By Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita

Cheap tags and technology simple and secure enough to ensure personal data privacy are required before retailers implement and consumers trust and confidently use them on a mass scale.

RFID Privacy Issues and Technical Challenges

In the future ubiquitous-computing environment, RFID tags will be attached to all kinds of products and other physical objects, even to people, and could become a fundamental technology for ubiquitous services where the tags are used to identify things and people automatically. However, despite this promise, the possible abuse (or just excessive use) by retailers and government agencies of RFID's tracking capability raises questions about potential violations of personal privacy.

Here, we discuss two protest campaigns—one against apparel manufacturer Benetton in Italy, the other against Tesco in the U.K.—that reflect the growing concern among consumer-privacy advocates regarding how RFID might affect personal data. Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN, www.nocards.org) criticized Benetton's plans to attach tags to its products, leading to a boycott of those products in 2003 [9]. Earlier this year, CASPIAN similarly criticized Tesco for conducting experimental trials of tags on a variety of its products [11].

illustration by Richard Downs

In order to increase consumer acceptance of RFID technology, RFID advocates must promote and implement comprehensive security measures, along with consumer education, enforcement guidelines, and research in and development of practical security technologies. Technical organizations (such as EPCglobal, Inc.) are developing standards for the Electronic Product Code, including its *Guidelines on EPC for Consumer Products* (www.epcglobaline.org public_policy/public_policy_guidelines.html). Japan's Ministry of Internal Affairs and Communications and Ministry of Economy, Trade, and Industry have jointly released RFID privacy guidelines (www.meti.go.jp/policy/consumer/press/0005294/0/040608denshitagu.pdf). Consumer advocates, including the Electronic Frontier Foundation, the Electronic Privacy Information Center, and CASPIAN, jointly released the *Position Statement on the Use of RFID on Consumer Products* in 2003 (www.privacyrights.org/ar/RFIDposition.htm). A bill that would impose strict limits on California's use of tags in state-issued identity documents has also been proposed [10].

A simple countermeasure—a built-in option designed to kill the functionality of an RFID tag when the consumer leaves the store—has been incorporated into the EPCglobal standard (Class 1 Generation 2 UHF Air Interface Protocol). For consumers, its purpose is easy to understand and thus easy to accept. However, killing a tag's functionality curtails the future potential use of RFID in consumer services (such as in smart refrigerators that automatically reorder food products, expiration-date and product-recall alarms, and personal library management). It would also prevent the use of RFID after a product with a killed tag is resold or recycled. For these reasons, it would be desirable for vendors and consumers alike to have low-cost, post-sale use of RFID tags, along with privacy protection.

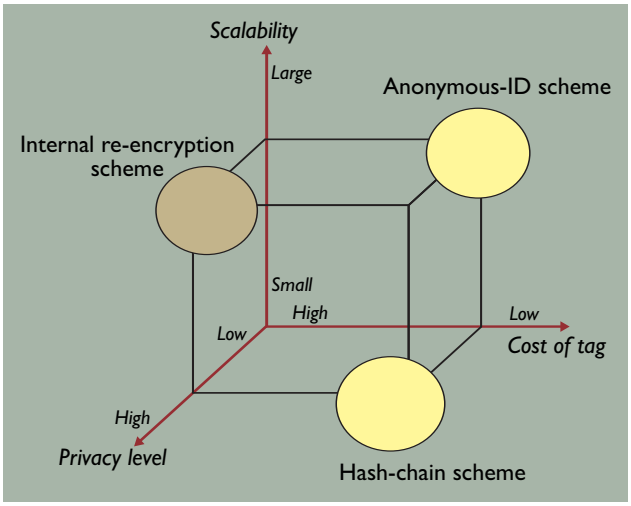

Figure 1. Three approaches to protecting user privacy, classified according to three axes, privacy level, tag cost, and scalability. The hash chain promises strong privacy and low cost but limited scalability. Anonymous ID promises low cost and greater scalability but limited privacy. And internal re-encryption promises strong privacy and greater scalability but high cost.

Privacy Threats

Two notable privacy issues complicate adoption of RFID systems:

Leaking information pertaining to personal property. If a generic naive RFID system is used, anyone can read, without restriction, the connection between the product and the tag and obtain information regarding the tagged contents of, say, a purse or any tagged item worn on the body in a manner about which the possessor is unaware.

