Visible and Controllable RFID Tags

Nicolai Marquardt
Dept. of Computer Science
University of Calgary
2500 University Dr NW
Calgary, T2N 1N4, Canada
nicolai.marquardt@ucalgary.ca

Alex S. Taylor
Microsoft Research
7 J J Thomson Avenue
Cambridge, CB3 0FB, UK
ast@microsoft.com

Nicolas Villar
Microsoft Research
7 J J Thomson Avenue
Cambridge, CB3 0FB, UK
nvillar@microsoft.com

Saul Greenberg
Dept. of Computer Science
University of Calgary
2500 University Dr NW
Calgary, T2N 1N4, Canada
saul.greenberg@ucalgary.ca

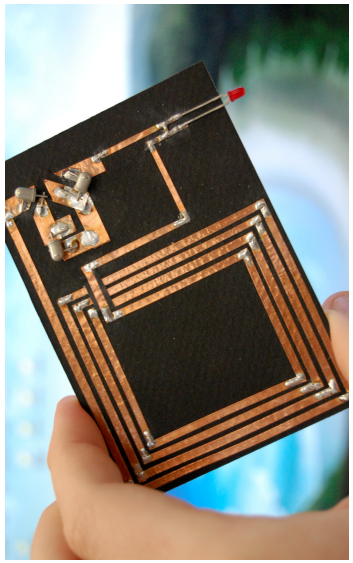

Figure 1. Alternative RFID tag designs that make RFID technology visible and controllable.

CHI 2010, April 10–15, 2010, Atlanta, Georgia, USA.
ACM 978-1-60558-930-5/10/04.

Abstract
Radio frequency identification (RFID) tags containing privacy-sensitive information are increasingly embedded into personal documents (e.g., passports and driver's licenses). The problem is that people are often unaware of the security and privacy risks associated with RFID, likely because the technology remains largely invisible and uncontrollable for the individual. To mitigate this problem, we developed a collection of novel yet simple and inexpensive alternative tag designs to make RFID visible and controllable. This video and demonstration illustrates these designs. For awareness, our tags provide visual, audible, or tactile feedback when in the range of an RFID reader. For control, people can allow or disallow access to the information on the tag by how they touch, orient, move, press, or illuminate the tag (for example, Figure 1 shows a tilt-sensitive RFID tag).

Keywords
RFID, privacy, awareness, feedback, control, sensors

ACM Classification Keywords
H.5.2 Information interfaces and presentation: User Interfaces; C.2.1 Network Architecture and Design: Wireless Communication.

General Terms
Human Factors, Security

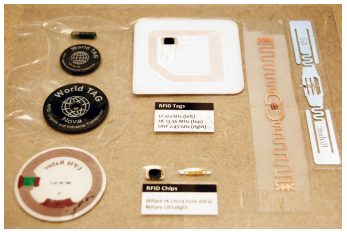

Figure 2. RFID tags in various form factors: stickers, labels, chips, cards.

Figure 3. Passport containing RFID tag (indicated by the symbol at the bottom).

Introduction and Motivation

Since its invention in the early 20th century, radio frequency identification (RFID) technology has been commonly used in many settings. Examples include commercial applications such as inventory control and supply chain management [2] (see example tags in Figure 2). In recent years, RFID tags are increasingly being used in cards and documents containing privacy-sensitive personal information, e.g., in passports, credit cards, and enhanced drivers' licences [5,7] (e.g., Figure 3). People, however, are often unaware of security and privacy risks associated with RFID, such as tracking people's location, eavesdropping on communications between tags and readers, and cloning and misuse of data stored on tags (e.g., [4,7,8]). While countermeasures exist to protect the private information stored on tags (e.g., encryption and authentication systems [3,12]), people have difficulties in applying these security mechanisms or understanding their functionality. In addition, people tend to have an incomplete or incorrect mental model of how RFID works (e.g., large reading distances, or the always-on characteristic of tags) [6,9,11]. All of these factors contribute to people's concerns and fears when using RFID-enabled documents and cards [9,11]. As such, RFID technology remains largely invisible and uncontrollable for the individual.

