portable RFID reader (ex. RFID-enabled mobile phone). People can also discover RFID readers by observing nearby RFID scanning activity, perhaps using a device like *c't* magazine's RFID detector.[1]

2. **Access and modification of RFID tag data**

   Accessing and changing the personal data on RFID tags requires the use of a trusted RFID reader in the vicinity of the RFID tags in question. (Portable RFID readers ensure the availablility of a trusted RFID reader.) Additionally, this access may require the knowledge of any encryption or authentication keys that a crypto-enabled RFID tag might use. This makes key management an important issue.

3. **Usage of Privacy-Enhancing Technologies**

   Upon purchase of RFID-tagged goods, all of the information relating to the RFID tags must be transferred to the user. This includes the information about privacy-enhancing technologies, like deactivation keys, sleep/wake keys, and cryptographic keys. This key transfer must be performed in such a way that the information becomes accessable to a nearby trusted RFID reader for subsequent use with the newly purchased RFID tags. The key transfer between the new and old owners of an RFID tag could use either non-RFID infrastructure (ex. paper, Bluetooth, WiFi), or in-band RFID communications to send the relevant information.

4. **Visibility of High-Level Query Details**

   Compliant RFID deployments will provide honest statements of identity and collection purpose to consumers. However, just in case the RFID deployment is not honest, the consumer would like a way to verify the truth of this passed information. The identity of the data controller or system deployer can be confirmed through the use of an authentication protocol with the consumer. Since people generally are not good at performing cryptography, a trusted portable computer might perform the authentication protocol on the behalf of the consumer. It is not yet evident how other passed information, like the collection purpose, can be verified. This exchange of high-level information between the consumer and RFID deployer could use either non-RFID infrastructure (ex. paper, Bluetooth, WiFi), or in-band RFID communications.

5. **Consent Withdrawal**

   If a consumer withdraws his or her consent for RFID-based data collection, on-tag access control primitives like tag killing[2], sleep/wake modes, hash locks[14], and pseudonyms[9] are all useful for cutting off access to the tag. In order to activate these on-tag primitives, people need to be able to access their own RFID tags, using a trusted RFID reader. Off-tag access control primitives like RFID blocker tags[10] are also a useful way to revoke access to low-cost RFID tags. Since a person may withdraw and reinstate consent on a moment's notice, tag access control and authentication mechanisms should support dynamic security policies, which can adapt to the consumer's situation by leveraging some kind of context awareness.

6. **Confidentiality of Personal Data**

RFID tag data can be encrypted by using on-tag cryptographic mechanisms, like stream ciphers[5] or low-power variants of symmetric-key algorithms (like reduced AES[4]) or public-key algorithms (like reduced NTRU[7]). Tag data can also be encrypted by using an off-tag mechanism like external re-encryption[8], which is especially useful for low-cost RFID tags. Both kinds of encryption mechanisms require key management, and the presence of a trusted RFID reader to carry out cryptographic operations on the behalf of the user.

4 An Integrated Solution

To adequately address the privacy and data protection issues raised by RFID Legislation, about 20 separate technological tools were necessary, which are summarized by Table 1.

Type of Tool	Specific Instances
Hardware	Portable computer, portable RFID reader, RFID detector[1]
Security Administration	Key management / key transfer, dynamic security policies
Communications	Out-of-band (paper, Bluetooth, WiFi), in-band (RFID)
On-tag authentication	Lightweight authentication protocols[13],[3]
On-tag access-control	Tag killing[2], sleep/wake modes, hash locks[14], pseudonyms[9]
Off-tag access control	Blocker tag[10]
On-tag cryptography	Stream ciphers[5], reduced AES[4], reduced NTRU[7]
Off-tag cryptography	Universal re-encryption[8]
Other	Context awareness

Table 1: RFID Technological Tools

Technological solutions need to be harnessed in a coordinated fashion, so people can take advantage of the mechanisms' complementary strengths and weaknessess. However, the heart of the problem lies in the fact that people currently have no means to coordinate the usage of so many technological tools and PETs at once. The consumer would benefit from a having single unified platform that can leverage and coordinate all of these separate tools. Additionally some of the necessary functionality, like key management/transfer and dynamic security policies, still have not been developed yet for the realm of RFID, and a unified RFID-privacy platform would provide the best starting point for implementing such functionality.

