In: Alfred Kobsa, Ramnath Chellappa and Sarah Spiekermann, eds.: Proceedings of PEP06,
CHI 2006 Workshop on Privacy-Enhanced Personalization, Montréal, Canada.

Better RFID Privacy Is Good for Consumers, and Manufacturers, and Distributors, and Retailers

David H Nguyen and Alfred Kobsa
School of Information and Computer Sciences
University of California, Irvine
Irvine, CA 92697
[dhn | kobsa]@uci.edu

ABSTRACT*

When the term RFID (Radio Frequency Identitification) is mentioned these days, it is followed not far behind by the term privacy. For all of RFID's potential to benefit manufacturers, distributors, retailers and consumers, the fear of privacy intrusion is preventing the technology from gaining acceptance. This privacy concern is largely due to the fact that RFID tags can be read by any RFID reader, without prior notice or consent. The fear is that as consumer goods are tagged, consumers wearing or using those goods can also be tracked, especially without the consumers' knowledge. We present a scenario whereby it will behoove the retailers to deal with privacy for their own sake, and in return, the consumers may also benefit from the retailers' solutions to the problem of tag reads that are both anonymous and invisible. We argue that better RFID privacy is not only good for consumers, but also for manufacturers, distributors, and retailers.

Author Keywords
RFID, privacy, personalization.

INTRODUCTION

One of the biggest proponents of RFID technology is the consumer goods industry. By tagging their products with a globally unique Electronic Product Code (EPC) that can be read remotely, the entire inventory and supply line can be made more efficient, which is expected to translate into large cost savings [3]. To gain acceptance of the technology, the proponents will likely press the value proposition for the consumers.

Benefits

A typical scenario to show the benefits for consumers takes place in the context of grocery shopping. When all items of a grocery store are tagged, the consumer can walk into a grocery store and some of the following can happen:

1. The shopping list (which was generated by the fridge at home) transfers to the shopping cart.
2. The cart can tell the shopper what items on the list are in stock, and show where to find them in the store.
3. As each item is added to the cart, the shopping list automatically updates.
4. The cart can show specials/promotions.
5. The consumer can view additional product information (recipes, reviews, etc…)
6. With personal information from an RFID-equipped loyalty card, allergies can be pointed out and needed nutrients can be recommended.
7. All the while, the cart can show a running total of all items.
8. Finally, the checkout is done by simply paying for what the cart has already scanned all along.

Afterwards, when the consumer is home, more benefits are possible:

9. Easy access to product-related information (recalls, recipes, instructions for assembly or usage, warranty information, location of repair shops, how to order parts, etc…).
10. The refrigerator can automatically update the food supply status, including what has been used and what will soon expire.
11. Items can be shown to friends, who can scan the product ID to also buy one.
12. When thrown away, the items can help the waste management department automate the recycling process.

Costs

However, the benefits of RFID, in its current form and implementation, are not without costs. Privacy advocates point out the fact that RFID tags will reveal their information to any RFID reader that asks. Moreover, the scanning and reading of tags is invisible to the human eye. Then it would be possible to have readers under doormats that keep track of which globally unique shoes have entered and left a certain place (see the EPC Discovery Service proposed in [1]). As people tend to wear their shoes for years, a database can track where that person has been.

* This research was supported by DST grant No. 0308277 of the National Science Foundation, and by a Research Prize of the German Alexander von Humboldt Foundation.

Turning the Situation Around

Anonymous, invisible reading of tags is one of the biggest arguments against RFID [2]. Adding authentication functionalities to the tags will increase cost, an unwanted option for everyone. Up till now, proponents of RFID saw little additional benefits, even for themselves, if the reading of tags were authenticated and accountable. Even simple post-purchase protection by a consumer-specified password [4] is precluded by the fact that current RFIDs are not rewritable for cost reasons.

For the sake of argument, we simplify the production and consumption chain for consumer goods to:

- *Manufacturers* who make the actual products
- *Distributors* who transport the products from the factories to the stores
- *Retailers* who sell the products to people
- *Consumers* who consume the products

There are more stakeholders in the chain, but let us work with these four for now.

Assume for a moment that the proponents of RFID (the non-consumers) "get their way" and that every item in the store is tagged with an unsecured EPC that can be read anonymously. We will demonstrate that this would make, specifically, retailers vulnerable to more effective price competition and, generally, manufacturers, distributors, and retailers vulnerable to corporate espionage by competitors.

We predict the introduction of a handheld device with an integrated RFID reader and a wireless connection to the Internet. Optional add-ons could be a small integrated keyboard or an optical scanner. Such a device could be built relatively easily from existing components. It could be held in one's palm or strapped to one's wrist, and it would be easily concealable.