To mitigate this problem and to make RFID technology *visible* and *controllable* for the individual, we developed a collection of alternative tag designs. This paper and video summarize how these tags and their privacy-enhancing mechanisms work. The following two sections discuss how we achieve our goal of making RFID visible and controllable.

Making RFID Activity Visible

To give people feedback of RFID activity we designed three tags, each presenting a different type of feedback: *visual*, *audible*, or *tactile* feedback.

Our *visual feedback* RFID tag (Figure 4, top) includes a light-emitting diode (LED) that lights up when the tag is in the range of an RFID reader. At this distance to a tag, the reader can potentially read the tag's content. This awareness mechanism proved very easy to implement, especially because energy harvesting suffices to power the LED. While simple, this is already a powerful method for end-users to verify tag activity, to estimate maximum reading distances (by exploring the distance to and from a reader), and to discover invisible (perhaps unauthorized) readers. Visual feedback, however, is limited to cases when the user is actually looking at the tag; feedback would be hidden if the tag were (say) in one's pocket, purse or wallet.

The *audible feedback* and *tactile feedback* RFID tags overcome this limitation. The underlying mechanisms are similar to the previous tag. The audible feedback tag uses a small piezzo speaker to generate an acoustic signal (Figure 4, centre), while the *tactile feedback* tag uses a vibro-tactile motor connected to the tag that vibrates whenever a reader is nearby (Figure 4, bottom). This comes at a cost. Both the speaker and the motor need more electric energy than induced by the reader. Thus a small battery connected to the tag provides auxiliary power (this tag design is commonly described as *semi-passive*). Indeed, a semi-passive design allows us to replace the piezzo speaker or vibro-tactile motor with a variety of other actuators (e.g., larger displays showing more details).

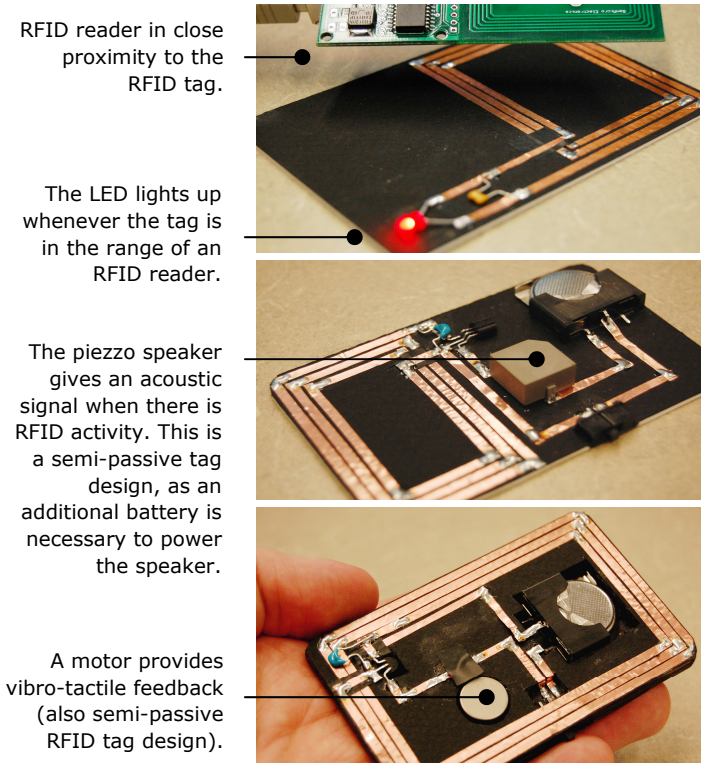

Figure 4. Feedback about RFID activity: LED light indicator, acoustic piezzo speaker, vibro-tactile feedback (from top to bottom).

In summary, the easy to understand feedback mechanisms about ongoing RFID activity provided by these three prototype tags counters the invisibility of traditional RFID tags. These feedback mechanisms – especially the LED example – are easy to implement and are reasonably cheap.

