Rethinking RFID: Awareness and Control For Interaction With RFID Systems

Nicolai Marquardt[1], Alex S. Taylor[2], Nicolas Villar[2], Saul Greenberg[1]

[1] Department of Computer Science
University of Calgary, Canada
[nicolai.marquardt] [saul.greenberg]@ucalgary.ca

[2] Microsoft Research Cambridge
United Kingdom
[ast] [nvillar]@microsoft.com

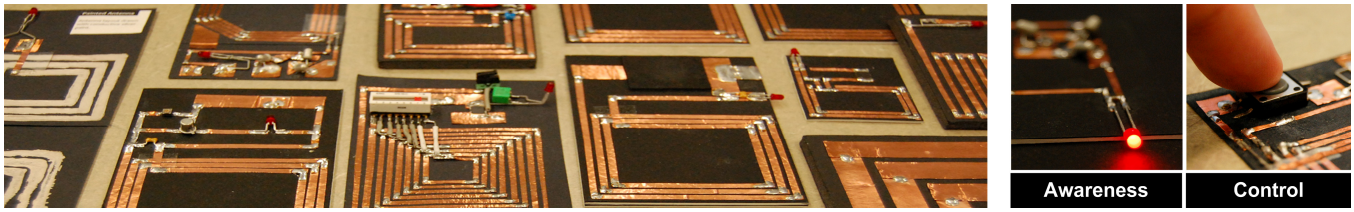

Figure 1. Exploring alternative RFID tag designs (left) to make RFID activation visible and controllable (right)

ABSTRACT

People now routinely carry radio frequency identification (RFID) tags – in passports, driver's licenses, credit cards, and other identifying cards – from which nearby RFID readers can access privacy-sensitive information. The problem is that people are often unaware of security and privacy risks associated with RFID, likely because the technology remains largely invisible and uncontrollable for the individual. To mitigate this problem, we introduce a collection of novel yet simple and inexpensive tag designs. Our tags provide *reader awareness,* where people get visual, audible, or tactile feedback as tags come into the range of RFID readers. Our tags also provide *information control,* where people can allow or disallow access to the information stored on the tag by how they touch, orient, move, press or illuminate the tag.

Author 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

INTRODUCTION

Radio frequency identification (RFID) technology is commonplace in many settings. Within HCI and Ubicomp research, RFID is the bases for a wide variety of novel user interface concepts, e.g., [24,38,40]. Within *commercial and industrial applications*, RFID is often used for object tracking, e.g., inventory control, pallet tracking, supply chain management, and luggage transportation [1,7]. Similarly, RFID systems for *governmental documents* are the fastest growing area of the RFID market, with nearly two billion tags across all application areas produced in 2008 alone [9]. For *personal use*, people are increasingly carrying and using RFID tags (sometimes unknowingly) in a variety of day-to-day situations, where tags contain information or have identifying 'handles' to information stored elsewhere. These include tags that contain: little or no personal information (e.g., transit passes and concert tickets), somewhat benign personal information (e.g., customer loyalty cards) and privacy-sensitive personal information such as biometric data (e.g., the trend to include RFID tags in passports, credit cards, medical cards, and enhanced drivers' licences) [17,20].

This paper concerns the personal use of RFID tags, the risks associated with them, and mechanisms for mitigating this risk. RFID comes at the cost of an increasing number of possible security and privacy threats and attacks. Examples include tracking people's location, eavesdropping on communications between tags and readers, and cloning and misuse of data stored on tags (e.g., [16,20,22]). Even so, we don't advocate abandonment of RFID technology: RFID provides clear advantages such as convenience, low cost, write access to data storage, small size, and reading information from a distance and without line-of-sight [1]. The question is how to make it more secure. The typical technical approach is to use a 'secure' RFID system based on encryption methods and authentication systems (e.g., [8,30]). Such systems raise problems for the user, however. As others have shown, people have difficulties in applying them or understanding their functionality (e.g., [2,10,19,29]). In spite of the added security, this incomplete understanding contributes to people's feelings of insecurity, defencelessness, and helplessness [15,19,25,29].

CHI 2010, April 10–15, 2010, Atlanta, Georgia, USA.

The problem is that people are often unaware of security and privacy risks associated with RFID, likely because the technology remains largely invisible, uncontrollable and difficult to understand. To mitigate this problem, we contribute a collection of novel yet simple and inexpensive RFID tag designs (e.g., Figure 1 shows various working prototypes). Our tags provide *reader awareness,* where people get visual, audible, or tactile feedback as tags come into the range of RFID readers. Our tags also provide *information control,* where people can allow or disallow access to the information stored on tags by how they touch, move, or press them. Besides tags with explicit control of RFID activity by a user, we introduce tags that provide implicit control by reacting to sensed properties, e.g., orientation, proximity, and illumination. Overall, our designs make RFID interaction more visible, controllable, and intelligible, properties routinely proposed as important for Ubicomp systems [3,10].

We first review the related work on RFID privacy and security issues (real and perceived), and the various countermeasures proposed. We then briefly summarize and deconstruct functionality and characteristics of RFID, and propose alternative tag designs that implement awareness and control mechanisms. Next, we provide a scenario envisioning how these new RFID tags could be used in everyday situations. We then list early feedback of our designs by a DIY community. Finally, we discuss limitations of our awareness and control mechanisms.

BACKGROUND

Privacy risks associated with personal RFID tags range greatly. Some tags are benign, as they contain little or no personal information, e.g., transit passes and concert tickets. Others do contain personal information (or are a handle to that information), but the risk is relatively modest, e.g., customer loyalty cards. Still others contain privacy-sensitive personal information, so the risks can be high, e.g., the trend to attach RFID tags to passports, credit cards, and enhanced drivers' licences (EDL) [20]. The threats are real, especially in these later cases, and include [11,16,17,22,26]:

- unauthorized scanning;
- unauthorized location tracking of individuals;
- eavesdropping of authorized communication;
- leakage of biometric data stored on RFID tags;
- hacked RFID deployments;
- cloning of cards.

