AUTO–ID LABS

Making Radio Frequency Identification Visible – A Watchdog Tag

Christian Metzger, Christian Flörkemeier, Philippe Bourquin, Elgar Fleisch

Auto-ID Labs White Paper WP-HARDWARE-037

Christian Metzger
Senior Researcher
ETH Zurich

Christian Flörkemeier
Senior Researcher
ETH Zurich

Philippe Bourquin
Student
ETH Zurich

Elgar Fleisch
Research Director
Co-Chair of Auto-ID Labs
University of St.Gallen and ETH Zurich

Contact:

Auto-ID Labs ETH Zurich/St.Gallen
Swiss Federal Institute of Technology (ETH) Zurich
Department of Management, Technology and Economics
Kreuzplatz 5
8032 Zurich
Switzerland

Phone: +41 44 632 83 45
Fax: +41 44 632 10 45

E-Mail: cmetzger@ethz.ch

Internet: www.autoidlabs.org

Hardware

Index

Abstract

To address the privacy concerns associated with RFID, previous work proposed an approach, where RFID readers do not only broadcast commands to inventory tag populations, but also transmit meta-information that describe the ongoing data collection. It was argued that RFID readers should explicitly declare the scope and purpose of their tag data collection by making this meta-information available to consumers and regulators through a watchdog tag. In this paper, we present the prototype of such a watchdog tag that is capable of decoding and displaying the meta-information broadcasted over the RFID communication channel for the visual inspection by the user. The paper details the design and implementation with discrete components, but also discusses limitations and future improvements. Our watchdog tag operates reliably and therefore, it suggests potential to enhance one's control over the data collected by RFID readers.

1. Introduction

When Mark Weiser envisioned that computing devices will be embedded everywhere in the environment in a way that they can operate unobtrusively, he also acknowledged that the invisible nature of those devices will make it difficult to know the entities that are in control, the network connections among devices, and the locations where information is collected [12]. The antagonism between the requirements for control and privacy on the one hand and usability and performance on the other is well illustrated by the privacy concerns associated with the deployment of RFID technology in supermarkets and retail outlets [10].

In [4], Floerkemeier et al. present an approach that addresses these privacy concerns by integrating a subset of the widely accepted fair information principles [8] into the communication protocols between RFID readers and tags. The authors contend that having RFID readers to explicitly declare the scope and purpose of their tag data collection, as well as disclosing the identity of their operators, will allow both consumers and regulators to better assess and control the effects of everyday RFID encounters. To display and log the meta-information, which is broadcasted over the RFID communication channel, the authors present the concept of a watchdog tag that allows privacy-concerned individuals to judge whether a particular RFID reader deployment complies with the corresponding regulations.

In that paper, the concept of a watchdog tag is only demonstrated on a PDA, which receives the meta-information about the ongoing data collection via a wireless LAN connection. The main contribution of this paper is a battery-powered watchdog tag that is capable of decoding and displaying the meta-information transmitted by the reader over the RFID communication channel. We believe that this prototype represents the first step towards a user study, which evaluates the concepts proposed in [1] and compares the suitability of the watchdog tag to

other privacy enhancing techniques such as disabling the tag or blocking the tag-to-reader communication.

This paper is organized as follows: In the next section, we review and summarize the privacy-enhancing technology proposed by Floerkemeier et al. In Section 3, we present the design and implementation of our watchdog tag; and before we conclude in Section 6, we discuss the limitations of our design and compare it to already existing approaches.

2. Scanning for a purpose – Integrating the Fair Information Practices into RFID protocols

Passive high frequency tags, which operate at 13.56MHz, are widely used to equip products in the consumer goods industry because of their small form factor, low cost, and resistance against interference. With the high adoption rate of RFID tags in the consumer goods industry, customers are more and more likely to carry around items that are equipped with RFID tags. These tags continue to respond to inventory scans of RFID readers even after purchase; mostly without the awareness of the consumer.