Controllable RFID Tags

We were also motivated to make the usually uncontrollable reading of a tag and its information controllable by an end user. We introduce several concepts of how simple control mechanisms can be integrated into RFID tag designs. The basic approach physically separates the antenna from the RFID chip, where the connection between the two is controlled by a particular mechanism. This makes it possible to limit the transmission activity of RFID tag information unless a specific condition is met.

Explicit Control

Our first group of examples integrate an on-off switch into the RFID tag. Thus an individual can use the switch to explicitly allow or disallow communication between the RFID tag and nearby readers. By using a *toggle switch* with two permanent positions a person can permanently activate or deactivate a tag (Figure 5.1). Integrating a *pushbutton* lets a person temporarily activate a tag while the button is pressed (Figure 5.2). Other switch designs provide variations. Our *pressure-sensitive RFID tag* is activated when a person applies pressure (e.g., by pressing fingers together) to a specific area on the tag (Figure 5.3). The *touch-sensitive RFID tag* is activated once a person touches large metal contacts on the tag with a finger or hand (Figure 5.4).

Implicit Control

Tag activity state can also depend on implicitly sensed properties [13] rather than explicit actions. We illustrate two RFID tag examples: *tilt-sensitive* and *light sensitive*. The *tilt-sensitive tag* (Figure 5.5) is activated when in a horizontal position, and deactivated otherwise. Tilt switches that are connected in series and arranged in a specific pattern close the contact between the antenna and RFID chip depending on the tag's position. The *light-sensitive tag* is activated in normal daylight and deactivated in darkness (Figure 5.6). Here, a photo transistor connected to a circuit measures the surrounding light, and activates the RFID chip only if the light is above a (changeable) threshold. This design affords RFID tags that are disabled when stored (e.g., a wallet, pocket, bag) but activated when brought outside for use. Thus unauthorized reading of the tag is inhibited.

Proximity-dependent Control

In general, RFID tags are built to be detectable from the maximum possible reading distance [17]. The following two tag designs, however, afford *variable detection ranges* and *proximity-dependent disclosures*.

The *variable detection range* tag (Figure 5.7) uses a slider to interactively modify the actual antenna length and the number of antenna loops used by the tag, which affects the maximum reading distance of a tag. A person could set the slider to use the maximum reading distance, thus allowing readers to gather information from afar (e.g., as in a secure work setting). Alternately, a person can reduce the reading distance (e.g., in more public settings).

The *proximity-dependent disclosure* tag varies the information transmitted with the actual distance between the reader and the tag (Figure 5.8). The tag includes an RFID chip detectable from a larger distance (around 30cm), and a second chip that is only readable in close proximity to the reader (around 1-2 cm). These two RFID chips could contain information at different levels of fidelity: while the far-distance chip includes public available information and is detectable by strangers, the close-distance chip includes more personal information that can be only read when the person is very close to the reader.

Related Work

Previous research has proposed alternative methods to make the usage of RFID more secure. One RFID security approach lets a person authorize individual reading access to a RFID tag [16], usually via an auxiliary device that allows the person to allow specific readers to access the tag information [12]. Recent advanced RFID techniques allow authorization by secret handshakes [3] – performing a particular gesture while holding the RFID tag activates the communication. This approach does not seem particularly viable for everyday situations: people are unlikely to carry extra devices or remember gestures for the multiple cards they carry.

The *Wireless Identification and Sensing Platform* by Intel [10] introduced sensing to RFID tags. With wireless powered circuits and connected sensors, researchers could identify tilting [1] and temperature changes of tagged objects. Smith et al. [15] embed advanced sensors in RFID tags for *human-activity detection*, and applied it in various ubicomp applications. Selker [14] integrated on/off switches into RFID tags to manually activate them. Our research extends this notion by providing simple sensing and control mechanisms that can enhance people's interaction with RFID systems and the protection of privacy-sensitive information.

