Where's The Beep?: Security, Privacy, and User Misunderstandings of RFID*

Jennifer King
U.C. Berkeley School of Law
Andrew McDiarmid
U.C. Berkeley School of Information

Abstract

While extant for decades in the industrial sector, radio frequency identification (RFID) technology is increasingly being incorporated into everyday products and objects. This growing ubiquity brings with it security and privacy concerns for end users due to implementations that fail to adequately protect personal or identifiable data stored on RF transponders, as well as RFID's inherently stealthy broadcasting capabilities. Accordingly, taking effective measures to mitigate the risk of undesirable data transmission requires understanding what RFID is and how RF transmissions work. In our exploratory research, we attempt to elicit user mental models of RFID technology by interviewing users of three existing implementations of consumer-focused RFID technology: RF-enabled credit cards, transit passes, and the U.S. e-Passport. We explore user comprehension of RFID technology generally and these implementations specifically to gain an understanding of how end users conceptualize RFID and its risks. We found in this initial inquiry that our subjects generally lacked a mental model of how RFID functions, and in turn did not understand risks posed by RFID implementations or how to mitigate them.

1. Background

RFID is a promiscuous technology: in its most basic implementation, an RF tag will transmit its stored data to any reader operating at its corresponding frequency. It is also a ubiquitous technology, imbuing everyday objects with "always on" computational and communication capabilities, though it is not yet ubiquitously deployed in the U.S. While the applications for "basic" tags are typically object tracking, such as inventory control, the possible linkage between a static identifier and an individual person raises privacy concerns, such as the tracking of individuals though public space. Contactless smart cards, a passive RF technology operating at 13.56Mhz with a general read range of around four to six inches, have far more computational power and storage capacity than simple RFID tags, including encryption capability. Contactless smart cards are generally (but not always) used in RF applications that require reader authentication and the secure storage of data. The applications we explore in this paper – credit cards, transit passes, and e-Passports – incorporate contactless smart card chips, though not all use smart cards' authentication and cryptographic abilities.

Due to the diversity of possible RFID deployments, assessing RFID's security and privacy risks requires a case-by-case analysis, dependent on the type of RFID used, the information stored on the chip, and the context in which the implementation is deployed. In this work, we focus on applications of RFID that store an end user's financial or personally identifiable information. We are interested in these implementations because unlike an RF tag attached to or embedded in a consumer product, ensuring the integrity of the data stored on an identity document or credit card is typically of concern to its owner since a breach of this data can have negative personal consequences, such as financial fraud or identity theft. Furthermore, there is a strong likelihood that the object will be used in a public space, increasing the opportunity that the RF chip could be read (or "skimmed") by an unauthorized party since, unlike traditional credit cards or passports, these objects can be read without the knowledge or consent of the user. Finally, because these are objects that the subjects already possess and use, establishing the context for our research presumably makes more sense to our subjects than investigating abstract concepts, particularly when talking to subjects with little or no knowledge about RFID.

It is possible to create secure implementations of RF technology using contactless smart card chips, though at this stage in RFID development not all companies or

* This work was funded by TRUST (Team for Research In Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award CCF-0424422). The authors wish to thank Shawna Hein, Jon Hicks, Travis Pinnick, and Aylin Selcukoglu for their assistance with interviews, and Deirdre Mulligan, Chris Hoofnagle, and Nathan Good for their valuable feedback.

agencies choose to do so. While there have been efforts to address security and privacy issues at the chip design level [Floerkemeier, Hachman], these efforts have yet to gain momentum, and thus users often bear some or all of the burden of mitigating privacy and security threats. For example, Heydt-Benjamin et al. [Heydt-Benjamin] discovered in 2006 that credit card issuers were not encrypting data stored on RF-enabled credit cards. The original proposal for the U.S. e-Passport had no security features in place to protect the passport holder's personal data. While the Department of State, in response to public criticism, incorporated both a Faraday cage and weak encryption (Basic Access Control) into the final e-Passport design, as of 2008 it appears credit card issuers continue to store credit card information in the clear. One can speculate that this choice is based in part upon the fact that despite adhering to the ISO 14443 standard, the data can only be accessed by readers using compatible software.[1] This "security through obscurity" approach is only viable as long as compliant readers or software are not obtained or hacked by malicious parties — a likely risk, in part, because payment systems are widely deployed by retailers of varying trustworthiness.[2]