Current RFID readers neither offer identification nor do they provide information about the purpose of the interrogation. Even though such an anonymous scan allows for high performance by keeping the exchanged data to a minimum, it does not satisfy the principles of openness and accountability. To meet the requirements by the fair information policy, Floerkemeier et al. suggest including a unique reader policy ID along with a purpose declaration and collection type into the inventory command of a reader (Figure 1).

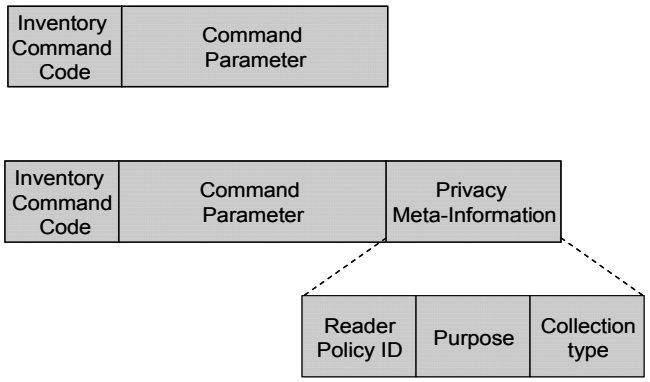

Figure 1: The figure shows the existing inventory command (above) and the proposed command extensions (below).

We incorporate these recommendations into our watchdog design. In order to test the design, however, we do not modify the existing reader protocol to avoid firmware updates. Instead, we include the reader policy ID, the purpose declaration, and the collection type in the data fields of the write command. The watchdog tag does not execute this write command but extracts the meta-information and reports it on a display for the user's interest (Figure 4). However, current passive tags do not provide interfaces for additional devices, and therefore, we built our own passive RFID tag with discrete components that allow attaching a display.

In the following, we describe the design of our watchdog tag, the analog front-end, the implementation of the air interface protocol on a microcontroller, and the integration of the display.

3. Watchdog Tag: System Design and Implementation

The watchdog tag consists of five components: a coil to pick up the reader signal, an analog front-end to demodulate the data transmitted by the reader, a logic unit to interpret the demodulated data, a display to make the meta-information accessible to the user, and an external power supply e.g. a battery (Figure 3). In the following subsections, we give an in-detail description of these components and elucidate the implementation of a watchdog tag that makes the RFID process more visible. We start with the analog front-end that decodes the reader signal.

3.1. Analog front-end to demodulate reader signals

Our watchdog tag implements the widely used ICODE1 communication protocol, which was originally developed by Philips. The ICODE1 protocol operates at 13.56 MHz. It is a reader-talks-first protocol, which uses amplitude modulation and pulse position coding on the reader-to-tag communication channel. The protocol uses a modulation index of 10% and, in standard mode, data is transmitted according the '1 out of 256' pulse position scheme. The value of the transmitted byte is thus encoded in the position of the pulse, which is set to one of 256 possible consecutive positions (Figure 2). The data transmission is preceded by a start pulse of 9.44µs, which signals the demodulator of the RFID tag that a new sequence of data is sent. The demodulator on the tag determines the bit position by measuring the elapsed time between the start pulse and the next detected pulse. Each bit has a length of 18.88µs. The division of the measured time by the sequence of one bit results in the exact bit position and allows decoding the value of the byte. The transmission of a single byte (excluding the start bit) requires 4.833ms. Hence, the transmission of an entire RFID reader command, which consists of 8 consecutive bytes, takes 38.7ms.