Tracking the consumer's spending history and patterns and physical whereabouts. If a product ID is specific to an individual (when, say, tags are used in clothes and other personal belongings like shoes, watches, handbags, and jewelry), tracking the person's movements over an extended period becomes an option. Not only can physical location be tracked, an individual's personal information (stored on multiple independently managed databases) might also be accessible based on a unique ID.

These RFID privacy threats follow from the basic functionality of RFID technology; an ID can be read without permission, is constant and unique, and con-

> The major problem in killing the tag is that the various RFID stakeholders would no longer be able to take advantage of the future emerging services that would rely on the millions of RFID tags likely to be dispersed throughout the consumer environment.

tains potentially sensitive data.

Protecting Privacy

A number of proposed RFID privacy-protection schemes are classified based on the new functionality they implement in RFID technology (see the table). They range from adding only memory to adding lightweight circuits. Each involves a trade-off between the cost of the tag and the value of privacy protection. Here are several approaches:

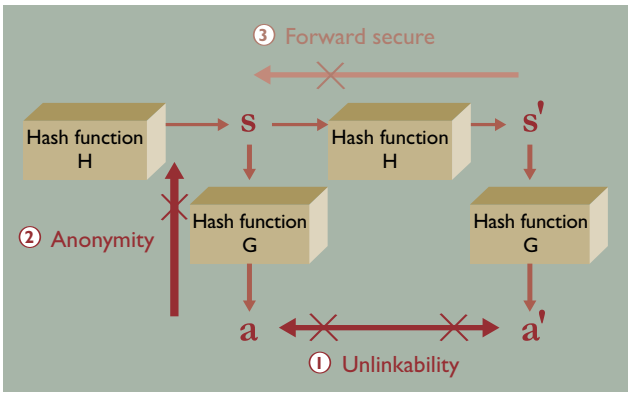

Figure 2. Hash-chain scheme. Each tag contains circuits for hash function G, H, as well as a secret key "s," shared by the tag and a trusted server. Each tag outputs hash value a=G(s). The next tag renews the secret key by overwriting s with hash value s'=H(s). The inability to link and provide anonymity resists malicious attacks through G's pseudo-randomness. Forward-security is achieved by H being one-way.

Kill function. The EPCglobal standard specifies that tags must be equipped with at least one nullification function as a way to address public opposition. This function—called the "kill command"—disables the functionality of the tag after consumers purchase a product. It involves a high degree of consumer privacy protection at negligible cost; however, since the disabling process is performed manually by millions of individual consumers, human error is always a possibility. Moreover, the major problem in killing the tag is that the various RFID stakeholders would no longer be able to take advantage of the future emerging services that would rely on the millions of RFID tags likely to be dispersed throughout the consumer environment.

Normal tags and smart tags. Other privacy-protection schemes generally reflect two main approaches: normal-tag and smart-tag. The normal-tag approach protects individual consumer privacy without having to modify the existing tag or cost the user organization more money. Smart tags are equipped with additional components (such as rewritable memory, basic logic circuits, hash function units, and common-key/public-key encryption units).

The normal-tag approach achieves privacy protection by preventing the unauthorized reading of the output from the tag, blocking electric waves with aluminum foil or jamming waves to interfere with a tag's ID being read by an adversary's unauthenticated reader. An example is the block-tag scheme developed by RSA Security [3]. The blocker tag simulates all possible tag IDs to prevent malicious people from identifying the target tag's ID; it pretends that all possible tags exist there, thus preventing the reader from identifying the tags that are actually present. Although the blocker tag is implemented cheaply (requiring no alterations to the tag), the extent to which user privacy is protected is limited and cannot be confirmed by the consumer. Consumers might thus be uneasy about the privacy protection afforded to their data.

Since any scheme that takes the normal-tag approach faces the same potential consumer-distrust issues as the block-tag scheme, especially uncertainty about how their own shopping data might be used, the practical application of the normal-tag approach is unlikely to be suitable in the future when many more tags have been dispersed.

Installation of additional circuits (such as those involving access control and encryption functions) in the tags can help overcome such uncertainty. However, they increase the technology's cost, which must be minimized in the first place because a key advantage of the tags is that they're cheap, perhaps only a few cents each.