For example, Juels et. al. [17] summarizes specific privacy threats of electronic passports. Ozer [27] describes insecure and hacked RFID deployments for passport and credit card systems. Heydt-Benjamin et. al. [16] demonstrate how a cardholder's name, credit card number and expiration date can be read by unauthorized readers, and how these cards can be cloned [20].

Countermeasures

The simplest countermeasure is to disable reading of the RFID tag. One approach, endorsed by the US Government, suggests protective sleeves to protect the RFID passports (usually a faraday cage around the tag, for example *ID Stronghold*, [www.idstronghold.com]). While this crude approach decreases an RFID tag's reading distance, it does not completely block access to the tag's information. Thus it is still possible for others to read this supposedly protected information [20].

There are a variety of privacy-enhancing technologies (PET) and methods - Spiekermann et. al. [36] provide a detailed overview. However, most were developed for electronic product codes (EPC) used for commercial product labels rather than for personal use.

The most common technical approach to securing RFID systems is via cryptographic algorithms, e.g., public-key methods [1,22]. Yet embedding these complex algorithms into low-resource RFID tags remains a demanding engineering challenge [36]. Moreover, although they provide a reasonable base layer for privacy, they are still susceptible to engineering attacks, something our proposed awareness and control methods are better suited to prevent.

Some methods disable tags after use. These are typically applied to checkout situations to deactivate tags on purchased items so they will not be read again (e.g., within the store or in other stores). The EPC tag *kill* function completely and permanently disables a tag at checkout so that it is no longer usable. With the *disable model* [37], tags are also disabled at a shop's check-out, but a password can re-enable the object tags if needed. Another method lets people physically disable a RFID tag by providing a layer with the antenna that can be peeled off the tag [18]. These one-time disabling approaches and heavy-weight methods for re-enabling tags are clearly not adequate for securing personal RFID cards, e.g., passports, EDL, and credit cards.

Another approach lets a person authorize individual reading access to a RFID tag [36], usually via an auxiliary device that allows the person to allow specific readers to access the tag information. The RFID Guardian [30] is a device that can record and display RFID scans, and manages RFID keys to authenticate nearby readers, and can block access attempts of unauthorized devices. Recent advanced RFID techniques allow authorization by secret handshakes [8] – 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.

Peoples' Perception of Ubicomp and RFID Security

In their studies of Ubicomp applications, Beckwith et. al. [2] showed that it is especially difficult for people to estimate the privacy and security risks of unfamiliar technologies such as RFID. First, people often failed to

realize the currently available privacy and security level of the system, often due to the lack of visibility of the system's behaviour [10,19]. Next, people's mental models were often naïve, incomplete or incorrect [19]. People were found to have factually incorrect knowledge of the inner workings of RFID [25,29], often perceiving the technology as a black box. In turn, this led to a limited understanding of possible security and privacy risks [19,25].

For example, people's naïve mental models were sometimes based upon line-of-sight communications (i.e., that an RFID tag can only be accessed when visible to the reader); this is incorrect, as line-of-sight is not required [19]. Participants also expected visual or audio feedback for the 'reading' activity of a card by the RFID reader (e.g., an acoustic signal when swiping a payment card over a transit fare RFID reader). If no feedback was presented, participants assumed that the RFID system to be inactive and no information accessed [19]. Again, this is incorrect: readers (such as unauthorized ones) do not have to provide such feedback. People's knowledge also proved incomplete: most were unaware of the large reading distances of RFID tags, their *always on* availability, or even that tags store data [19]. Even without this detailed knowledge of RFID technology and its possible threats, people remained concerned "about their own autonomy and control in the face of an ill-understood and effectively invisible technology" [29]. They felt powerless, as they did not see themselves in a position to do anything against possible threats [25].

Even so, people remain positive about RFID. When asked to weigh potential advantages and disadvantages of RFID applications, most study participants in [25] favoured the advantages. Thus the question is not whether to use RFID. Rather, as summarized by Guenther and Spiekermann [15], people need to feel that they have the ability to control the RFID infrastructure if they are to trust its services.

Suggested Privacy Guidelines and Frameworks

Researchers and policy makers are not blind to these problems of Ubicomp in general and RFID specifically, and have suggested various guidelines to mitigate the problems. Some examples follow.

1. Ubicomp system designers should not separate security-related decision-making from activities done when using the technology. Rather, designers should allow decision-making from within the application context itself (Dourish et al. [10]).
2. The individual should be able to decide about "when, how, and to what extent information about them is disseminated to other parties" (Nguyen et al. [25]).
3. Following the *privacy by design* paradigm, RFID should be disabled by default and allow individuals to activate tags when needed (Ann Cavoukian, Privacy Commissioner of Ontario [6]).
4. Bellotti and Sellen [3] describe the RAVE framework for privacy in ubiquitous computing that is based on two important principles: feedback and control. It helps identify privacy problems and supports finding solutions to address these problems.
5. More generally, Langheinrich [21] provides six principles for privacy in Ubicomp: notice, choice and consent, proximity and locality, anonymity and pseudonymity, security, and access and recourse.

We consider these frameworks and suggestions in our research, where we explicitly focus on RFID technology redesign that allows people to be *aware of* and *actively control* their interaction with RFID-based systems.

Scenario of Possible Privacy-Threats

To better illustrate the privacy threats mentioned in this section we provide a scenario of how such threats might affect a person's life in everyday situations.

