# Keep on Blockin' in the Free World:
## Personal Access Control for Low-Cost RFID Tags

Melanie R. Rieback, Bruno Crispo, Andrew S. Tanenbaum

Computer Systems Group
Vrije Universiteit
Amsterdam, The Netherlands

## Abstract

*This paper introduces an off-tag RFID access control mechanism called "Selective RFID Jamming". Selective RFID Jamming protects low-cost RFID tags by enforcing access control on their behalf, in a similar manner to the RFID Blocker Tag. However, Selective RFID Jamming is novel because it uses an active mobile device to enforce centralized ACL-based access control policies. Selective RFID Jamming also solves a Differential Signal Analysis attack to which the RFID Blocker Tag is susceptible.*

## 1 Introduction

Radio Frequency Identification (RFID) is coming, and it's bringing a streamlined revolution. Passive RFID tags are batteryless computer chips that are powered externally by their RFID readers. These "radio barcodes" can transmit information using radio waves, eliminating the need for a line of sight. RFID tags pose unique security and privacy challenges. Because of their severe processing, storage, and cost constraints, even standard security properties like access control are difficult to implement. Several access control solutions exist for high-end RFID tags, but these mechanisms increase the price of RFID tags beyond what some application scenarios (e.g. supply chain management) will allow. This leaves low-cost (<$0.10) Electronic Product Code (EPC)-style tags without the ability to protect the privacy of their users.

In this paper, we suggest an access control mechanism for low-cost RFID tags called Selective RFID Jamming. Selective RFID Jamming extends protection to low-cost tags by enforcing access control on their behalf. Selective RFID Jamming achieves this by performing RF signal "jamming" (similar to the RFID Blocker Tag). However, Selective RFID Jamming has three unique characteristics: 1) It is implemented on active mobile device, 2) It utilizes ACL-based security policies, 3) It uses a Digital Signal Analysis (DSA) resistant jamming signal.

## 2 Radio Frequency Identification

Radio Frequency Identification (RFID) is the latest phase in the decades-old trend of the miniaturization of computers. RFID transponders are tiny resource-limited computers that do not have a battery that needs periodic replacement. RFID tags are inductively powered by their external reading devices, called RFID readers. Once the RFID tag is activated, the tag then decodes the incoming query and produces an appropriate response by modulating the request signal, using one or more subcarrier frequencies. RFID Tags can do a limited amount of processing, and have a small amount (<1024 bits) of storage.

RFID tags are useful for a huge variety of applications. Some of these applications include: supply chain management, automated payment, physical access control, counterfeit prevention, and smart homes and offices. RFID tags are also implanted in all kinds of personal and consumer goods. For example, RFID tags are used in passports, partially assembled cars, frozen dinners, ski-lift passes, clothing, and public transportation tickets. Implantable RFID tags for animals allow concerned owners to label their pets and livestock. Verichip Corp. has also created a slightly-adapted implantable RFID chip, the size of a grain of rice, for use in humans. Since its introduction, the Verichip was approved by the U.S. Food and Drug Administration, and this tiny chip is currently deployed in both commercial and medical systems.

### 2.1 RFID Threat Model

Like many other pervasive technologies, the success of RFID threatens to bring unwanted social consequences. RFID tags face unique security and privacy risks, not just because the transponders will be located everywhere, but because they are too computationally limited to support traditional security and privacy enhancing technologies. This lack of protection leads to some undesirable scenarios, like

the unauthorized access of tag data, interception of tag-reader communications, and location tracking of people and objects.

A growing number of RFID security and privacy solutions have been proposed, but none have yet succeeded to ensure security and privacy in a wide range of RFID application scenarios. The least amount of progress has been made in protecting the application scenario that is the most common - supply chain management, using low-cost Electronic Product Code (EPC) tags. Low-cost RFID tags require new RFID security and privacy techniques. For the sake of clarity, we will now make a distinction between low-cost and high-cost RFID tags:

**Low-cost RFID tags.** Low-cost RFID Tags should cost between five and ten cents. They are usually used in supply-chain management, and they usually conform to the EPC standard. These RFID tags usually have a kill mechanism, but they are not powerful enough to support cryptography.

**High-cost RFID tags.** High-cost RFID Tags will cost more than ten cents. They are used in the numerous applications outside of supply-chain management, and they can support many different standards. These RFID tags usually have one or more security mechanisms (kill/sleep/wake modes, cryptography).