Tags with Rewritable Memory

Tag cost, security level, and scalability are likely to be the key factors in any trade-off equation calculated by any organization thinking about implementing these schemes (see Figure 1). Illustrating the smart-tag approach are tags with rewritable memory and tags with lightweight circuits. When the tag incorporates rewritable memory, the reader rewrites the information in the tag to achieve privacy protection [2, 5]. This approach is notable for its low cost, because the tag requires only rewritable memory.

A noteworthy example of this technology is the "anonymous-ID scheme" proposed in [5] in which an encrypted ID—E(ID)—is stored in the tag, where E denotes the encryption function. In response to a reader's request, the tag replies with the encrypted ID directly to the reader. The reader then sends the encrypted ID from the tag to the server, requesting the server decrypt the encrypted ID. The server does so to obtain the ID of the tag and sends the ID back to the reader. The scheme prevents the leaking of private consumer data by encrypting the ID. Addressing the problem of being able to track a consumer's phys-

ical location, the encrypted ID stored in the tag must be renewed by re-encrypting it as frequently as possible. The reader obtains the encrypted ID from the tag's memory and re-encrypts it, creating a new randomized ciphertext—E(ID)—with the same plaintext ID and overwrites the old encrypted ID with the new encrypted ID.

The drawback is that the reader must renew the encrypted ID with the consumer's cooperation while the frequency of ID re-encryption directly affects the level of privacy protection. If, for example, re-encrypting the ID is performed once a month, the tag can be traced by a malicious adversary during that month.

Approach		Required Circuit	Proposed Schemes	Cost
Kill Command		Not required	Hardware processing Software processing	Low
Keep-Alive Approach	Normal-tag approach	Not required	Electric wave interception Jamming wave Blocker Tag (RSA) [3]	
	Smart-tag approach	Writable ROM	Anonymous-ID (NTT) [5] External Re-encryption (RSA) [2]	
		Basic logic circuit	XOR-based OTP (RSA) [1]	
		Hash function, Common-key encryption	Hash-Lock scheme (MIT) [7] Randomized Hash-Lock scheme (MIT) [8] Hash-Chain scheme (NTT) [6]	
		Public-key encryption	Internal re-encryption scheme (NTT) [4]	High

Approaches for protecting user privacy, classified according to required circuit, proposed schemes, and cost. The trade-offs involve security level vs. tag cost.

Tag with lightweight circuits. In this approach, a lightweight circuit is incorporated into the tag, and a re-encrypted ID to the reader is calculated by the circuit [1, 6–8]. Although public key cryptosystems come close to providing good privacy protection, they are not suitable for tags because public key primitives are complex and costly [4]. A noteworthy scheme employing this technology is the "hash-chain scheme" proposed in [6] in which a hash-function circuit is embedded in the tag, and the tag response is calculated by the hash function. The scheme holds down the cost of the tag, since the hash function is a lightweight operation.

Because the tag randomizes its own responses, it doesn't need an outside reader to randomize its response. The circuit of two hash functions—G and H—are embedded in the tag. The secret key s is stored in the tag's memory, which is linked to the object's ID server, which manages the link between the secret key s and the object's ID. At the reader's request, the tag outputs hash value a=G(s) of secret s, computes new secret s' = H(s), or the hash value of the previous secret, and overwrites the memory with new secret s' (see Figure 2). The reader sends the output from the tag to the server and requests the server reveal the ID. The server identifies the ID of the tag from a=G(s) received from the reader and sends the ID back to the reader. The link between secret keys and the ID is maintained by the server, enabling it to identify the ID from a=G(s).

The hash function is lightweight, pseudo-random, and one-way. Here, pseudo-random means the output of the hash function is computationally indistinguishable from a true random value. Being one-way means it is computationally infeasible to compute the input of the hash function from output of the hash function. The scheme addresses ID leakage and tracing problems through the pseudo-randomness of the hash function, which prevents leakage and tracing. Moreover, the scheme is forward-secure, that is, even after the tag's secret is exposed through tampering, the tag's past history cannot be traced due to the hash function being only one-way.

If the tag scheme were not forward-secure, consumers could not throw it away with a sense of assurance that their privacy is protected. In schemes that are not forward-secure, adversaries might remove the tag from the trash, then recover its secret key through tampering. They could thus trace the tag's history to determine the possessor's history. Even if the secret key is stolen through tampering (and since the "hash-chain scheme" is forward-secure), tag history cannot be traced. The drawback to the hash-chain scheme is that the load on the server is proportional to the number of tags, though the load can be reduced through advanced computation.