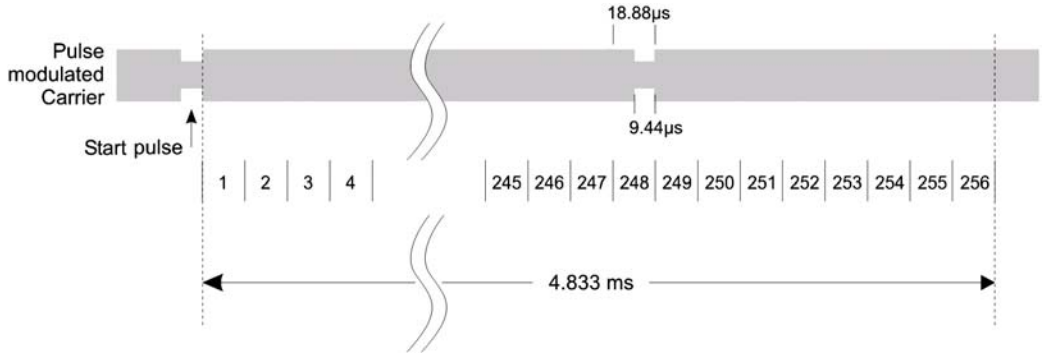

Figure 2: The value of a transmitted byte is encoded in the 256 possible consecutive positions for a pulse [9].

The analog front-end on the tag consist of an envelop detector to identify relative changes in amplitude, which is a representation for modulated bits. However, amplitude variations can also be caused by changes in the coupling between a reader and a tag coil (e.g. tilting of the tag or a change in the distance to the reader). In order to distinguish variations that are due to data transmission from those that are caused by changes in coupling, the output of the envelop detector is compared to a relative reference voltage. The reference voltage reflects variations in distance and orientation but its time constant is chosen so that the voltage remains unaffected by short pulses. Both, the envelop signal and the reference voltage are extracted by two RC filter elements (Figure 3). The RC elements are designed to meet the specifications of the ICODE1 air interface protocol with a 10% amplitude modulation and a signal drop of 9.44µs for the modulated signal as well as the negative peak clipping, which is caused by the half-wave rectification.

The two signals are compared by an operational amplifier element, which generates a binary output based on the detection of a modulated signal. The output goes low as long as the signal is modulated and remains high otherwise (Figure 3).

3.2. Logic unit

A PIC16F88 microcontroller that runs internally at 5MHz forms the core of the watchdog tag system. The clock is not obtained from the carrier signal of the RFID reader but from an external oscillator, which is used to avoid building a clock extractor.

The PIC16F88 microcontroller offers two different methods to listen for changes on the comparator's output – polling and interrupts. While polling proved inadequate because it does not meet the timing constraints for the detection of two consecutive pulses, the interrupt-based approach performs well. The asynchronous interrupt is triggered by a falling edge at the comparator's output. When an interrupt occurs, the interrupt dispatcher reads the value of the timer, which was started after the detection of the start bit. This allows determining the byte transmitted by the reader. After the detection of 8 consecutive bytes, the main routine in the microcontroller code starts decoding the complete command.

The most restrictive time constraints occur when a pulse is sent in the first slot. This pulse follows 18.88µs after the falling edge of the start pulse. The detection of each pulse triggers an interrupt, which is used to measure the elapsed time between consecutive pulses. However, the processing of an interrupt must be completed before the next pulse can be detected. This sets an upper time limit for interrupt processing of 18.88µs. Our optimized interrupt dispatcher requires 77 clock cycles, which corresponds to 15.4µs. Hence, our design fulfills even the most restrictive time constraints