# 3 Selective RFID Jamming

Selective RFID Jamming is a form of "off-tag" access control that produces a jamming signal when an access control check fails.

| On-Tag | Off-Tag |
|---|---|
| Kill commands | Faraday cages |
| Sleep/wake modes | Blocker tags |
| Pseudonyms | External re-encryption |
| Hash locks | |
| Cryptography/authentication | |

Table 1: On-tag vs. Off-tag Security Mechanisms

To understand how Selective RFID Jamming works, it is useful to understand the difference between on-tag and off-tag access control. Table 1 lists some on-tag and off-tag versions of access control mechanisms. As the name implies, on-tag access control mechanisms are located on the RFID tags themselves. On-tag access control is the most common type of RFID access control, with mechanisms including: tag deactivation, cryptography, and tag-reader authentication. In contrast, off-tag access control mechanisms put the access control mechanism on a device external to the RFID tag. Examples of this include the RSA Blocker tag and external re-encryption. Off-tag access control has the advantage that it can protect low-cost RFID tags (like EPC tags), because the access control doesn't require any extra complexity (hence, extra cost) on the RFID tag itself.

Here is how Selective RFID Jamming works:

1. An RFID reader sends a query to an RFID tag
2. The mobile device captures and decodes the query (in real-time), and determines whether the query is permitted
3. If the query is not allowed, the mobile device briefly sends a jamming signal that is just long enough to block the RFID tag response

The top-level concept is similar to the idea behind the RSA Blocker Tag[8]. However, Selective RFID Jamming has three unique characteristics: 1) It is implemented on active mobile device, 2) It utilizes ACL-based security policies, and 3) It uses a DSA-resistant jamming signal.

## 3.1 Active Mobile Devices

Selective RFID Jamming is always implemented in a battery-powered mobile device (e.g. PDA or mobile phone). This is important because Selective RFID Jamming needs to perform resource-intensive security protocols, such as signal jamming and authentication. To implement such functionality on an RFID tag would cause severe restrictions in terms of power and storage. Using a device with an 'active' power-source avoids problems that 'passive' solutions like RFID tags face, such as the unreliable production of jamming signals based upon physical orientation. Adequate storage space is also important, because it limits the complexity of the access control policies that can be used. On-tag RFID access control mechanisms only have access to 1024 bits of storage at most. However, battery-powered mobile devices are full-blown computers, that have no comparable storage restrictions. This allows access control policies to contain enough entries that they can provide very granular access control.

| Action | Source | Target | Command | Comment |
|---|---|---|---|---|
| block | * | MYTAGS | * | Suppress all queries targeting user's tags |
| allow | Home | MYTAGS | * | Home system can query user's tags |
| allow | Wal-Mart | MYTAGS | Read data block | Wal-Mart can read (not write) data from user's tags |
| allow | * | * | * | All queries to other RFID tags are OK |

Table 2: Example Access Control List

## 3.2 Access Control Lists

Selective RFID Jamming uses Access Control Lists (ACLs) to represent security policies. It 'selectively filters' RFID tag responses, much in the same way that a firewall filters packets from a network. ACLs specify which RFID query responses are blocked or allowed, based upon the source (the reader issuing the query), the target (the RFID tags affected by the query), and the command (ex. read data/write data/inventory). Table 2 shows a sample ACL.

RFID queries do not contain information about the issuing RFID readers, so the source of RFID requests are ascertained by means of an authentication protocol (using in- or out-of-band communications). "Friendly" RFID Readers may explicitly perform authentication ahead of time, swapping some information that can be used to create authenticated 'sessions'. These authenticated RFID Readers may have their own entries in the ACL, giving them special permissions to perform certain kinds of queries. "Unfriendly" RFID Readers (or RFID Readers that simply are not familiar with Selective RFID Jamming) will not perform any authentication protocol at all, and will simply issue their queries. The ACL should also specify a set of 'default' access control rules, that govern access for these unknown readers. Table 2 shows how authenticated RFID Readers from the user's home and the Wal-Mart, are given special dispensation to query the user's RFID tags. [1].

The jamming device extracts the targeted tags and the command type from the query signal, and match these values to the information stored in the access control lists. The jamming device may store lists of RFID tags, including 'tag ownership' lists, that specify tags owned or otherwise associated with the user. (Another one might list the former owners of RFID tags). Ranges of RFID identifiers might be represented similarly to ranges of IP addresses. For example, the mask "01.0000A89.00016F.0/60" specifies an 8-bit EPC Header, 28-bit EPC Manager, and 24-bit EPC Object Class, but not the 36-bit EPC Serial Number. Access is then restricted based upon the stored RFID tag information. Table 2 illustrates how access control is restricted for certain commands, for tags in a specific ownership list called MYTAGS.

