MAINTAINING PRIVACY IN RFID ENABLED ENVIRONMENTS

Proposal for a disable-model

Sarah Spiekermann[1], Oliver Berthold[2]
Humboldt University Berlin, Unter den Linden 6, 10099 Berlin, Germany
[1]Institute of Information Systems, sspiek@wiwi.hu-berlin.de
[2]Department of Computer Science, berthold@informatik.hu-berlin.de

Abstract: The presence of RFID technology in every-day life is expected to become a reality in the near future. Yet, as RFID tags enter consumer households and threaten to identify their owners' belongings, whereabouts and habits concerns arise about the maintenance of privacy. People are afraid of being 'scanned' or tracked with the help of a technology that is invisible to them and not under their control. To address this consumer concern standardization bodies such as the Auto-ID Center have proposed to integrate a kill functionality into RFID tags. The present article argues that killing tags at the store exit is, however, not a viable long-term strategy to ensure *default* privacy. Too many business models and services are already in the pipeline to use RFID functionality after a purchase has taken place. Economic interest and consumer benefits risk undermining widespread tag killing. As a response to this dilemma we propose a simple *disable*/*enable* mechanism. Our suggestion is to disable all tags by default as part of the shopping check-out process and provide consumers with a password that enables them to re-enable their objects' tags if needed.

Key words: RFID, Privacy Enhancing Technologies, Privacy

1. INTRODUCTION

RFID technology is a major enabler of ubiquitous computing environments or the pervasive Internet as described and researched by technologists. Today, the technology is introduced to facilitate supply chain management. Yet, as the technology's cost decreases it also allows for new

business models and applications beyond logistics. In fact, manufacturers, retailers and consumers can all take advantage of the technology's ability to uniquely identify objects, view their characteristics and relate to their owners. Intelligent home environments, improved reclamation and recycling processes, brand protection, safety- and security applications, but also less queuing time in super markets and more personalized information services count among the myriad benefits expected from 'living' RFID tags at the item level. Due to these benefits we argue that it is unrealistic to expect RFID tags to be systematically killed at store exits.

As this is true, considerable privacy concerns are accompanying the introduction of RFID technology. Public debate is rising over the potential presence of smart chips in all of peoples' belongings. Privacy rights organizations call for a complete abolition of tags in all those areas where they can be in touch with people [10]. *Uncontrolled* technology surrounding us and even in our cloths opens up a whole new dimension for the privacy debate which has the potential to considerably damage well established brands (figure 1). As a result, we argue that industry investment in privacy enhancing technologies (PETs) along with pro-active transparency should be part of any RFID introduction strategy.

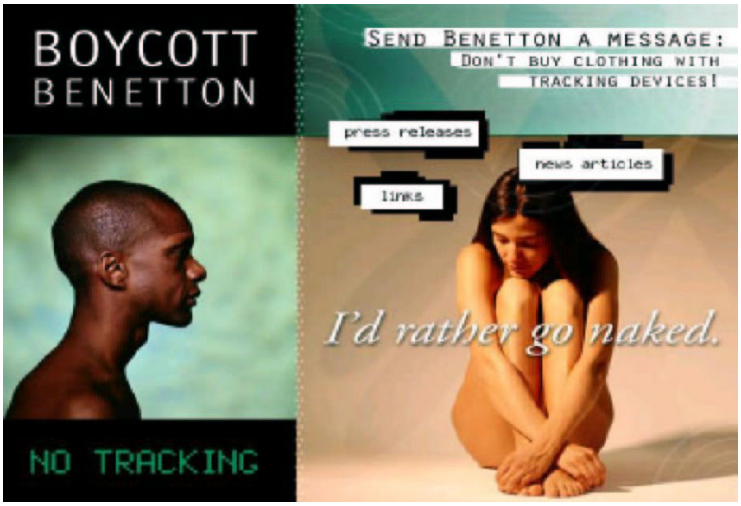

Figure 1: Example of how the privacy debate can impact the brand

Certainly, privacy is a multi-layered challenge when it comes to RFID. Section 2 will give a brief overview of the issues raised. Yet, what has strongly dominated public debate so far is peoples' fear to be spied on by others, to be scanned and tracked. The immediate response by technology