> *Claire uses the train to commute to work. She owns a payment card for easy electronic payment of fares. As she enters the train station, she takes out her wallet (that includes the payment card) and swipes it over the reader at the entrance as usual. This time, however, Claire is surprised that the access to the train station is declined, even though she is sure that she just recently deposited several hundred dollars on the train payment card. When complaining about the rejected payment card at the counter, she is told that the credit balance of her card is $0. A later police investigation reveals that a criminal, likely located near the station's entrance, has illegally scanned and later cloned and sold copies of Claire's payment card. Police believe that her identification documents were also scanned - her employee pass, credit card, passport and driver's licence - and that she should be concerned about identity theft and further financial theft. Claire was shocked; she was completely unaware of the risk of surreptitious wireless access to the personal and financial information stored on the cards she carries.*

This is a fictitious but realistic scenario about an extreme case of identity and financial theft. More and more people will carry RFID-enabled payment and identification cards, increasing the incentive for criminals to misappropriate this technology. The previously mentioned privacy and security threats are both impending and likely.

EXPLORING AND DECONSTRUCTING RFID

Before detailing our new designs of RFID tags, we first provide some technical background and common properties of RFID systems (also see [1,38,39]).

Basic Principles of Conventional RFID

A deployed RFID infrastructure consists of two main types of hardware: a *reader* and *tags*. A *tag* combines an antenna and an RFID chip, where both are combined in a carrier material (e.g., card or label sticker). The *reader* is an electronic circuit that transmits a radio signal across a (larger) antenna. When a tag approaches a reader, the signal transmitted by the reader induces an electrical current in the tag's antenna. This induced current is sufficient to power the integrated circuit on the RFID chip. When powered, the RFID chip modulates a response signal that is transmitted back to the reader which, in turn, decodes the signal. The

signal minimally provides a unique tag identification number, although some RFID chips can transmit other information (e.g., balance information on payment cards or biometric data like fingerprints) stored in the chip memory.

RFID tags are usually passive: no energy source on the tag is necessary. A few use auxiliary power (*semi-passive*), or actively send signals themselves (*active*). RFID standards define diverse frequencies for radio transmissions: the majority of systems transmit via the 13.56 MHz frequency standard (we use this frequency, but as shown later in this paper, our techniques also apply to other standards). The maximum reading distance with 13.56 MHz tags is ~1m, although ultra-high frequency RFID tags can be read from over 10m.

Enhancing RFID Tags with Sensors

While equipping RFID tags with embedded sensors is rare [31], it is relevant to our design strategy. Thus a few research efforts are described below.

The *Wireless Identification and Sensing Platform* by Intel [28,4] introduced sensing to RFID tags. With wireless powered circuits and connected sensors, researchers could identify tilting [5] and temperature changes of tagged objects. Their context was industrial supply chain applications, for example detecting if the storage or temperature range of an object was correct during transport. In a separate project, Smith et al. [35] embed advanced sensors in RFID tags for *human-activity detection*, and applied it in various ubicomp applications. Similarly, the tags we will go on to describe are designed to be context-sensitive. However, they response to basic sensed information – e.g., orientation, illumination, and proximity to the reader – and are based on an implicit model of human-device interaction (see Schmidt [33]).

Overall, combining passively-powered sensor platforms with RFID tags allows enhanced sensor readings and many possibilities for wireless sensor network applications [31]. Our research (discussed shortly) extends this notion by providing simple sensing mechanisms that can enhance people's interaction with RFID systems and the transmission of privacy-sensitive information.

Common RFID Properties

From our review of standard RFID hardware and applications, a number of common properties and characteristics emerge.

- *Invisibility of tags.* Tags are usually embedded and hidden, and manufactured as small as possible (while preserving the reading distance).
- *Invisibility of use.* There is no indication on a tag about its activity when a reader communicates with it. As mentioned, line of sight is not necessary to establish a connection; thus the reader may not even be visible.
- *Unique identifiability.* Tags respond to requests with at least one unique identification number. This number is usually globally unique and cannot be altered.
- *Permanent availability.* RFID tags are designed to be always available, and they transmit a response to all readers that send a valid request via the transponder signal.
- *Autonomy.* The tags are designed as stand-alone units. Interaction with or control of the RFID tag's behaviour by a person is neither intended nor supported.

These properties contribute to the strength of RFID technology. Indeed, they are often critical to the successful deployment of many industrial and commercial applications [1]. However, they also compromise privacy and security. We question the necessity of these properties in many use cases that involve personal use, for instance, when using RFID in governmental documents such as passports and EDLs. In our later explorations of alternative RFID designs, we will describe how our designs raise questions about the criticality of each of these five properties.

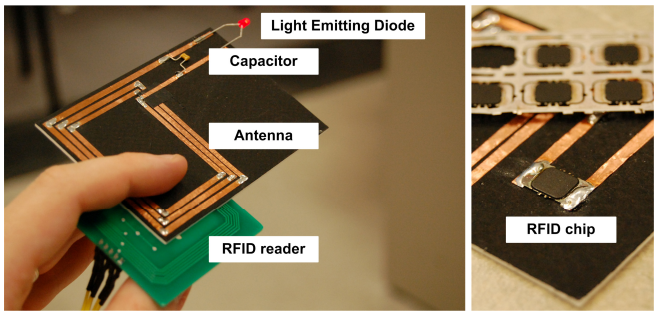

Figure 2. Tag makes RFID visible (left), RFID chip (right).

Building Custom Tags and Exploring the Design Space

We explored existing RFID technology in-depth. Our investigations drew on research publications, technical specifications, whitepapers about building RFID antennas (e.g., [23]), and even disassembling multiple RFID tags and measuring their properties. This provided us with the bases for building traditional RFID tags, and the expertise to explore and design alternative tag designs with non-traditional interactive functionality.

Our approach was to build functional prototypes. Several are briefly described below to illustrate our prototyping process and its mechanics; see [23] for our detailed 'do it yourself' instructions. Discussions about the purpose of these and other designs are deferred until the next section.

