PCB: Physically Changeable Bit for Preserving Privacy in Low-End RFID Tags

Cliff C. Zou

School of Electrical Engineering and Computer Science

University of Central Florida

Orlando, FL 32816

czou@cs.ucf.edu

May 2006

Abstract

Consumer privacy is a major concern impeding the wide deployment of radio-frequency identification (RFID) tags in consumer market. To tackle this privacy issue, a simple and effective approach is proposed in this paper via adding one bit called ”physically changeable bit” (PCB) in RFID tags. The PCB bit can and only can be altered ”physically”. It controls whether RFID tags respond to queries sent by RFID readers. In this way, tags can be deactivated and reactivated easily by their owners via a simple device or even with no device. On the other hand, adversaries cannot track tags deactivated by their owners since adversaries cannot reactivate those tags “remotely”. PCB design is based on the fundamental assumption that adversaries have no physical contact with RFID tags owned by others. When extended with multiple built-in PCB bits, RFID tags can be configured to respond with appropriate ID information to queries while still preserving consumer privacy at the same time. PCB design combines the remote-identification benefit of RFID technology together with the safety of current barcode system, and most importantly, easy to be understood and accepted by general consumers.

1 Introduction

An **RFID** (Radio-Frequency Identification) tag is a system that transmits the identity (in the form of a unique serial number) of an object or person wirelessly using radio waves [5]. Although its functionality is similar to barcode identification system, RFID technology promises many benefits to manufacturers and consumers. Barcode system requires a person to manually scan labels or tags one by one, while RFID is designed to enable readers to automatically capture data on tags wirelessly and transmit it to a computer system without needing a person to be involved [5]. Due to its tremendous benefits, people believe that RFID is going to be widely deployed in the near future.

Because of the remote access property of RFID tags, privacy becomes a serious concern [8, 9]. For example, adversaries can silently read RFID tags on you to know what products or medicine you have bought, what cloths you wear, etc. To solve this privacy issue, the most obvious way is to cryptographically enforce the authentication of RFID readers and encryption of tags' serial numbers. However, this approach is only valid for high-end RFID tags that have their own power source and enough computation/storage resources, such as highway electronic toll pass (e.g., EZ-pass [1]), ExxonMobil Speedpass, etc. For low-end RFID tags in consumer market, where each tag is supposed to be 5 cents or less, it is very hard to use cryptography or hash function [7, 8] to protect privacy considering the high computation power owned by adversaries and the complicated issue in authentication. In addition, these approaches are hard for consumers to understand and accept. In this white paper, I only consider the privacy issue in low-end RFID consumer market where cryptography is out of the consideration.

People have presented several ways to protect privacy in low-end RFID systems. The most simple and reliable way is the so-called "kill-tag" approach [6]: when tags are in consumer hands, they can be permanently killed, e.g., destroyed or thrown away. However, the remote identification benefit of RFID tags is still wanted for many products when they are in the hands of consumers, e.g., "smart" home appliances that can automatically check and alert users of food in refrigerators, clothes in closets, medicine that needs to be refilled. [6] has presented many other benefits of keeping RFID tags intact. For these products or applications, killing tags would not be a good option.

The second approach is to shield tags with metal mesh or foil that is impenetrable by radio signals from readers. This approach is effective in some specific situations, such as wallets or bags equipped with foil cover to protect tags inside them. However, many products cannot be placed conveniently in containers, and we need to protect their identity via some other ways.

The third approach is to actively or passively jam radio frequency signals to disrupt the operation of nearby RFID readers. Active jamming approach may be illegal and it stops all functionalities of nearby RFID tags. Juels et. al. [6] presented "RFID blocker", which can selectively block the queries sent by an RFID reader if the reader tries to read tags in the restricted zone specified by the blocker. The restricted zone can be set up using a "privacy bit" in tags — blockers only block tags having their privacy bit turned on. The privacy bit in a tag on an article is only turned on when the article is purchased by a consumer [6]. However, even a selective blocker would stall the legitimate recursive queries sent by RFID readers. To solve this problem, current RFID communication protocol must be revised, which is not easy considering the large amount of RFID systems (especially the readers) already deployed today.

In this white paper, I present an alternative privacy protection approach called “PCB” by adding a physically changeable bit in RFID tags. I do not claim that it is better than the approaches introduced above. But it can solve some problems met by the other methods and thus provides an alternative choice for privacy protection in low-end RFID systems.

2 PCB: Physically Changeable Bit

2.1 PCB Design Principle

Currently, the “kill-tag” approach is the most widely used method in RFID privacy protection. For example, a guideline was proposed by a group of businesses and consumer advocates that “it should be clear to consumers how to disable disposable forms of the tags and that it should be easy to do so once items with such tags have been purchased.” [3] To overcome the kill-tag problem (RFID functionality permanently killed), PCB design lets consumers to easily deactivate and reactivate tags identification functionality according to their wishes.