developers and early adopters has been to integrate a kill function into the specification of RFID tags (see section 3). Yet, even though 100% killing of all tags would be the perfect privacy solution economic interest risks undermining this approach to be used *by default*. In section 3, the current article therefore suggests to replace the kill function with a disable/enable function. The disable/enable model does not prohibit RFID tags' after-sales benefits. Instead it puts the use of RFID tags under peoples' control who can re-enable tags any time they need to (with a personal password). With this, our solution integrates industry, consumer and visionaries' interests.

One major cornerstone of our proposal is the *default* disabling process we recommend for supermarket check-out systems. Even though the discussion of such an automated check-out system is not subject of this article it still is an important requirement to make our solution work from a privacy perspective. While tag killing could only be applied to those goods where there are definitely no after-sales use scenarios, tag disabling can always be applied to all goods without after-sales sacrifices.

Section 4 closes with an acknowledgement of the challenges accompanying our proposal, especially password management, tag- and infrastructure cost.

2. IMPACT OF RFID ON PRIVACY

Consumer privacy is discussed today on the basis of three distinct temporal phases (see figure 2): in the retail outlet, at the retailers' check-out and outside of the retailers' premises.

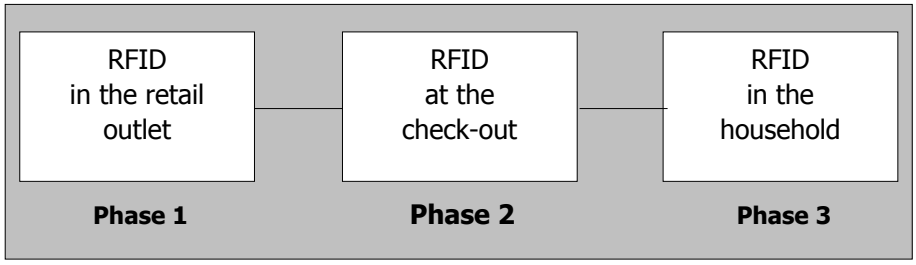

Figure 2: The 3 phases of the RFID Privacy Debate

RFID in supermarket premises (phase 1) allows for the creation of comprehensive profiles on how people move through the store [13]. These can be used to analyze how they buy in a similar way as is the case today for web click-stream data collected in Internet stores. Privacy activists

consequently call for not using RFID tags in retail outlets [10]. Especially when RFID tracking data is combined with video surveillance techniques concerns are high [5]. Early in-store trials, e.g. at the GAP were stopped [7].

Assuming that RFID will be used in retail outlets, privacy activists have stressed the point that at least when paying for goods (phase 2) it is unacceptable to have consumers queue again for deactivating tags [5]. Other sources call to "…prohibit merchants' pressure tactics to coerce keeping the tag alive…" ([9] citing a hearing before the California State Senate). As a result, deactivation, whether this means killing or disabling of the tag, needs to be integrated into the payment process.

Another thread of fear relevant at the supermarket check-out (phase 2) is concerned with the combination of highly granular EPC data with personal identity data.[1] Personal identity data is usually collected with the help of loyalty cards. Combining a person's identity at the moment of purchase with such detailed product information allows for a degree of psychographic segmentation of individuals that has not been available before.

Finally, direct abuse is feared of RFID tags' being read out uncontrolled and unnoticed of by unauthorized readers (phase 3). Thus, privacy could be intruded if people or institutions with readers were able to read out unrecognized on the belongings and whereabouts of others. This fear is fueled by the fact that information stored on an RFID tag can be read out unnoticed and from a distance.

3. PRIVACY ENHANCING FUNCTIONALITY FOR RFID TAGS

3.1 Background

The discussion has shown how and why privacy concerns arise around RFID technology. In the remainder of this paper we will focus on how privacy could be enhanced in phase 3, thus when people take RFID tags home and are tracked or read out unnoticed by others.