In contrast to credit cards, the transit agency pass we examined, the Bay Area Rapid Transit (BART) EZ-Rider pass, encrypts the data stored on their passes. As BART is a self-contained agency, managing their own readers and encryption keys is relatively possible; it is the complexity brought on by interoperability and key management that was stated as one of the most common reasons why the new U.S. passports were not using public key encryption [Kuchinskas]. In public implementations requiring large-scale interoperability, such as the new Department of Homeland Security PASS card and state issued enhanced driver's licenses, no anti-skimming protections will be deployed. Instead, the only data stored on the chip will be a static identifier linked to the cardholder's record in DHS databases, a design DHS considers to be protective of card holder privacy [DOS]. For those concerned with the thirty-foot read range of the UHF tags used in these cards, DHS will provide a Faraday shield for use with the card, placing the burden of preventing uninitiated reads on the individual cardholder.

In our work, we aim to examine assumptions regarding end user comprehension and risk. For instance, what are end users' mental models of how RFID systems work, and how do they compare to the actual functioning of these systems? Do they understand that tags and chips can often be read without their knowledge, and the steps they would need to take to mitigate skimming risks? How do their mental models affect their ability to make risk assessments about potential security or privacy threats? These questions present different challenges with ubiquitous technologies than with software, primarily because unlike software, where the tool for communicating with the user is the visual interface, RFID effectively has no user interface; both legitimate and illegitimate transactions can occur with no signaling of any kind to the user. To confound matters, with the applications we examine, the RF component has been laid atop a pre-existing form factor where a physical action on the part of the end user was previously required to share the information stored on the object. With the addition of RFID, the same actions can be accomplished without physical contact, or indeed conceivably without any action on the part of the user at all. These changes force users to reconceptualize how these objects "work," violating established norms of information flow, an example of what Nissenbaum calls "contextual integrity" [Nissenbaum]. Because users can unwittingly transmit information without having taken direct action on their part,[3] having a basic understanding of how RFID works (or being notified about this potential risk) is necessary in deciding whether or not to modify this risk to their privacy. As our initial examination discovered, users rely upon understandings of RFID that are often incorrect or based upon similar but not directly comparable technologies, and thus do not understand both the risks and how to mitigate those risks.

2. Related Work

To date, there is little published work investigating RFID and usable security. As ubiquitous technologies are still in their infancy, most extant work in usable security focuses on user interface and interaction design for software systems, although several researchers have developed frameworks to account for security and pri-

[1] This underscores a confounding issue in the RFID field today – while chips may conform to an ISO standard, the operating system software on the chip itself is proprietary, and thus chips and readers produced by different manufacturers may not interoperate. Purchasing an ISO 14443 compliant RFID reader in no way guarantees that you will be able to read a 14443 compliant chip.

[2] Heydt-Benjamin et al. were able to purchase a compatible credit card reader on eBay.

[3] Sophisticated malware today can find its way on to a user's computer without the user realizing they took some precipitating action, but the user still generally had to take some action, such as clicking a link, to initialize the download.

vacy issues in ubiquitous systems. Bellotti [Bellotti] introduced privacy principles for ubiquitous systems in 1993, focusing on the feedback given to the user and the user's control over the capture of data, what is done with the data once in the system, the user's ability to access and correct that data, and the purpose for ubiquitous data collection itself. More recently, Langheinrich [Langheinrich] proposed a set of privacy aware design principles for ubiquitous systems that draw upon the Organization for Economic Co-operation and Development's Fair Information Practices [OECD], targeting notice, choice and consent, and the need for security, among others. Expecting ubiquitous technology to be invisible to the user, Dourish [Dourish] has suggested reframing security for ubiquitous computing environments from the user's point of view instead of the designer's, to express security "not as mathematically grounded cryptographic concepts, but in terms that fit users' activities and needs at the time," in order to make them visible and comprehensible to the user. Kuo et al. [Kuo] used this approach in their study of the usability of configuration interfaces for wireless networking equipment, examining users' mental models of wireless networks, comparing them to the system or experts' model, and identifying areas where the two models were in conflict.