Conclusion

RFID technology is inevitably intervening in our everyday life. We show how there is value in rethinking characteristics of this technology, and exploring a variety of alternative tag designs. These custom built RFID tags made it possible to make RFID activity *visible*. They also provide people *control* about the tag-reader activity – explicitly by pressing a button or touching the tag, or implicitly by activating or deactivating the tag in response to light, orientation, or proximity.

These advanced RFID tags give people control over the activity of a technology that is usually experienced only passively and often occurs invisibly. The combination of both feedback and control mechanisms into the design of RFID tags gives individuals the means to assert some sort of agency over this ubiquitous technology.

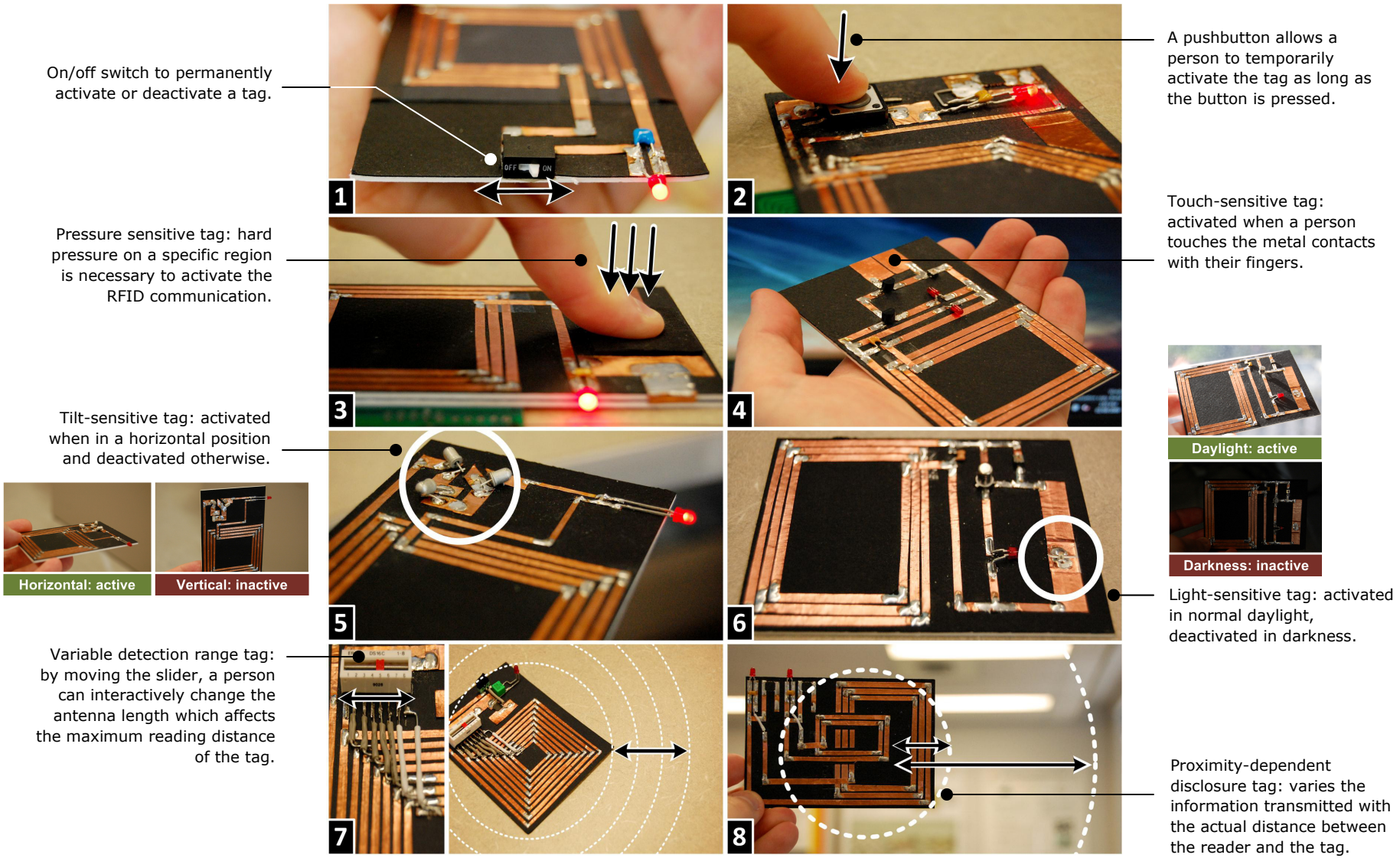

Figure 5. Controllable RFID tags.