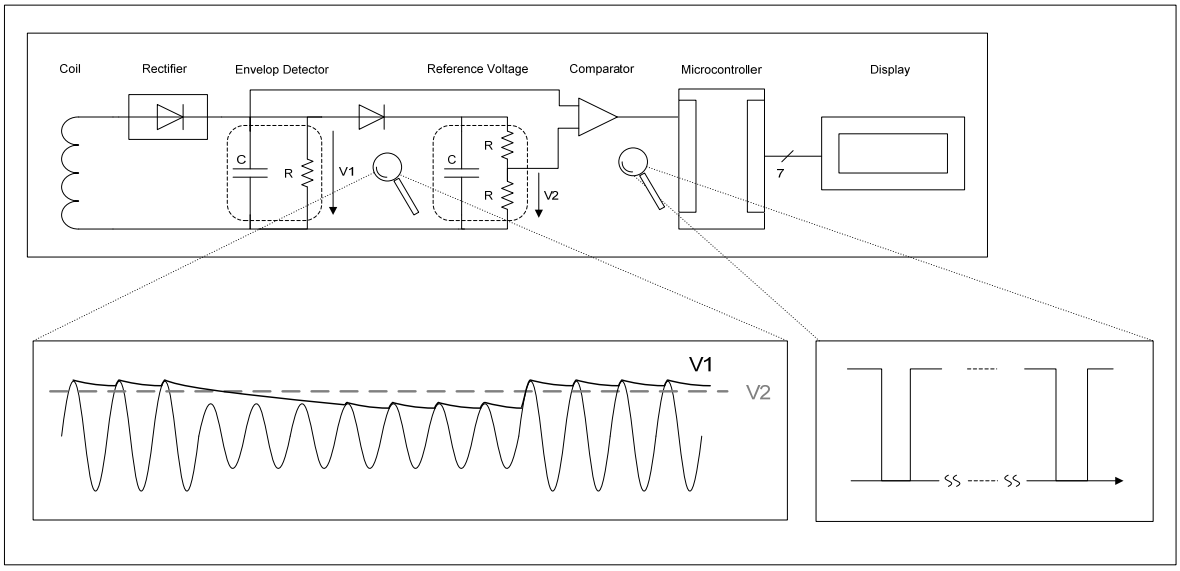

Figure 3: The schematic represents the analog front-end and shows the signals for the envelop detector and the reference voltage before and after the comparator.

3.3. Display

Our watchdog tag incorporates a dot-matrix display that contains a HD44780 controller. The controller allows addressing 2 lines, on which 20 characters each can be displayed (Figure 4). The LCD display consumes about 2mW. Therefore, it is unrealistic to build a passive watchdog tag that harvests all its energy from the magnetic field of the reader and operates at ordinary distances rather than at very close proximity to the RFID reader.

For everyday use, however, a watchdog tag should be incorporated into a cellular phone, which already contains a battery and a high resolution display. This would also allow translating reader identifiers into more meaningful information about the operator using the long-range communication capabilities as mentioned in [1].

Figure 4: The display of the watchdog tag shows the decoded reader policy ID.

4. Discussion and Future Work

In vicinity of the reader, our watchdog tag successfully decodes the meta-information included in the modified write command of an ICODE1-compliant RFID reader. The tag reports the reader policy ID, the purpose declaration, and the collection type on a display for the inspection by the user. It is desirable that a watchdog tag achieves a longer read range than ordinary passive tags, which may be attached to items a user carries along. Thus, the watchdog tag would not miss any inquires made by a RFID reader even if the watchdog tag is further away from the reader than the other tags. Situations where the watchdog tag is not in direct vicinity to the other tags may occur when a user carries its watchdog tag as a separate device or integrated in a cellular phone in her/his pocket and carries a bag with purchased items in a shopping bag.

Our current design successfully detects commands up to 87% of the reading distance of an ordinary tag with a coil of the same dimensions. However, our battery-equipped tag does not extract energy from the field of the reader to power the logic parts, and therefore, a further optimization of the analog front-end would lead to significantly longer read ranges.

Currently, the watchdog tag only incorporates the ICODE1 air interface protocol. However, to provide visibility to all RFID reader requests at high frequency, we intend to also integrate the ISO 15693 protocol. Furthermore, we will build watchdog tags that operate at low and ultra high frequency to offer complete coverage of all RFID frequencies.

Once the above modifications to our watchdog tag have been made, we aim at using the device in a user study, where we compare this privacy enhancing technology against other approaches, such as killing and temporarily silencing the RFID tag.