Our first prototype adds reader awareness capabilities to a tag. Figure 2, left, is an RFID reader detector: a light-emitting diode (LED) attached to the tag turns on when the tag is within range of an RFID reader. The tag is composed of an *antenna* made with conductive copper tape, a *capacitor* to calibrate the RFID tag to the reader's frequency, and the LED. The basic principle we are using is known as *energy harvesting*: the LED illuminates as the nearby RFID reader induces a current in the loops of the tag's antenna. We then turned this into a fully functionally tag by replacing the capacitor and antenna with a separate

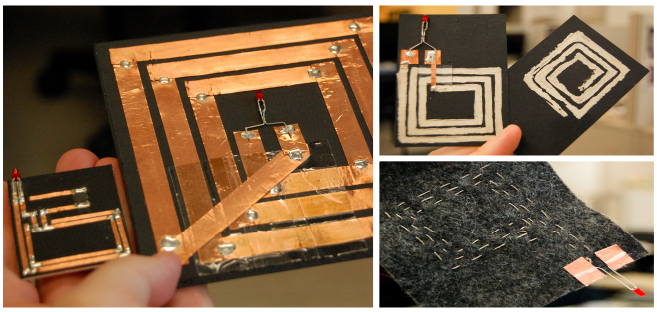

Figure 3. Altering properties: size (left) and material (right)

RFID chip (Figure 2, right); this arrangement transmits the chip's unique serial number to the reader.

Our next prototypes explored various material properties of tags, where we found basic tag design quite robust in terms of the changes that could be made while still delivering a functional tag. For example, we found altering the size, length, and layout of the tag's antenna influenced, as expected, the maximum reading distance of the tag (e.g., Figure 3, left shows 2 tags with small and large antennas). We also used different materials for building the antenna, where we substituted conductive silver ink and conductive thread to build the antenna loops (e.g., Figure 3, right). The material also impacts the reading distance, and provides completely different affordances for integrating tags into other objects (e.g., wearable computing).

AWARENESS AND CONTROL OF RFID ACTIVITY

We describe how and why our RFID tag designs integrate *reader awareness* and *information control* mechanisms.

Reader Awareness and Visibility

One of our main motivations was to make the usually invisible activity of RFID systems *visible* to the individual. As mentioned, various studies (e.g., [19,29]) have stated that people often have an incomplete understanding of the functionality of RFID, which can not only result in misuse, but also fear and insecurity about privacy risks. We believe that providing feedback about a tag's reading activity can help people to better understand what is going on, even if they do not know how RFID tags technically work.

We designed three tags, each varying the type of feedback about RFID reading activities provided to a person: *visual*, *audible*, or *tactile* feedback.

The *visual feedback* RFID tag (Figure 4.1) was already introduced in the previous section. An LED lights up when it is in range of an RFID reader, i.e., when a reader can potentially read the tag's content. This proved very easy to implement, especially because energy harvesting suffices to power the LED. While simple, it is 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.

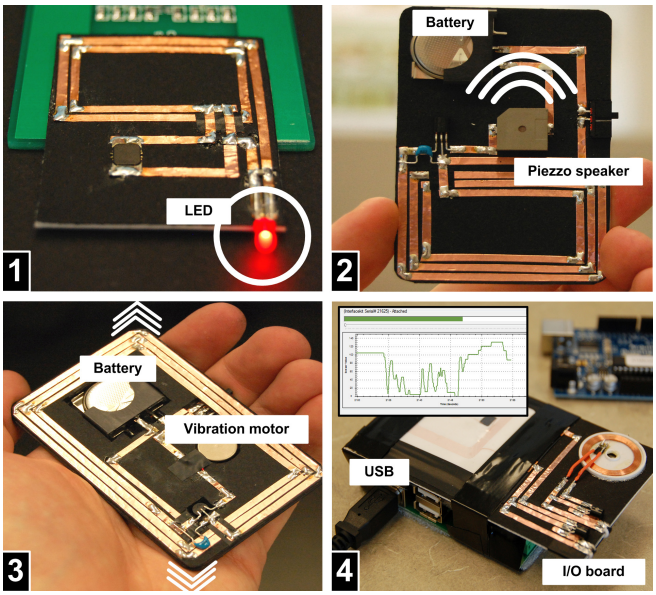

Figure 4. Feedback about RFID activity: (1) visual, (2) audible, and (3) tactile; and (4) USB connected RFID-sensing board.

Our *audible feedback* RFID tag and *tactile feedback* tag 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 4.2), while the *tactile feedback* tag uses a vibro-tactile motor connected to the tag whenever a reader is nearby (Figure 4.3). This comes at a cost. Both 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).

As with cell phones, the choice of a visible, audible or tactile tag depends on the circumstances of the end user. A tag can, of course, be designed to have all three feedback mechanisms, where a person can chose the desired feedback mode. This could be done by including a switch, or by swapping plug and play feedback modules onto a tag.

To aid prototype exploration, we can also connect our tags to a generic computer-controlled input-output sensor boards (e.g., [www.phidgets.com] or [www.arduino.cc]) as shown in Figure 4.4. The intensity of the electromagnetic field of nearby RFID readers is now measured through its analog input, relayed to a desktop or mobile computer, and (for example) visualized as a graph in software on the computer display (see inset of Figure 4.4). Thus we can rapidly experiment with software that reacts in different ways according to detected RFID activity. This approach opens up new RFID possibilities when such boards are miniaturized and integrated with the tag. For example, a person's mobile phone or PDA can log when RFID reader activity is detected by the tag and record the GPS coordinates; this allows one to review detected RFID readers later on (e.g., as overlay on a geographical map).