With such a device, customers could easily read the EPCs of products in their vicinity and use them to look up competitive offers from price comparison websites. This would allow them to obtain a product for a better price from an online vendor, or give them a better idea of the competitiveness the retailer's prices.

Customers could also walk through the aisles of the store and automatically transmit its complete inventory to a citywide database. This information could be used by others, e.g. to decide whether it is worth driving to a specific store (and thus potentially lead to a loss of store visitors). It can, however, also be connected with information from product recommendation sites and allow customers in the store to find out immediately whether a better-rated product of the same type is available elsewhere in the city.

By punching in store prices or reading them with the optical scanner of the device, customers could even populate the citywide inventory databases with the prices of stores. The handheld device may even be able to gain access to the retailer's price database (after all, the merchant's computer in the customer's shopping cart has access to it). If so, then automatic price collection and transmission to the citywide database would be possible by simply walking through the store.

The handheld device would not only be valuable to customers, but also to competitors. By wandering the store (or scanning a warehouse) every other day or so, competitors can get a history of which products are selling (recall that EPCs are unique per item), which products are stagnant, and which products are even offered [5]. The competitor could also get a layout of the products in the store and see if that layout is effective or not. The same technology can be used by other manufacturers or distributors for corporate espionage.

Of course, the functionality of this handheld device can be achieved at the moment using current barcodes and barcode readers. The argument is not to show that RFID will enable something that was not possible before, but that RFID makes scanning far more efficient. And when a process is more efficient, it encourages practices that were not done before, even if they were possible. If checking for lower prices were to become a trivial task, a task which requires neither extra energy nor effort, people will just do it.

By giving out information about their products and inventory so easily, manufacturers, distributors, and retailers inadvertently give away competitive advantages.

RESEARCH QUESTIONS

Presumably, retailers will not want unintended exploitation of their RFID deployment; neither do the manufacturers nor distributors. It will therefore become vital for them to be more "private" with their information. Privacy for these three groups is seemingly different from the privacy for consumers. What are the differences that set them apart? More importantly, how are they the same? How can privacy of these four stakeholders be aligned?

Another topic of concern is infrastructure. Ownership of the product will change hands as it flows from the manufacturer to the distributor to the retailer to the consumer. Each owner will want control of the RFID tag to serve their respective needs. The change of ownership will require an infrastructure. How much infrastructure is needed? If an infrastructure was set up to enable RFID access-control for pre-sales activities, how well could it align with consumer privacy needs? Who will fund this access control infrastructure? Would it benefit the pre-sales entities to form a group to administrate the infrastructure? If so, how can we ensure that consumers' privacy interests are also supported?

CONCLUSION

Given the scenario of inventory/price scanning and publication, and similar non-intended exploitations of unsecured RFID tags, it seems that manufacturers, distributors, and retailers have two options. They could deploy the current unsecured RFID technology, but then consumers and competitors could exploit the same weaknesses, that privacy advocates fear, to their own advantage. The proponents could instead push for changes in RFID technology, especially those that will protect their own interests for privacy. In turn, consumers' privacy may also be strengthened.

Privacy, it seems, is not only good for the consumers, but also for manufacturers, distributors, and retailers. This may increase the pressure to deploy privacy-enabling RFID technology at reasonable costs.

REFERENCES

1. VeriSign (2004): The EPC Network: Enhancing the Supply Chain. http://www.verisign.com.au/guide/epc/epc_whitepaper.pdf
2. Garfinkel, Simson & Rosenberg, Beth, eds. (2005): *RFID: Applications, Security, and Privacy*, Addison-Wesley Professional, ISBN 0321290968.
3. Hardgrave, B.C., Waller, M., and Miller, R. *Does RFID Reduce Out of Stocks? A Preliminary Analysis*. RFID Research Center, Information Technology Research Institute, Sam M. Walton College of Business, University of Arkansas, Nov 2005.
4. Spiekermann, Sarah and Oliver, Berthold (2005): *Maintaining Privacy in RFID Enabled Environments: Proposal for a Disable Model*. In Robinson, Philip; Vogt, Harald; Wagealla, Waleed, eds.: Privacy, Security and Trust within the Context of Pervasive Computing. Vienna, Springer Verlag, ISBN 0-387-23461-6.
5. Stapleton-Gray, Ross (2005). *Would Macy's Scan Gimbels?: Competitive Intelligence and RFID*. In Simson Garfinkel & Beth Rosenberg, eds. (2005): *RFID: Applications, Security, and Privacy*, Addison-Wesley Professional, ISBN 0321290968.