Version 1.0 of the EPC Network Specification [2] distinguishes several tag classes (currently form 0 to 5) depending on their sophistication as far as

[1] Similar to the bar code, the Electronic Product Code, EPC, contains a serial number that can be related to a product category and a manufacturer. However, the EPC also contains a unique serial number associated with more detailed and comprehensive back-end data. This allows for retrieving an object's detailed characteristics, history and potentially other related data (Auto-ID Center, 2002).

memory, power supply and communication range is concerned. A kill function is foreseen in conjunction with an 8- or 24 bit password scheme even for the simplest and lowest-cost type of tag class 0 and 1.

However, as we have outlined in section 1, economic interest is likely to impede a widespread killing of tags by default. Therefore, we would suggest replacing the kill function in the specification with a password protected enable/disable mechanism. Depending on product nature and value we would propose two types of privacy enhancement with different levels of security and tag cost attached to them. In essence we argue that read-only chips (classes 0 and 1) should not be the long-term mass market solution for item level taging. From a privacy perspective we strongly believe in the necessity to use tags with some write-capability in order to integrate long-term viable privacy functionality. Table 1 gives a requirements overview of privacy functionality foreseen for class 0 and 1 tags in comparison to our proposal described below.

RFID tag specification	**Class 0/1**	**Type 1 priv. enhmt.**	**Type 2 priv. enhmt.**
Memory			
ROM	**X**	x	x
EEPROM	x	**X**	**X**
Objects in Memory			
8 or 24 bit password related to kill function	**X**		
24 bit password to disable or enable the EPC		**X**	**X**
Status (enabled/disabled)		**X**	**X**
Operations			
Kill EPC function	**X**		
Verify (kill-)password	**X**		
Cryptographic one-way function			**X**
Disable function (to disable EPC based on password)		**X**	**X**
Enable function (to enable EPC based on password)		**X**	**X**
Verify password to disable/enable EPC		**X**	**X**
Change password		**X**	**X**
Generate random number (pseudoRNG)			**X**
XOR function			**X**

Table 1: RFID tag functionality relevant in the privacy context and potential enhancements

3.2 The Disable Model

The enhancement we propose is to integrate a *disable/enable*-function instead of a kill function into tags. We distinguish between two types of disablement. Type 1 implies a simple exchange of the kill function with a disable-function. The goal here is not to provide for perfect cryptographic protection of tag information, but to have good-enough protection in place to prohibit wide-spread tracking and spying. This is suitable for low-cost goods. Type 2 privacy enhancements include a more sophisticated crypto-based password scheme similar to proposals of other researchers (e.g. [14]). This type of more cost intensive privacy enhancement only makes sense in the context of high value goods.

- **Type 1 privacy enhancements**

The way we envision the disabling process to flow is as follows: Instead of storing the kill password and function, the RFID tag stores a 24-bit *enable/disable* password and function. When a consumer pays for his products all tags are by default and automatically disabled. The disabling process is handled by the cash-registrar in order to avoid consumer time cost. With disablement a new password is randomly set on all tags. This one password is printed out on the customer's receipt.[2] It can be used by the new product owner to potentially re-enabling the EPC if needed for recycling, reclamations or intelligent home applications.

If unauthorized reader devices request the EPC from a disabled tag without the correct password the tag denies access to the EPC stored on it. From a layman perspective this means that *by default* objects bought do not communicate with any reading device except at one's personal request. The approach thus lends itself to calm all those privacy concerns related to unauthorized tracking and spying. At the same time, all economically driven intelligent home appliances and future consumer information needs are maintained. Trust in back-end reader architecture is not required. Control resides completely with the user.

From a technical perspective, of course, the tag still reacts to process re-enable requests. At this point several issues can arise from a security perspective: The most important one is that it is possible for an adversary to not decipher the password, but instead mime an anti-collusion procedure. Anti-collusion is a function used to uniquely recognize and communicate

[2] Long-term, the password will probably be transferred to an identity device such as a PDA owned by the consumer.

with one tag when several tags respond at the same time. If anti-collusion is now based on the EPC - the structure of which is standardized - our disable-proposition could be circumvented. Our solution therefore relies on the fact that the EPC itself is not used for anti-collusion. At first sight, this may be considered a major drawback of our solution. Yet, requirements in logistics suggest that full EPCs are not suited as a numbering scheme for anti-collusion anyways. Forging through a full EPC is too time consuming. Therefore, other numbering schemes have been proposed for anti-collusion including EPC dependent hash-values, a random number pre-integrated in the tag, RNG integrated into tags or a 12 to 14 bit serial number extract from the full 96 bit EPC [3]. For all these suggestions, our solution is feasible.