Conclusion

RFID technology is likely to proliferate and play a key technological role in the Internet-linked worldwide economy, including in residential design and home appliances. However, before it is secure and trusted enough by millions of ordinary consumers to be absorbed into the economic and social infrastructure, the related security threats must be recognized and appropriate countermeasures taken by RFID developers and vendors, as well as by government regulatory agencies.

Perceptions of these privacy problems vary, depending on personal tolerance and the purpose of a particular tag's use. Both technological and social countermeasures must be implemented in a mutually beneficial manner, helping retailers control their inventory and ensuring consumers their data won't be misappropriated. Each result is indispensable to pro-

tecting privacy.

Educational efforts, along with corporate application policy, are required to reassure consumers that their data is indeed safe. The technological countermeasures needed for privacy protection must also cost no more than a few cents per tag without resulting in lost convenience to RFID users, particularly retailers.

Comprehensive countermeasures must combine a variety of viewpoints—legal, social, and technological—to address any potential security threats to the personal data of tens of millions of consumers worldwide. C

References

1. Juels, A. Minimalist cryptography for low-cost RFID tags. In *Proceedings of the Security in Communication Networks Conference* (Amalfi, Italy, Sept. 8–10). Springer-Verlag, 2004.
2. Juels, A. and Pappu, R. Squealing Euros: Privacy protection in RFID-enabled banknotes. In *Proceedings of Financial Cryptography* (Gosier, Guadeloupe, FWI, Jan. 27–30). Springer-Verlag, 2003.
3. Juels, A., Rivest, R., and Szydlo, M. The blocker tag: Selective blocking of RFID tags for consumer privacy. In *Proceedings of the 10th ACM Conference on Computer and Communications Security* (Washington, D.C., Oct. 27–30). ACM Press, New York, 2003, 103–111.
4. Kinoshita, S., Ohkubo, M., Hoshino, F., Morohashi, G., Shionoiri, O., and Kanai, A. Privacy-enhanced active RFID tag. In *Proceedings of ECHISE 2005* (Munich, Germany, May 11, 2005).
5. Kinoshita, S., Hoshino, F., Komuro, T., Fujimura, A., and Ohkubo, M. Low-cost RFID privacy protection scheme. *IPS Journal 45,* 8 (Aug. 2004), 2007–2021 (in Japanese).
6. Ohkubo, M., Suzuki, K., and Kinoshita, S. A cryptographic approach to 'privacy-friendly' tags. Presented at the RFID Privacy Workshop (MIT, Cambridge, MA, Nov. 15 2003); rfidprivacy.ex.com/2003/agenda.php.
7. Weis, S. *Security and Privacy in Radio-Frequency Identification Devices.* Masters thesis, MIT, Cambridge, MA, May 2003; crypto.csail.mit.edu~sweis/.
8. Weis, S., Sarma, S., Rivest, R., and Engels, D. Security and privacy aspects of low-cost radio frequency identification systems. In *Proceedings of Security in Pervasive Computing* (Boppard, Germany, Mar. 12–14). Springer-Verlag, 2003.
9. Wired News. What your clothes say about you. (Mar. 12, 2003); www.wired.com/news/wireless/o,1382,58006,00.html; see also www.boycottbenetton.com.
10. ZDNet. California bill would ban tracking chips in IDs. (Apr. 28, 2005); news.zdnet.com/2100-1035_22_5689358.html.
11. ZDNet. Privacy activists demand Tesco boycott over RFID. (Jan. 26, 2005); news.zdnet.co.uk/09,39020330,39185481.00.htm; see also www.boycotttesco.com.

Miyako Ohkubo (ookubo.miyako@isl.ntt.co.jp) is a research engineer in NTT Laboratories, Nippon Telegraph and Telephone Corporation, Yokosuka, Japan.
Koutarou Suzuki (suzuki.koutarou@lab.ntt.co.jp) is a research engineer in NTT Laboratories, Nippon Telegraph and Telephone Corporation, Yokosuka, Japan.
Shingo Kinoshita (kinoshita.shingo@lab.ntt.co.jp) is a senior research engineer in NTT Laboratories, Nippon Telegraph and Telephone Corporation, Yokosuka, Japan.