PCB design adds a “physically changeable bit” into an RFID tag. The status of this bit, off or on, can only be altered with physical contact. The PCB bit can be either a logical bit saved in memory, or a hardware bit, such as a tiny switch that connects or disconnects the RFID hardware circuit. When its PCB bit is off, an RFID tag is deactivated and thus will not respond to any queries. When the owner of a deactivated tag wants to take advantage of the tag’s identification benefit again, she can turn on the PCB bit by a special device (according to the PCB design) or simply by her fingernail (for the switch-based PCB bit).

PCB design relies on the following principle: an RFID tag’s owner can easily obtain physical contact with the tag, while an adversary is very hard to do that since the adversary does not physically possess the tag. By saying this, I do not consider the privacy issue of stolen tags or tags that can be physically grasped by adversaries. Compared with barcode systems, the privacy problem brought up by RFID tags solely comes from their “remote” identification process. Therefore, by adding a PCB bit that is hard or impossible for adversaries to turn on, PCB design combines the remote-identification benefit of RFID technology together with the safety of current barcode systems.

2.2 RFID tags with multiple PCB bits

The above PCB design only adds one bit to RFID tags. When the PCB bit is off, the tag is “dead” and there is no way for a nearby reader to know the tag’s existence. While preserving consumers’ privacy, some applications would require tags to give back limited identification information, such as announcing the existence or types of tags.

For such applications, RFID tags can be designed with multiple PCB bits. A tag with two PCB bits could provide four different responses to queries, which is enough for most applications. For example, to track patients in a hospital, each patient wears an RFID watch equipped with two PCB bits that can be set by the doctors or the patient[1]. When PCB=00 the tag does not respond to any queries at all; when PCB=01 the tag will respond to a query with limited information showing that it belongs to a patient; when PCB=10 the tag will respond to a query with more detailed information showing that it belongs to a patient in which department; when PCB=11 (the default value) the tag will respond with its full serial number.

2.3 PCB Implementations

A good PCB implementation would satisfy the following requirements:

- The PCB bit can only be altered via physical contact (or a very closed-range contact).
- The PCB bit is easy for consumers to turn on or off.
- If the design requires a special device to alter the PCB bit, the device much be cheap since consumers need to have one to use by themselves (e.g., at home when they want to activate tags).

Due to the lack of knowledge and resource, I have not built any prototype RFID tags equipped with PCB bit. Here I present some possible ways I can think of to implement the PCB design in RFID tags. The methods I present below are surely not complete and may not be good choices considering the cost and other factors, but they could give readers some ideas on how to implement PCB design.

Circuit switch:

The simplest implementation of PCB in RFID tags is to add a tiny switch that connect or disconnect the radio antenna circuit from the RFID main chip. A tag's owner can use his or her fingernail to change the switch status. The advantage of this implementation is that it does not require consumers to use any device to activate/deactivate RFID tags. A tag with multiple PCB bits can be built with n switches to represent the n PCB bits (tags with $n = 2$ PCB bits are enough for most applications).

EEProm:

[1] If the hospital does not want patients to change the PCB bits, an RFID watch can be pre-configured and then locked to prevent physical access of the PCB bits from patients.

A second implementation of PCB is to build EEProm bits in RFID tags — one EEProm bit represents one PCB bit. EEProm stands for “electrically erasable programmable read-only memory”, which is a special type of read-only memory that can be rewritten by exposing it to an electrical charge. Such tags have two electrical charge points built on their surface so that their owners can use a special device to power and change the EEProm bits.

Magnetic bits:

A third implementation of PCB is to build magnetic bits in RFID tags. To ensure that the PCB bit can only be correctly activated via physical contact, we can use a pair of magnetic bits to represent one PCB bit. A “U”-shaped device is needed to alter a pair of magnetic bits: one foot of the device magnetizes one magnetic bit on the tag (i.e., changes it to be “1”) while another foot degausses the other bit. Since these two magnetic bits are close to each other, they can be changed to 01 or 10 only by a device with physical contact (or in a very closed range). If an adversary uses a magnetic device remotely, these two magnetic bits can only be changed to 00 or 11 — the tag will not respond to queries if the pair of magnetic bits have the value of 00 or 11.

Compared with the previous two implementations, the magnetic PCB design means that adversaries can deactivate RFID tags remotely. However, this is not an issue for many consumer tags.

3 PCB Design Discussion and Limitations

3.1 Comparison with prior related patents

US patent No. 6025780:

The patent discusses how to activate and deactivate RFID tags “electronically, physically or virtually” [2]. For the physical deactivation of tags, the patent presents how to use switch to connect/disconnect the coil antenna or the capacitor from the IC chip. The switch-based PCB design presented in this white paper can actually use the same design.