The second security weakness that may be argued is that a 24-bit password scheme is not a 'good-enough' protection. We argue that the effort required by an adversary to decipher a 24 or 32 bit password is not worthwhile if the result is nothing, but the EPC of a low-cost/low involvement product. We therefore argue that the cost-benefit rationale of most adversaries in most situations will effectively protect consumers.

The third drawback is that there will be authorized readers (e.g. at the cash-register or in the consumer's smart home) which send the new owner's password around in plain text without encryption. A serious attacker, e.g. a thief, could therefore sniff on the cash-register or home environment and retrieve the password. Again, we would argue that for low-cost products the incentive for thieves or other adversaries is rather low.

Yet, for higher value objects (such as CD players, TVs, etc.) a systematic 'spying-attack' of this sort, e.g. on private homes could be realistic. Consequently we argue that for higher-value goods another (more sophisticated) password scheme may be necessary referred to here as type 2 privacy enhancement.

- **Type 2 privacy enhancements**

In order to defeat sniffing practices on high value goods, type 2 privacy enhancements foresee a challenge response method to verify the password. This method is based on a typical cryptographic one-way function [4]. First the tag sends a randomly generated value to a reader. Here, a pseudoRNG may be the most realistic solution for 'good-enough' security, where a standard RNG solution is too costly. The reader answers with a combined hash from the random value and the password. Using the same one-way function, the tag can then verify the reader's password.

The vulnerability of this procedure is that in the moment of resetting the password the new password is transmitted in plain text. An adversary could thus sniff on the new password (e.g. at the cash-register). In order to defeat

such an attack the Vernam-Chiffre, a simple XOR function using the old password as the key to encrypt the new password can be applied for password re-set [11].

Compared to solutions proposing published hash functions or symmetric encryption for RFID environments [8,12,14] our solution does not require a database for personal tag management. Only one common password is used by a consumer or household. Switching product ownership implies just two password changing steps using a randomly selected temporary password. Key management is equally not required. This makes our solution more cost efficient and less complex.

4. DISCUSSION

Obviously, both types of privacy enhancements imply additional cost for tag manufacturers. The most important cost driver is that the privacy enhancements we propose require tag manufacturers to use non-volatile and re-writeable memory (e.g. EEPROM) instead of ROM for all item-level tags. Even though this is generally foreseen for tags of class 2 and upwards, the current specification does not include it for those low-cost tag classes 0 and 1. In addition to this memory cost the tags would need to be able to integrate two (or even five) additional functions[3].

Disabling a tag as we propose here only from time to time does not make sense. Our proposal integrates the requirement that the disable process itself takes place automatically when goods are checked out at the cash-register. While the disable model allows for default privacy and is therefore superior to the kill function industry players will argue that integrating disablement in cash-registers is costly. We argue that this may be true, but privacy needs justify the investment. With RFID cash-registers will undergo considerable technical changes in any way. Disabling will only be an additional requirement.

Password management has been a criticism for the proposed solution. Password management can be a challenge in moving goods through the supply chain as well as in the user domain. Yet, as far as logistics is concerned our proposal is identical to the kill model. Probably, password information is transferred along with EPC information. When consumers take products home future scenarios foresee home agents and identity management systems [1] which manage peoples' assets, data and access

[3] In fact, the loow cost RFID tags "Philips I-CODE SL2 ICS10/11" already contains all components needed for type 1 privacy enhancements, needing only a few design changes.

rights.[4] In our thinking, such an agent could check new goods into the home system and set all devices to *one common* home password. Consequently, future consumers would not have to remember a myriad of passwords for each product. We believe that common password architecture for home readers or smart homes makes sense as consumers can access their devises more easily. A back-end database containing all tag data as proposed by Weis [14] as well as processing infrastructure to test all possible passwords [6] is not required. In the short- and mid-term, passwords printed out on receipts also don't increase consumer transaction cost since proof concepts in recycling and reclamation have been based on receipts for the last decades.