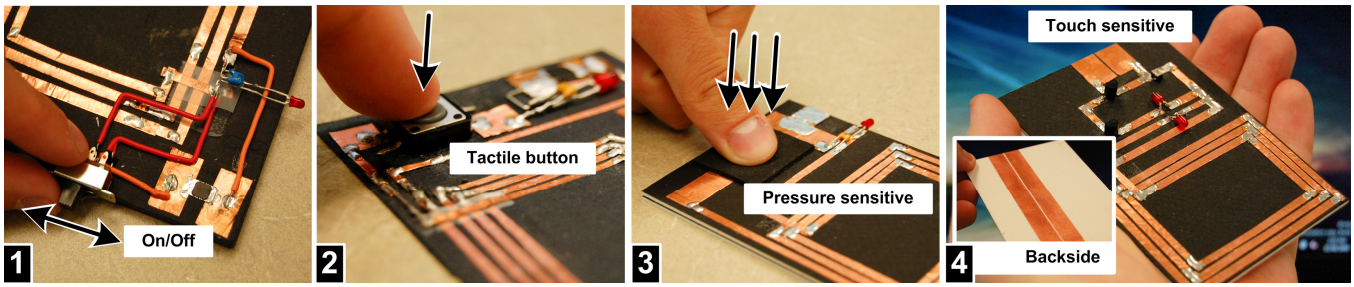

Figure 5. Controlling RFID communication: sliding switch, push button, pressure-sensitive button, touch-sensitive contacts.

In summary, the easy to understand 'visible' feedback about ongoing RFID activity provided by these three prototype tags - as well as the tag coupled with a mobile PC - counters the *invisibility* property of traditional RFID tags. These feedback mechanisms – especially the LED example – are easy to implement and are reasonably cheap.

Information Control of RFID Activity

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. We explain the technical concept behind each of these control mechanisms, and illustrate their application by scenario.

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. We extend the concept originally introduced in the patent by Selker et al. [34] by introducing a variety of options for allowing user interaction with tags that react to pressure, touch, light, or orientation. These tag designs counter the *permanent availability* and *autonomy* properties typical of common RFID tags.

Control by Using On-Off Switches

Our first two 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. (Our examples also implement visible feedback via an LED, as described in the previous section). Depending on the switch, two quite different modes of control can be offered.

1. *Activating or deactivating the tag for long time periods*. A toggle switch with two permanent positions lets a person either activate or deactivate the tag (Figure 5.1). The switch remains in the last selected state until toggled again.
2. *Temporarily activating the tag*. A pushbutton is pressed to activate the RFID tag, where releasing the button automatically inactivates it (Figure 5.2). Thus the tag is normally inactive, which implements the *Privacy by design* concept [6]. This mechanism is suitable for confirmation. For example, the LED visible feedback is interpreted as a 'read request'. The person then presses the button while the LED is lit (i.e., the tag is in reader range) before the reader can communicate with a tag.

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). We can adjust the pressure sensitivity of the tag, which changes the threshold that determines when the tag becomes active. A low pressure threshold could be used for RFID tags containing benign information, whereas a high pressure threshold could be used for RFID tags containing privacy-sensitive information (e.g., personal biometric data).

The *touch-sensitive RFID tag* is activated once a person touches large metal contacts on tag with a finger or hand (Figure 5.4). A circuit on the tag measures the resistance between the metal contacts and activates the RFID chip once it detects a resistance below a certain threshold (in this case the threshold is calibrated to the resistance of human skin). The contacts begin on the front side of the tag but continue on the backside as well (visible in inset of Figure 5.4). This RFID tag design has the advantage that the person using the tag does not have to press a specific button on the tag, but can simply hold the tag in the hand to activate it.

The above examples illustrate the easy integration of buttons and switches into RFID tags, allowing the individual to explicitly turn the tag on and off, or to temporarily activate the tag as desired.

Tilt- and Light-Sensitive RFID Tags

Tag activity state can also depend on implicit sensed properties [33] rather than explicit actions. We illustrate three RFID tag examples: two *tilt-sensitive* and one *light sensitive*.

The *tilt-sensitive tag* (Figure 6, left) is activated when in a horizontal position (bottom left), and deactivated otherwise (bottom right). 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 (top). The tag position determining tag activity can be changed by altering the mounting angles of the tilt switches on the tag, and by changing their parallel and/or serial connection. This design may be suitable for cards that are normally kept in a wallet (which is rarely horizontal) that are intended to be read on or above a surface (which is usually horizontal).

A *flipping tag* (not shown) also uses tilt switches, but in this case it flips between two different RFID chips. Depending

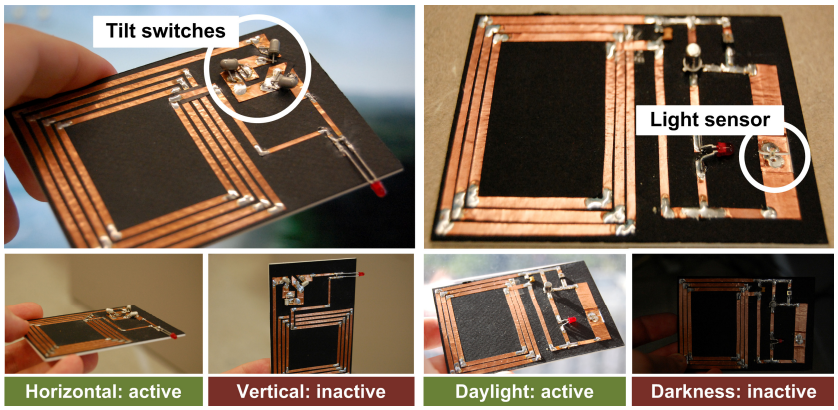

Figure 6. Tilt-sensitive (left) and light-sensitive (right) RFID tags.

on which side of the tag faces upwards (measured by the tilt sensors), one or the other RFID chip is activated. This design thus gives people the ability to decide what information on a tag to transmit in a given situation.

Next, a *light-sensitive tag* is activated in normal daylight and deactivated in darkness (Figure 6, right). 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 RFID Tags

Usually RFID tags are built to be detectable from the maximum possible reading distance [39]. The following two tag designs, however, afford *variable detection ranges* and *proximity-dependent disclosures*.