In reviewing the literature, the yet-to-be developed ubiquitous systems these various authors are envisioning, such as smart homes or ambient sensing devices, are implied through many of the principles they offer. However, the implementations of RFID we examine here bear little resemblance to these visionary systems and either cannot or choose not to adhere to these design principles. This is likely because they are generally primitive, first-generation systems, or as discussed in [Meingast], due to a lack of interest in or ability to assess the user's mental model of the system and map it to the deployment model to ensure usability. This is particularly a problem with systems designed by public agencies, which may not have the same incentives as the private sector or the expertise necessary to deploy user-centered design.

Due to length restrictions a comprehensive review of each system against these principles is outside our scope here, but in brief summary, the predominate system model we observed consists of an opaque, one-way flow of information (from chip to reader to system) with no opportunity for user querying or configuration, as well as a general invisibility into the inner workings of the system. This is typically compounded by a lack of educational information provided to users about how these systems operate, as well as any admission of possible risk and how to mitigate it. While the level of technical sophistication required to build the ideal set of privacy and security tools that would allow visibility to comprehend what is taking place is not possible in these systems presently, the consequences are that in systems where privacy and security controls are lax or lacking, users typically won't understand enough about how RF systems work in order to modify these risks, particularly when, as we discovered, users have significantly differing mental models of how these systems work than they actually do.

3. Methods

In this first phase of our project, following an approach outlined by Morgan et al. [Morgan], we conducted a series of exploratory qualitative interviews, structured to elicit subjects' mental models of radio communication generally, and of existing implementations of RFID technology specifically. The analysis of mental models is well established in usability research, and is appropriate for ascertaining users' understanding of their tools and those tools' vulnerabilities.

Building on theory developed by Craik [Craik], Johnson-Laird argues in [Johnson-Laird 1983] and [Johnson-Laird 1989] that mental models are a central feature of cognition and comprehension. Norman has famously applied this theory to system design and usability, describing the critical features of useful models [Norman], in addition to advocating comparison of users' models to expert models of systems. Morgan et al. [Morgan] have applied mental models to the study of risk communications in an effort to create "public-centered" risk information, a concept easily applicable to usable security. With respect to RFID specifically, [Makela] and [Poole] have used a mental models approach to explore user comprehension.

As a preliminary stage in developing our interview protocol, we recruited nine subjects to meet distinct cases outlined by two three-state criteria: general technical familiarity (novice, intermediate, advanced) and possession of particular RFID devices (transit card, credit card, and e-Passport). Subjects completed a short baseline survey (Appendix I) regarding their use and familiarity with various wireless technologies. A subject's responses then served as the starting point for a semi-structured interview in which the subject described when and how he/she used a particular device. The interview protocol was designed to probe for the rationale and reasoning behind the users' actions, as well as for their perceptions of the benefits and costs of using RFID-enabled devices. Near the completion of the interview, subjects were given or shown communication

materials produced by the issuer (e.g. a pamphlet, webpage, or online movie providing an overview of how to use the object) and then asked to explain if the material aided their understanding of the object's operation in any way.

As Norman [Norman] and others have cautioned about difficulties with the elicitation of mental models, we tested several inductive approaches focused on actual use cases, usage scenarios, and comparison to other technologies. Rather than immediately ask subjects directly to describe the workings of the devices they had used, we focused on use cases, inferring and eliciting subjects' assumptions and mental models based on their described actions. Subjects were also encouraged to draw comparisons to other RF-based devices, in the hopes that those comparisons would further expose their understanding their RFID-enabled devices. We did not assume any prior knowledge of RFID on the part of the subjects, but did require that each had used at least one of the required devices.