Finally, from a security perspective our proposal does, of course, not allow for highest level protection as is needed in many application areas. However, we also do not believe that military-level security is required for yogurt cans or even stereos. Even if the 'one-common-home-password' we suggest would be decrypted, what would the thief learn more about my belongings than if he just unlocked the window and stepped in?

5. CONCLUSION

RFID technology will be a ubiquitous reality in every-day life in the future. This paper argues that economic interest seeks to maintain an RFID tag's functionality after a purchase has been made. On this basis it is argued that killing RFID tags is an unrealistic solution to preserve *default* privacy in the long run. The authors conclude that mass market RFID should be enhanced with privacy functionality which in our proposal implies write-enhanced memory. Two types of privacy protection are suggested implying different cost and sophistication.

The major benefit of the solution outlined is that the disable-model puts RFID communication into the sole control of the user. With this, the solution embraces current thinking in the development of PET technologies which takes a user-centric view. Secondly, a compromise is made between state-of-the-art security and what is economically feasible. Only 'good-enough' security is used to develop a proposition that will meet the privacy needs in a majority of situations. Finally, the model is the only proposition to our knowledge which allows for a realistic compromise between RFID-based market aspirations and business models on one side and peoples' desire for

[4] For a reference on agent solutions currently developed to address the challenge of increasingly complex password management see e.g. HP's work on the 'e-person': http://www.hpl.hp.com/research/iil/themes/eperson/eperson.htm

privacy on the other. Consequently, we believe that the disable-model is a good road to take.

6. LITERATURE

[1] Clauß, S., Köhntopp, M., 2001, Identity management and its support of multilateral security, Computer Networks, Nr. 37, 205-219

[2] EPC Global, 2003a, Version 1.0 Specifications for RFID Tags, http://www.epcglobalinc.org/standards_technology/specifications.html

[3] EPC Global, 2003b, Specifications for 900 MHz Class 0 RFID Tags, page 15, http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf

[4] Ivan Bjerre Damgård, 1988, Collision free hash functions and public key signature schemes, Eurocrypt '87, LNCS 304, Springer-Verlag, Berlin, pages 203-216

[5] FoeBuD e.V., 2003, Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, Presseerklärung, http://www.foebud.org/texte/aktion/rfid/positions-papier.pdf

[6] Juels, A., 2003, Privacy and Authentication in Low-Cost RFID Tags, Submission to RFID Privacy Workshop @ MIT

[7] McGinity, Meg, 2004, RFID: Is This Game of Tag Fair Play?, Communications of the ACM, Vol.47., No.1, page 15

[8] Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita, 2003, Cryptographic Approach to “Privacy-Friendly” Tags, Submission to RFID Privacy Workshop @ MIT

[9] Pottie, Gregory J., 2004, Privacy in the Global E-Village, Communications of the ACM, Vol. 47, No. 2, page 21

[10] Schüler, Peter, 2004, Dem Verbraucher eine Wahl schaffen – Risiken der RFID-Technik aus Bürgersicht, c’t, Heft 9

[11] C. E. Shannon, 1949, Communication Theory of Secrecy Systems; The Bell System Technical Journal 28/4, pages 656-715

[12] Shingo Kinosita, Fumitaka Hoshino, Tomoyuki Komuro, Akiko Fujimura and Miyako Ohkubo, 2003, Nonidentifiable Anonymous-ID Scheme for RFID Privacy Protection. to appear in CSS 2003 in Japanese.

[13] Spiekermann, S., Jannasch U., 2004, RFID in the retail outlet: implications for marketing and privacy, IWI Working Paper

[14] Weis, S., 2003, Security and Privacy in Radio-Frequency Identification Devices, Disseration at Massachusetts Institute of Technology (MIT)