The *variable detection range* tag (Figure 7, top) 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 minimal length of the antenna (one short loop of the antenna material) limits the reading distance to a few millimetres – which affords activation only by explicit direct touch of the card to the reader.

The *proximity-dependent disclosure* tag varies the information transmitted with the actual distance between the reader and the tag (Figure 7, bottom). This idea reflects the security principle that larger distance means less trust, whereas closer distance implies trustworthiness (as described with the tiered authentication scheme by [12]). 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.

All our tag designs counter the *permanent availability* and *autonomy* properties typical of common RFID tags. They are not permanently available as people can control their on/off state via either explicit or implicit actions. They are not autonomous as people have control of tag behaviour. The proximity-dependent and flipping tag counter the *unique identifiability* property; multiple identities (with varying levels of information detail) are available on these tags, where the identity exposed is a matter of the person's choice and actions.

REVISITING THE SCENARIO

We now refer back to our earlier scenario and describe how our reader awareness and information control methods could change the way how Claire might use the RFID technology in everyday situations.

> *Claire is using the electronic payment system for the train. When she swipes her wallet over the reader at the entrance, her card inside the wallet activates once in a horizontal position; it vibrates, and the reader communicates with the tag to perform the fare transaction. When Claire puts the card back into her pocket, she knows that her fare has been read. She also knows her card is inactive, and thus others cannot read and copy her card.*
>
> *She arrives at work and uses her employee ID card to access the company building. Following company security policy, she takes her ID card out of her wallet and clips the card onto her shirt; the light in the building switches the light-sensitive RFID card on. As she passes by computers and doorways, a light on her tag shows her that those devices can be used by her. When she later leaves the building to drive to the airport, she puts her*

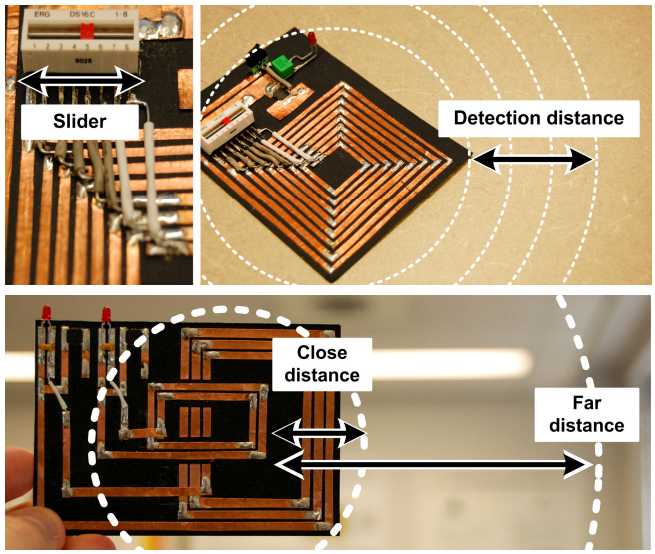

Figure 7. Proximity-dependent RFID tags: variable detection range (top) and proximity-dependent disclosure (bottom).

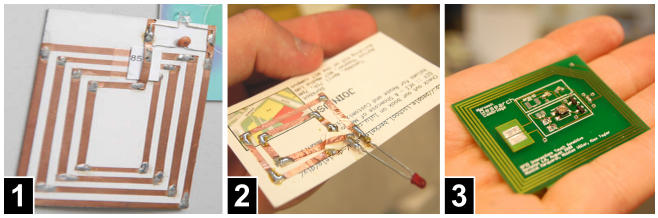

Figure 8. (1,2) DIY tag experiments and (3) printed circuit board of the touch-sensitive RFID tag.

ID back in her wallet, thus disabling the card. This is according to company policy, as the company does not want anyone outside its doors to access her employee number.

Outside the airport, her credit card vibrates. This raises her suspicions about financial theft, so she informs airport security. They investigate, and capture a person with an illicit credit card reader. Claire knows that her own financial information has not been read, as the card's communication is switched off.

Once at the airport, she buys lunch at a restaurant. She places her credit card near a 'pay here' spot at her table; her card vibrates, and now she knows she can pay wirelessly at her table. When she finishes eating, she pays by activating her card and pressing the card's push-button.

Later at the security check for her flight to Paris, Claire hands her passport to the security officer. The officer opens the passport page, and the light-sensitive switch activates the integrated RFID chip that transmits the passport number to the system. By touching a sensitive area on the passport, the officer also activates the transfer of biometric data to the computer. After confirming her passport documents, Claire proceeds to the gate.

This scenario relies, of course, on a somewhat idealised vision of a ubiquitous infrastructure. However, what we hope it illustrates is how awareness and control methods (explicit and implicit) can be integrated into everyday usage of RFID. Current tag technologies do not provide such visible reader activity feedback (building access systems, transit fare payment, illicit card reading detection, wireless credit card payment, and getting biometric information from passports). Nor do current tags provide a control mechanism to allow or disallow a reader to access the information content on the tag. With traditional tags, it would be possible for an adversary to access the information on Claire's identification and payment cards without her knowledge as described in our earlier scenario; this is now much more difficult to do.

EARLY FEEDBACK AND DIY EXPERIMENTS

In this paper, we've emphasized how the careful examination with RFID and our practical experimentation with its particular features offered some useful starting points for re-thinking the technology. Specifically, we've tried to show how starting from first principles and also combining RFID with lightweight sensing and output technology provided a number of interesting possibilities for addressing problems of privacy and security.

As yet, we have not done any formal evaluation of our early tag designs. However, in closing we want to briefly discuss the feedback we received from posting a number of how-tos on the online DIY pages, *Instructables*.[1] Importantly, our interest in posting the how-tos were not to test the usability of the tag designs. Rather, we wanted to see whether the Instructables community were open to thinking differently about RFID and to participating on the kinds of experimentation we had. In short, we were interested in how our practical approach and preliminary designs might encourage new ways of addressing RFID tag design.