4.1 The RFID Guardian

The RFID Guardian is a platform that offers centralized RFID security and privacy management for people. The RFID Guardian integrates RFID privacy-enhancing technologies, and leverages their complementary strengths and weaknessess to ultimately protect people. The idea is that consumers who want to enjoy the benefits of RFID-tagging, while still protecting their privacy, can carry a battery-powered mobile device that monitors and regulates their RFID usage. The RFID Guardian is meant for *personal use*; it manages the RFID tags within physical proximity of a person (as opposed to managing RFID tags owned by the person, that are left at home). For this reason, the operating range of the RFID Guardian must extend at least from the head to toe of the user; a radius of 1-2 meters should be sufficient. This full-body coverage requires the RFID Guardian to be *portable*. It should be PDA-sized, or better yet, could be integrated into a handheld computer or cellphone. The RFID Guardian could then occupy a vacant shirt pocket, handbag, or belt loop, and thus remain close to the person that it is supposed to protect. The RFID Guardian is also *battery powered*. This is necessary to perform resource-intensive security protocols, such as authentication and access control, which would not be possible if the RFID Guardian was implemented on a passive device, like an RFID tag. The RFID Guardian also performs *2-way RFID communications*. It acts like an RFID reader, querying tags and decoding the tag responses. But far more interestingly, the RFID Guardian can also emulate an RFID tag, allowing it to perform direct in-band communications with other RFID readers. This tag emulation capability allows the RFID Guardian to perform security protocols directly with RFID readers. The major functions provided by the RFID Guardian are *auditing*, *key management*, *access control*, and *authentication*. More detail on each of these functions will be provided in a future paper.

5 Conclusion

Legislation is necessary to codify the actual needs of people in RFID-enabled environments, but technology is necessary ensure legal compliance. To uphold the legislation, RFID privacy-enhancing technologies must be combined and coordinated to achieve a single end – the protection of an individual. People currently do not have a tool that allows them to do this, so we suggest a unified platform called the RFID Guardian. The RFID Guardian is a mobile personal privacy platform that integrates RFID privacy-enhancing technologies, and leverages their complementary strengths and weaknessess to ultimately protect people. Our future work involves the further design and prototyping of the RFID Guardian.

References

[1] c't magazine, *Bauanleitung fur einen simplen rfid-detektor*, (2004), no. 9.

[2] EPCglobal, *13.56 MHz ISM band class 1 radio frequency (RF) identification tag interface specification*.

[3] Martin Feldhofer, *An authentication protocol in a security layer for RFID smart tags*, Proc. 12th IEEE Mediterranean Electrotechnical Conf., May 2004, pp. 759–762.

[4] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, *Strong authentication for RFID systems using the AES algorithm*, Workshop on Cryptographic Hardware and Embedded Systems, LNCS, vol. 3156, Aug 2004, pp. 357–370.

[5] Klaus Finkenzeller, *RFID Handbook: Fundamentals and applications in contactless smart cards and identification*, John Wiley & Sons, Ltd., 2003.

[6] Simson Garfinkel, *An RFID bill of rights*, Technology Review (2002), 35.

[7] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, *State of the art in public-key cryptography for wireless sensor networks*, Proc. of 2nd IEEE Intl. Workshop on Pervasive Computing and Communication Security, 2005.

[8] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, *Universal re-encryption for mixnets*, Proc. of 2004 RSA Conference, 2004.

[9] Ari Juels, *Minimalist cryptography for low-cost RFID tags*, Proc. 4th Intl. Conf. on Security in Communication Networks, LNCS, September 2004.

[10] Ari Juels, Ronald L. Rivest, and Michael Szydlo, *The blocker tag: Selective blocking of rfid tags for consumer privacy*, Proc. of the 10th ACM Conf. on Computer and Commun. Security, ACM Press, 2003.

[11] Rakesh Kumar, *Interaction of RFID technology and public policy*, RFID Privacy Workshop, November 2003.

[12] Peter Schaar, *Working document on data protection issues related to RFID technology*, Working Document Article 29 - 10107/05/EN, European Union Data Protection Working Party, January 2005.

[13] István Vajda and Levente Buttyán, *Lightweight authentication protocols for low-cost RFID tags*, 2nd Workshop on Security in Ubiquitous Computing, October 2003.

[14] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, *Security and privacy aspects of low-cost radio frequency identification systems*, Security in Pervasive Computing, LNCS, vol. 2802, 2004, pp. 201–212.