Video

The video about the research presented in this abstract is available at: http://www.vimeo.com/6960041 and as download in the ACM digital library.

Acknowledgements

This research is partially funded by Microsoft Research Cambridge, iCORE/NSERC/SMART Chair in Interactive Technologies, Alberta Ingenuity, iCORE, NSERC, and SMART Technologies Inc.

References

[1] Buettner, M., Prasad, R., Sample, A., et al. RFID sensor networks with the Intel WISP. *Proc. of SenSys '08*, ACM (2008), 393-394.

[2] Curtin, J., Kauffman, R.J., and Riggins, F.J. Making the `MOST' out of RFID technology: a research agenda for the study of the adoption, usage and impact of RFID. *Inf. Technol. and Management 8*, 2 (2007), 87-110.

[3] Czeskis, A., Koscher, K., Smith, J.R., and Kohno, T. RFIDs and secret handshakes: Defending against ghost-and-leech attacks and unauthorized reads with context-aware communications. *Proc. of CCS '08*, ACM (2008), 479–490.

[4] Heydt-Benjamin, T.S., Bailey, D.V., Fu, K., Juels, A., and O Hare, T. Vulnerabilities in first-generation RFID-enabled credit cards. *LNCS 4886*, Springer (2008), 2.

[5] Juels, A., Molnar, D., and Wagner, D. Security and Privacy Issues in E-passports. *Proc. of SecureComm '05.* (2005), 74-88.

[6] King, J. and McDiarmid, A. Where's the beep?: security, privacy, and user misunderstandings of RFID. *Proc. of Conf. on Usability, Psychology, and Security*, USENIX Assoc. (2008), 1-8.

[7] Koscher, K., Juels, A., Brajkovic, V., and Kohno, T. EPC RFID tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond. *Proc. of CCS '09*, ACM (2009), 33-42.

[8] Langheinrich, M. A survey of RFID privacy approaches. *Personal and Ubiquitous Computing*, (2008).

[9] Nguyen, D.H., Kobsa, A., and Hayes, G.R. An empirical investigation of concerns of everyday tracking and recording technologies. *Proc. of Ubicomp '08*, ACM (2008), 182-191.

[10] Philipose, M., Smith, J.R., Jiang, B., Mamishev, A., Roy, S., and Sundara-Rajan, K. Battery-free Wireless Identification and Sensing. *IEEE Pervasive Computing 4*, 1 (2005), 37-45.

[11] Poole, E.S., Dantec, C.A.L., Eagan, J.R., and Edwards, W.K. Reflecting on the invisible: understanding end-user perceptions of ubiquitous computing. *Proc. of Ubicomp '08*, ACM (2008), 192-201.

[12] Rieback, M., Crispo, B., and Tanenbaum, A. RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. *Australasian Conference on Information Security and Privacy – ACISP'05*, Springer-Verlag (2005), 184-194.

[13] Schmidt, A. Implicit human computer interaction through context. *Personal and Ubiquitous Computing 4*, 2 (2000), 191-199.

[14] Selker, E.J. Manually Operated Switch for Enabling and Disabling an RFID card. US Patent 6863220, (2005).

[15] Smith, J.R., Fishkin, K.P., Jiang, B., et al. RFID-based techniques for human-activity detection. *Commun. ACM 48*, 9 (2005), 39-44.

[16] Spiekermann, S. and Evdokimov, S. Critical RFID Privacy-Enhancing Technologies. *Security & Privacy, IEEE 7*, 2 (2009), 56-62.

[17] Want, R. The Magic of RFID. *Queue 2*, 7 (2004), 40-48.