We published the step-by-step instructions of how to build our basic RFID tag and reader detector on Instructables and received electronic[2] feedback, and later face to face feedback (during a conference workshop). This exercise raised the following encouraging results:

- *Tags proved easy to build and vary.* Various people not only rebuilt our RFID tag designs, but proposed alternative solutions (e.g., changing antenna material, making them much smaller). Surprisingly for us, this included people with no prior experience in electronic hardware (two sent-in photos of tags built by non-experienced people are shown in Figure 8.1 and 8.2).
- *People were interested, regardless of their experience.* They also exchanged suggestions of where to buy material. They asked many questions about details of RFID technology (e.g., standards, frequencies, reader hardware).
- *People contributed RFID experiences.* People described their observations of RFID in everyday situations. For example, one described how readers at transit stations can detect large amounts of tags simultaneously. Another described details about the maximum distances of where their RFID cards were detected by RFID readers. Others described the kind of RFID-enabled cards they personally use (e.g., employee IDs, credit cards), and their experiences with them (e.g., reliability, broken hardware).
- *Opinions and discussions*. People were opinionated about RFID technology use, especially about its most recent integration into passports. They mentioned their fears about the security of their personal information. They described their lack of control, e.g., their inability to do anything against RFID introduced in passports and drivers licences. Yet people also made positive points, where they discussed the usefulness of integrating RFID into governmental documents.

We're encouraged by these preliminary results. We find it promising that members albeit of a DIY community were able to take what is often seen as a black-boxed technology and begin experimenting with it, openly. What we hope this suggests is that unpacking or opening up a technology

[1] http://www.instructables.com/id/RFID_Reader_Detector_and_Tilt_Sensitive_RFID_Tag/

[2] 42000 views of the initial posted article on the website, 127 forum and blog entries, as well as various email responses in 7 months.

exposes it, in some sense, to further examination. It provides a basis, we hope, for better understanding the affordances and constraints of the technology, including its security and privacy issues.

DISCUSSION AND LIMITATIONS

We discuss limitations of our RFID tag designs – explicitly issues that arise when our proposed awareness and control mechanisms are integrated and used in actual real-world RFID deployments.

Usage Limitations

Interaction costs in frequent and long term situations. When RFID cards are in daily and frequent use, the user's interaction costs may become problematic. Our introduction of more advanced forms of interaction – compared to the simple swiping of current RFID cards – changes the way people have to use the technology. The many activity notifications (e.g., an acoustic tone) could become annoying, and the required manual activation of the tag (e.g., repeatedly pressing a button) may become an irritant. The problem becomes even more apparent when considering the increasing number of RFID enabled cards people might possess in the near future. This could lead to situations where people prefer to disable the awareness and control mechanisms completely and instead fall back to an always-on RFID tag.

Several different paths can help lessen this problem. First, as with any technological deployment, the use of a particular method must be designed to be appropriate to its setting. For instance, frequently used RFID cards containing no privacy sensitive information might be protected with an unobtrusive *implicit* method, whereas cards containing highly sensitive information (e.g., payment) would suggest more secure forms of protection that require *explicit* action by the person. Similarly, for reader awareness, perhaps the simpler visual feedback mechanisms would become a reasonable default for personal RFID tags. Depending on the sensitivity of data on the tag, more noticeable feedback might be included. Second, we could put this power into the hands of the people, allowing them to choose a *preferred* awareness and control mechanism (perhaps by attaching plug and play modules to the card). Third, we could combine both implicit control mechanisms (such as the tilt sensors) to provide a general safeguard, while including more explicit control mechanisms (such as switches). Fourth, it is possible to introduce awareness mechanisms that monitor the usage of multiple cards simultaneously; for instance a vibration feedback integrated into a wallet monitoring the access to all RFID cards inside.

Low information feedback. Our methods only give feedback about ongoing RFID reading activity. They do not detail the content of the transmitted information. This is possible, although we have not done it. For example, small powered displays on the tag can show the information being read or, as mentioned previously, that information could be relayed to a cell phone or PDA. This could be valuable for situations where people do not know what the card actually contains. However, it also introduces another level of complexity and necessary cognitive load by providing this detailed information to the user.

Integration in RFID System Deployments

As we've noted, our design suggestions have been meant as enabling rather than predictive. We do not know yet how our proposed awareness and control techniques might be integrated into existing and future RFID systems.

Of course, our redesigned tags are only one of many important mechanisms safeguarding the security and transparency of deployed RFID systems. We expect them to be interwoven with other security mechanisms, such as cryptographic methods, secure back-end databases, and adequate security policies defining privacy and access (e.g., [13,14,22]).

Technical challenges remain for the integration of such advanced RFID tags in commercial deployments. Industrial manufacturing of much smaller and low priced tag designs is possible by using micro components assembled on printed circuit boards (PCB). Indeed, we built several of our RFID tags in a small form-factor PCB design (see Figure 8.3). Many other form factors and designs are feasible, as well as more advanced circuits to read sensors, detect switches, and control RFID communication.

Moreover, there are many remaining questions that need to be answered before any significant real-world deployment. For example, would feedback about RFID activity alleviate people's perception of RFID security? Would it change their mental models of the inner workings of this technology? How would people handle (or appropriate) the gained control of their ongoing RFID activity? What real-world constraints and contextual issues must we consider when we choose particular RFID designs? Our work opens the door to these and other questions.

Several of these questions could be further explored in a formal evaluation of our proposed approaches. Studying the usage of the enhanced RFID tags in real-world situations could provide further insights of how the awareness mechanisms could affect peoples' perception of the technology, and how the more advanced and unfamiliar forms of interaction with RFID (explicit control or implicit sensing) might be used in practice.