However, by claiming that “a deactivation event may be performed on the tag when legitimate access is obtained to the tagged article”, the patent [2] does not explain how to ensure an access is “legitimate access”. The patent does not study how to protect privacy of tag owners from adversaries. In addition, the electronic deactivation mentioned in this patent simply uses RFID tags with rewriteable bits — no mechanism has been mentioned on how to ensure such a bit change is conducted securely.

US patent application No. 20050012616:

This patent application [4] presents RFID tags designed with two parts: a short-range antennaless RFID that can only be read in closed range, and a second antenna portion that is coupled with the first portion to increase its communication range. The second antenna portion can be destroyed by physical, chemical or electrical forces. After the second portion is inactivated, the RFID tag is readable only within a closed range so that it is hard for adversaries to invade privacy.

This patent attempts to solve the privacy issue by making it harder for adversaries to eavesdrop or query RFID tags remotely. However, its deactivation of the second portion of tags is still non-reversible, e.g., by tearing off the second portion, or dissolving the second portion via solvent. The patent never mentions the needs or the ways to reactivate the second portion to restore the normal operation of tags. In this sense, it still belongs to the "kill-tag" class of approaches.

3.2 PCB design limitations

The PCB design presented in this white paper is simple and effective to some low-end RFID applications. The biggest advantage of the PCB design, perhaps, is that it is effective and convienent to use and so simple for people to understand. In the general consumer market, the success of a techonlogy is mostly decided by the feeling and understanding of ordinary people. This is the reason why the "kill-tag" approach is widely used nowadays instead of other privacy-protection technologies.

However, the PCB design has its own limitations, too. Frist, because each tag needs to be deactivated individually due to the physical contact requirement, the PCB design is not suitable for supply chains or the process of a large volume of articles. It is suitable for the checkout of individual consumer from a supermarket or a library, but not suitable for a wholesale process.

Second, due to the phyiscal contact requirement, tags attached to articles should be visible, or easy for consumers to make phyiscal contact with. For this reason, tags that must be hidden in articles to prevent access from consumers (e.g., anti-theft purpose) are not suitable to implement the PCB design.

One exception is the magnetic-based PCB design presented in this white paper. In this case, tags do not need to be visible, but they should be close to the outside (e.g., sticked to the internal side of a box) and should have clear sign on the outside of articles showing where consumers should put the "U"-shaped device to activate/deactivate tags.

In fact, the above limitations are also true for any "kill-tag" approach. Therefore, the PCB design is suitable for most applications that can use kill-tag approaches.

Third, the switch-based PCB design requires tags to have space to install switch, and the switch must be easily adjustable by human fingernail. Therefore, the switch-based PCB design is not suitable for applications that require tiny-sized or paper-thin tags.

Finally, it is not suitable to use RFID tags based on PCB design for anit-theft purpose. Anti-theft RFID tags need to be unaccessible by consumers, which is contridictory to PCB design principle. To provide anti-theft objective without exposing consumer's privacy, an RFID tag could be designed to merely provide a general ID information, e.g., the ID information showing that the tag is a non-purphased product (the check-out cashier can use a special device to change the tag ID).

4 Conclusion

In this white paper, a simple approach called "PCB" is proposed for privacy-protection in low-end RFID tags. PCB stands for "physically changeable bit", which adds one bit to tags that can be and only be changed via phyisical contact. This PCB bit can be turned on or off repeatedly, and it controls whether a tag responds to queries or not. PCB design is based on the fundamental assumption that adversaries have no physical contact with RFID tags owned by others. It combines the remote-identification benefit of RFID technology together with the safety of current barcode system. Several possible implementations of PCB design are also proposed. In summary, PCB design is simple, effective, and most importantly, easy to be understood and accepted by general consumers.

References

[1] E-zpass. www.ezpass.com/.

[2] J.H. Bowers and T.J. Clare. Rfid tags which are virtually activated and/or deactivated and apparatus and methods of using same in an electronic security system. In *United States Patent No. 6025780*, Feburary 2000.

[3] B.J. Feder. Guidelines for radio tags aim to protect buyer privacy. In *The New York Times*, May 1 2006.

[4] I.J. Forster and Y. Sasaki. Rfid device with changeable characteristics. In *United States Patent Application No. 20050012616*, January 2005.

[5] RFID Journal. What is rfid? http://www.rfidjournal.com/article/articleview/1339/1/129/.

[6] A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of rfid tags for consumer privacy. In *Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03)*, pages 190–199, October 2003.

[7] D. Molnar and D. Wagner. Privacy and security in library rfid: issues, practices, and architectures. In *Proceedings of 11th ACM Conference on Computer and Communications Security (CCS'04)*, pages 210–219, October 2004.

[8] M. Ohkubo, K. Suzuki, and S. Kinoshita. Rfid privacy issues and technical challenges. *Communications of the ACM*, 48(9):66–71, September 2005.

[9] S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In *Proceedings of Security in Pervasive Computing*, 2003.