Building on the principles noted in the previous section, we developed the following framework of "security" and "privacy" to provide consistency to our interview process. In considering the context in which these objects are used, a secure implementation from a user's perspective would be one where the data on the chip were protected from unauthorized access or alteration, and where reader–chip communication was encrypted and not subject to eavesdropping. An implementation that protects individual privacy would not allow the chip to be queried without user's consent and knowledge; data broadcast by the chip should not allow a third party to track or infer information about the user (e.g. a static identifier that could be associated with that user); and the object would make available (or be easily used with) a physical shield to prevent all RF communication without explicit consent of user.

4. Initial Findings and Analysis

Common themes in subjects' perceptions of the benefits of RFID devices were ease of access to physically restricted areas, speed, and convenience. Even subjects who were not interviewed about their use of toll tags often volunteered them (FasTrak, EZPass) as a baseline for comparison, noting expectations of special treatment (such as dedicated queues) and faster transactions. Metaphorical comparisons to more familiar RF-based technologies (such as garage door openers) proved useful in eliciting subjects' perceptions of RFID.

Our survey results showed a remarkable disjunction in subjects' comfort levels with various usage scenarios. While subjects across levels of technical familiarity were generally comfortable using RFID technology for applications they perceived as either having a single-purpose or limited in the type or amount of data shared, such as home/office entry or toll collection systems, subjects were more wary of applications that had multiple purposes or that involved personal or financial data. Whether this is related to perceived sensitivity of the data stored on the latter devices or an indication that users' mental models include notions about where the use of wireless communication is appropriate will be a critical question for the next phase of our investigation.

While our advanced subjects understood how RF readers and chips communicate and were aware that radio signals could be blocked, our novice and intermediate subjects with little or no grasp of radio communications generally could not explain how RF functioned ("magic" and "witchcraft" were explanations suggested by novices). While most novices and intermediates were aware of circumstances when RF products had difficulty in transmitting or functioning, none had a systematic understanding as to what factors could affect this. When attempting to explain how RF worked, novices and intermediates tended to make comparisons to optical scan technologies with similar use cases, such as bar codes, than to more technically similar radio broadcast technologies with the expectation that a chip had to be in visual line-of-sight proximity to a reader. This notion is contradictory to the omnidirectional way in which radio signals are typically broadcast, a subtle distinction that may have implications for design and security. Finally, several subjects expressed the hope and/or assumption that RFID chips were reader-specific, and were not aware of formal communication standards.

All subjects were accustomed to visible or audible feedback upon their RFID-enabled devices being read, and indeed universally expected it. Most were not aware that reading was possible from distances greater than a few inches, nor that chips could be read without visual or audio feedback, or for that matter, without their consent or knowledge. This finding, coupled with the lack of understanding of RFID's 'always-on' broadcasting, is something we intend to explore in more depth in the next phase of our project. Recognizing these features is crucial to users' taking steps to mitigate risk, particularly when physical shielding is required to block RF transmissions.

Subjects were generally unaware whether or not any security measures were in place for the objects we examined. This is understandable: in reviewing online

(and offline, when available) documentation for each of these objects, with the exception of the e-Passport none discussed any security measures or any potential risk. In the case of the e-Passport, this communication was poorly made; when presented with an official e-Passport brochure describing the passport's security features, upon review subjects were generally unable able to ascertain what risks were present or what security measures were in place.[4]

Finally, subjects were unaware of what data was stored on each object, often assuming far more (such as a social security number and home address on the credit card) than was actually stored. Again, this was understandable, since the vendors did not publish this information in their public communications materials. Lack of knowledge about what data was stored on each object made it difficult for subjects to accurately assess risks, their comfort level with risk, and contributed to a lack of transparency that in turn obfuscated subjects' mental models.

5. Future Work

In this exploratory phase we discovered that intermediate and novice subjects, lacking an understanding of how RFID functions, generally rely upon their experiences with optical scan technologies to reconcile their (mis)understandings of RFID. While subjects overwhelmingly associate RFID with creating efficient, friction-free transactions, their level of comfort with these uses was reliant upon the sensitivity of the information and the context of its use. Subjects of all experience levels expected visual or audio feedback when an RFID chip was read, and nearly all of our subjects were unaware that RFID readers could operate without providing them feedback. While we were not surprised to find that most subjects had a minimal or factually incorrect understanding of RFID's potential security risks, of particular concern is the reliance upon a mental model based upon optical line-of-sight technology; failing to understand the omnidirectionality of RF communication may lead users to miscalculate their level of risk, in particular with implementations that require direct action, such as shielding, on the part of the user to prevent RF transmissions.