CONCLUSION

RFID technology is inevitably intervening in our everyday life. We show how there is value in rethinking and questioning common properties and characteristics of this technology. By deconstructing RFID technology and questioning some of its common properties, we were able to explore a variety of alternative tag designs. These custom built RFID tags made it possible to integrate *reader awareness* feedback about the access to those tags. They also provide people *information 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 awareness and control mechanisms into the design of RFID tags gives individuals the means to assert some sort of agency over this ubiquitous technology.

ACKNOWLEDGMENTS

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

REFERENCES

1. Ahson, S. and Ilyas, M. *RFID Handbook*. CRC Press, 2008.
2. Beckwith, R. Designing for ubiquity: the perception of privacy. *Pervasive Computing, IEEE 2*, 2 (2003), 40-46.
3. Bellotti, V. and Sellen, A. Design for privacy in ubiquitous computing environments. *Proc. of ECSCW '93*, Kluwer (1993), 77-92.
4. Brunette, W., Lester, J., Rea, A., and Borriello, G. Some sensor network elements for ubiquitous computing. *Proc. of IPSN '05*, IEEE (2005), 52.
5. Buettner, M., Prasad, R., Sample, A., et al. RFID sensor networks with the Intel WISP. *Proc. of SenSys '08*, ACM (2008), 393-394.
6. Cavoukian, Ann. *Privacy by Design... Take the Challenge*. Information and Privacy Commissioner of Ontario (Canada), http://www.ipc.on.ca/images/Resources/PrivacybyDesignBook .pdf, 2009.
7. 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.
8. 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.
9. Das, R. and Harrop, P. *RFID Forecasts, Players and Opportunities 2009-2019*. IDTechEx Inc. Report, www.idtechex.com, Cambridge, MA, USA, 2009.
10. Dourish, P., Grinter, E., Flor, J.D.D.L., and Joseph, M. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal Ubiquitous Comput. 8*, 6 (2004), 391-401.
11. Eckfeldt, B. What does RFID do for the consumer? *Commun. ACM 48*, 9 (2005), 77-79.
12. Fishkin, K.P., Roy, S., and Jiang, B. Some Methods for Privacy in RFID Communication. In *Security in Ad-hoc and Sensor Networks*. 2005, 42-53.
13. Garfinkel, S. An RFID Bill of Rights. *Technology Review, http://www.technologyreview.com/communications/12953/*, 2002.
14. Garfinkel, S., Juels, A., and Pappu, R. RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Security and Privacy 3*, 3 (2005), 34–43.
15. Günther, O. and Spiekermann, S. RFID and the perception of control: the consumer's view. *Com. ACM 48*, 9 (2005), 73-76.
16. 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.
17. Juels, A., Molnar, D., and Wagner, D. Security and Privacy Issues in E-passports. *Proc. of SecureComm '05.* (2005), 74-88.
18. Karjoth, G. and Moskowitz, P.A. Disabling RFID tags with visible confirmation: clipped tags are silenced. *Proc. of the workshop on Privacy in the electronic society*, ACM (2005), 27-30.
19. 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.
20. Koscher, K., Juels, A., Kohno, T., and Brajkovic, V. EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. *RSA Laboratories. In Submission. http://www.rsa.com/rsalabs/node.asp?id=3557*, (2008).
21. Langheinrich, M. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. *Proc. of Ubicomp '01*, Springer (2001), 273-291.
22. Langheinrich, M. A survey of RFID privacy approaches. *Personal and Ubiquitous Computing*, (2008).
23. Marquardt, N. and Taylor, A.S. RFID Reader Detector and Tilt-Sensitive RFID Tags. *DIY for CHI Workshop*, (2009).
24. Martinussen, E.S. and Arnall, T. Designing with RFID. *Proc. of TEI '09*, ACM (2009), 343-350.
25. 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.
26. Ohkubo, M., Suzuki, K., and Kinoshita, S. RFID privacy issues and technical challenges. *Com. ACM 48*, 9 (2005), 66-71.
27. Ozer, N.A. Rights “Chipped” Away: RFID and Identification Documents. *Stanford Technology Law Review, http://stlr. stanford.edu/pdf/ozer-rights-chipped-away.pdf 1*, 1 (2008).
28. 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.
29. 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.
30. Rieback, M., Crispo, B., and Tanenbaum, A. RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. *Proc. of ACISP'05*, Springer (2005), 184-194.
31. Sample, A., Yeager, D., Powledge, P., and Smith, J. Design of a Passively-Powered, Programmable Sensing Platform for UHF RFID Systems. *Proc. of RFID '07*, IEEE (2007), 149-156.
32. Sample, A., Yeager, D., and Smith, J. A capacitive touch interface for passive RFID tags. *Proc. of RFID '09*, IEEE (2009), 103-109.
33. Schmidt, A. Implicit human computer interaction through context. *Personal and Ubiq. Computing 4*, 2 (2000), 191-199.
34. Selker, E.J. Manually Operated Switch for Enabling and Disabling an RFID card. US Patent 6863220, (2005).
35. Smith, J.R., Fishkin, K.P., Jiang, B., et al. RFID-based techniques for human-activity detection. *Commun. ACM 48*, 9 (2005), 39-44.
36. Spiekermann, S. and Evdokimov, S. Critical RFID Privacy-Enhancing Technologies. *Security & Privacy, IEEE 7*, 2 (2009), 56-62.
37. Spiekermann, S. and Berthold, O. Maintaining Privacy in RFID Enabled Environments. In *Privacy, Security and Trust within the Context of Pervasive Computing*. 2005, 137-146.
38. Want, R. Enabling ubiquitous sensing with RFID. *Computer 37*, 4 (2004), 84-86.
39. Want, R. The Magic of RFID. *Queue 2*, 7 (2004), 40-48.
40. Want, R., Fishkin, K.P., Gujar, A., and Harrison, B.L. Bridging Physical and Virtual Worlds with Electronic Tags. *Proc. of CHI '99*, ACM (1999), 370-377.