5. Related Work

As mentioned earlier, there is a large variety on privacy enhancing technologies available. This includes concepts that rely on disabling the tags permanently [2] [7] or at least temporarily [3], but also approaches that block the tag-to-reader communication [6]. In this paper, we focus exclusively on the technique proposed by Floerkemeier et al. [4].

There have also been other efforts to decode RFID reader commands and to reply to the reader with data. In [5], Ignatov describes an elegant way to build an LF tag with a PIC microcontroller that requires very few discrete components. Carluccio et al. developed an RFID reader command detector that works based on the ISO 14443 protocol, which is primarily used for contact-less smartcards [1]. However, their implementation uses a ready-made analog front-end transceiver chip that demodulates and decodes the reader data. Unfortunately, there is no such chip available for the long range HF protocols, such as ICODE1 and ISO 15693. At UHF, Smith et al. recently presented the WISP platform that emulates an EPCglobal Generation1 Class 1 tag [11], but features additional sensors, such as a light sensors. The WISP platform operates without an additional battery to power the microcontroller.

The work presented in this paper focuses on HF RFID systems that are used for item-level tracking. Since we attached a power-consuming display, our watchdog tag requires a battery and cannot operate passively.

6. Conclusions

We presented the design and implementation of a high frequency battery-powered watchdog tag that provides transparency to RFID reader requests by incorporating the fair information practices. The tag decodes and extracts reader policy ID, purpose of data collection, and collection type from a reader command, which is transmitted over the RFID communication channel according to the ICODE1 air interface protocol. To avoid updates to the RFID readers' firmware due to the extension of the RFID reader protocol, the meta-information is included in the data fields of the write command. This meta-information is made available on a display for the user's inspection. In order to provide an interface to attach a display to the tag; we built a watchdog tag with discrete components. The watchdog tag reliably detects and interprets the commands and shows decent read ranges. Therefore, it suggests potential to increase one's control over its RFID data.

References

[1] D. Carluccio, T. Kasper, C. Paar, “Implementation Details of a Multi Purpose ISO 14443 RFID-Tool”, Workshop on RFID Security 2006, Austria, 2006.

[2] EPCglobal Tag Data Standards Version 1.3, March, 2006.

[3] B. Fabian, O. Günther, S. Spiekermann, “Security analysis of object name service for RFID. Proc. of the 1st Int. Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, July, 2005.

[4] C. Floerkemeier, R. Schneider, M. Langheinrich, “Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols”, 2nd Int. Symposium on Ubiquitous Computing Systems UCS 2004, Japan, 2004.

[5] I. M. Ignatov, Microchip Application Note DS40160A/3, 1997.

[6] A. Juels, R.L. Rivest, “The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy”. 10th Annual ACM CCS 2003, 2003.

[7] G. Karjoth, P.A. Moskowitz, “Disabling RFID tags with visible confirmation: clipped tags are silenced”, Workshop on Privacy in the Electronic Society (WPES), pp. 27-30, ACM, 2005.

[8] Organisation for Economic Co-operation and Development (OECD). Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. September, 1980.

[9] Philips Semiconductor, “I-CODE1 System Design Guide”,www.semiconductors.philips.com/acrobat_download/other/identification/SL048611.pdf, 2002.

[10] Privacy Rights Clearinghouse, Position Statement on the Use of RFID on Consumer Goods, www.privacyrights.org/ar/rfidposition.htm, 2003.

[11] J. Smith, A. Sample, P. Powledge, S. Roy, A. Mamishev, “A wirelessly-powered platform for sensing and computation”, Proc 8th Int. Conference on Ubiquitous Computing, USA, 2006.

[12] M. Weiser, R. Gold, J.S. Brown, “The origins of ubiquitous computing research at PARC in the late 1980s”, IBM Systems Journal, 1999, pp. 693-696.