We plan to continue this study in 2008 with a larger number of subjects by refining our protocol and narrowing our focus to the two devices in which RFID was introduced onto an existing form factor: e-Passports and credit cards. Our exploratory work revealed one weakness in our protocol: novices struggled with some of our questions and thus it became clear we needed to adjust the phrasing to make novices more comfortable with discussing technology they knew little about. We also plan to remove transit cards from our study for both practical reasons (*i.e.* to reduce complexity and because they are not yet in widespread use in the Bay Area) and because the cards do not store personal information about the card holder, and thus are not as directly comparable to the other two devices we examine. Due to the growing number of credit cards and passports in circulation, as well as planned initiatives in 2008 by the Department of Homeland Security and several U.S. states to incorporate RF chips into passport "cards" and driver's licenses, gaining a clearer understanding of users' mental models of and concerns with the use of RF in identity documents and payment cards is imperative to ensure secure, privacy-protecting, and user-friendly implementations of RFID [Federal Register].

Citations

Bellotti, V. and Sellen, A. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the third conference on European Conference on Computer-Supported Cooperative Work*, Milan, Italy, 1993.

Craik, Kenneth J.W., *The Nature of Explanation*, Cambridge and New York: Cambridge University Press and The MacMillan Co., 1943.

Department of State. Fact Sheet: Western Hemisphere Travel Initiative Passport Card Technology Choice: Vicinity RFID. http://www.dhs.gov/xnews/releases/pr_1161115330477.shtm. Last accessed January 14, 2008.

Dourish, P., Grinter, R., Delgado de la Flor, J., Joseph, M. Security In the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. Springer: Personal and Ubiquitous Computing, 2004, 391-401.

Federal Register. Card Format Passport; Changes to Passport Fee Schedule. Vol. 72, Number 249, December 31, 2007. Pages 74169-74173.

Floerkemeier, C., Schneider, R., Langheinrich, M. Scanning With a Purpose: Supporting the Fair Informa-

[4] Notably, most subjects never received the printed brochure with their passport, or they failed to read it. The information presented on the brochure differs than that available on the Department of State website where a clearer description of security measures and threats are available at http://travel.state.gov/passport/eppt/eppt_2788.html.

tion Principles in RFID Protocols. In *Second International Symposium on Ubiquitous Computing Systems*, Springer (2004), 214-231.

Hachman, M. IBM Develops Scratch-off RFID Tags. ExtremeRFID, November 2005. http://www.extremerfid.com/article/IBM+Develops+ScratchOff+RFID+Tags/164620_1.aspx. Last accessed January 14, 2008.

Heydt-Benjamin, T.S., Bailey, D.V., Fu, K., Juels, A., O'Hare, T. Vulnerabilities in First-Generation RFID-Enabled Credit Cards. In *Proceedings of Eleventh International Conference on Financial Cryptography and Data Security*, Lowlands, Scarborough, Trinidad/Tobago, February 2007.

Johnson-Laird, P.N. Mental Models. In Posner, M. I., ed. *The Foundations of Cognitive Science*. Cambridge, MA: MIT Press, 1989. 469-499.

Johnson-Laird, P. N. *Mental Models: Toward a Cognitive Science of Language, Inference, and Consciousness*. Cambridge, MA: Harvard University Press, 1983.

Kuchinskas, S. EPassports Could Have Blocking Mechanism. Internetnews, December 3, 2004. http://www.internetnews.com/security/article.php/3443671. Last accessed January 14, 2008.

Kuo, C., Goh, V., Perrig, A., Walker, J. Empowering Ordinary Consumers to Securely Configure Their Mobile Devices and Wireless Networks. CyLab Technical Report, CMU-CyLab-05-005, December 2005.

Langheinrich, M. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. Ubicomp 2001. Springer, Atlanta, GA, USA (2001) 273-291.

Mäkelä, K., Belt, S., Greenblatt D., Häkkilä, J. Mobile Interaction with Visual and RFID Tags – A Field Study on User Perceptions. CHI 2007.

Meingast, M., King, J., Mulligan, D. Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport. In *Proceedings of IEEE International Conference on RFID*, 2007, 7-14.

Morgan, M.G., Fischoff, B., Bostrom, A., Atman, C. Risk Communication: A Mental Models Approach. Cambridge, UK: The Cambridge University Press, 2002.

Nissenbaum, H. Privacy as Contextual Integrity. Washington Law Review Vol. 79, No. 1, February 2004: 119-157.

Norman, D. Some Observations on Mental Models. In Gentner, D., and Stevens, L., eds. *Mental Models* Hillsdale, NJ: L. Erlbaum Associates, 1983. 7-14.

Organization 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. http://www.oecd.org/document/20/0,3343,en_2649_201185_15589524_1_1_1_1,00.html. Visited January 22, 2008.

Poole, E.S., Le Dantec, C., Eagan, J., Edwards, W.K.: Calm Computing or Paranoid Computing? Unintended Consequences of the Disappearing Computer. 2007, currently unpublished.

Appendix I – User Survey

UC Berkeley Technology Study

Thank you for participating in our research study! Before we get started, we'd like to take a few minutes to ask you some questions about your familiarity with different wireless technologies. Your answers will be kept confidential. Unless otherwise indicated, please circle your responses. After you have completed this survey, we will review your answers with you.

Remember that we are interested in your opinion – there are no right or wrong answers.

1. In general, how would you rate your understanding of technological products?

Little to no understanding	Moderate understanding	Advanced understanding

2. Below is a list of different types of products that use wireless technology.
For each product, please indicate:

1 - I've used this product before, and I understand how the technology works.
2 - I've used this product before, and I sort of understand how the technology works.
3 - I've used this product before, and I have no understanding of how the technology works.
4 - I've never used this product before.

Product	Have used and understand	Have used and sort of under-stand	Have used and have no under-standing	Haven't used
Garage door opener	1	2	3	4
Keyless entry remote for car	1	2	3	4
Keyless entry ID card or badge	1	2	3	4
FasTrak toll transponder	1	2	3	4
Computer using wireless internet (wi-fi)	1	2	3	4
Mobile phone	1	2	3	4
GPS unit (handheld or car)	1	2	3	4
ID chip implanted in your pet	1	2	3	4

3. Have you heard of the term "smart card" before? Yes No

4. Do you own any smart cards? Yes No Don't know

5. Have you heard of the term "RFID" before? Yes No

6. To the best of your knowledge, do you own any products that contain RFID? Yes No Don't know

If yes, please list:

7. Please rate your personal understanding of how RFID technology functions:

Little to no understanding	Moderate understanding	Advanced understanding

8. What is your general impression of RFID?

Negative	Somewhat negative	Neutral	Somewhat positive	Positive

9. Please rate your comfort level with the following scenarios:

A. Using a keyless/contactless device to gain access to your home:

Very uncomfortable	Somewhat uncomfortable	Neutral	Somewhat comfortable	Very comfortable	Don't know

B. Traveling with a prepaid contactless transit pass:

Very uncomfortable	Somewhat uncomfortable	Neutral	Somewhat comfortable	Very comfortable	Don't know

C. Making a purchase using an contactless credit card:

Very uncomfortable	Somewhat uncomfortable	Neutral	Somewhat comfortable	Very comfortable	Don't know

D. Traveling with a contactless/electronic passport ("the new e-passport"):

Very uncomfortable	Somewhat uncomfortable	Neutral	Somewhat comfortable	Very comfortable	Don't know

Thanks! Before you finish, can you please:

10. Tell us your gender:

Male	Female	Decline to state

11. Tell us your age:

Under 18	18-24	25-34	35-44	45-54	55-64	65 and over	Decline to state

Thank you for your time!