[1] Authentication requires shared keys, which require key setup between RFID Readers and the jamming device

## 3.3 DSA-Resistant Jamming Signal

**The Problem** RFID Blocker Tags[8], introduced by Juels, Rivest, and Szydlo, interfere with RFID Readers' tree-walk tag singulation algorithm by always replying with a '0|1' signal. This response causes a collision, which forces the RFID reader to traverse the entire ID space to discover the IDs of nearby RFID tags.

RFID Tags will usually not meet the singulation criteria, during the Blocker Tag induced full binary tree ID traversal. This means that the majority of the time during tag singulation, the Blocker Tag(s) are the only entities that are responding. Additionally, because the responses from RFID Blocker Tags are always the same, the analog signals received from the RFID Blocker will also be identical.

**The Attack** In order to perform differential signal analysis, we need to modify an RFID Tag Reader to measure and record the additive waveform that results from the interference of all incoming RFID signals. If an RFID Reader records the analog signal received during tag singulation, the mode (or most commonly appearing) 'tag response' signal will be the combined waveform of the '0|1' responses, sent from the one or more Blocker Tags that are present. Because this signal never changes, it can be mathematically averaged out from the total recorded waveforms. The left-over signal will be the genuine RFID tag responses.

**Illustrating the Attack** We will illustrate our attack through use of an example, shown in Figure 1 .

Let's hypothetically say that we use RFID tags with 3-bit ids (8 possible tags). We also assume that RFID tag IDs are

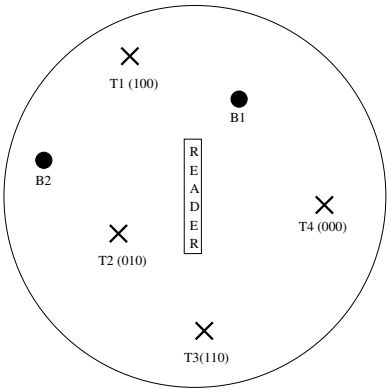


Figure 1: Scenario: RFID Tags and Blockers

unique – no two authentic RFID tags will use the same ID. We have an RFID reader in the center of a circular range, and four RFID tags (T1-T4), and two RFID blocker tags (B1-B2) are present.

It's easy to detect the presence of RFID blocker tags. If no (or few) tags seem to be missing during singulation, then it's likely that one or more RFID blocker tags are present. Additionally, if we attempt to perform singulation on each of the 'leaf nodes' (3-bit complete ID's), we will constantly get collisions, that will be composed of the combined signals shown in Table 3.

| Queried Tags | Combined Signal |
|---|---|
| Sub-tree starting with '000' | T4+B1+B2 |
| Sub-tree starting with '001' | B1+B2 |
| Sub-tree starting with '010' | T2+B1+B2 |
| Sub-tree starting with '011' | B1+B2 |
| Sub-tree starting with '100' | T1+B1+B2 |
| Sub-tree starting with '101' | B1+B2 |
| Sub-tree starting with '110' | T3+B1+B2 |
| Sub-tree starting with '111' | B1+B2 |

Table 3: Analog waveforms received during an RFID tag sweep

In each of these cases, we received collisions, so the reader will not be able to read the individual tag ID's. However the reader is able to detect total additive signal, produced by the multiple RFID tags.

Half of the measured analog waveforms received are equal to B1+B2. If we take the mode (most frequently occurring value) of all of the measured 3-bit ID signal strengths, we will get B1+B2. If we use 8-bit tag IDs instead of 3-bit tag ID's, the predominance of the mode throughout a range sweep will be even more obvious. Now all we have to do is subtract the signal (B1+B2) from each total signal received during the actual tree-walk singulation process, and we'll get the following results, shown in Table 4. The RFID Reader can now easily determine which RFID tags are present.

| Singulated Node | Combined Signal | Subtracted Signal |
|---|---|---|
| Sub-tree starting with '0' | T2+T4+B1+B2 | T2+T4 |
| Sub-tree starting with '00' | T4+B1+B2 | T4 |
| Sub-tree starting with '000' | T4+B1+B2 | T4 |
| Sub-tree starting with '001' | B1+B2 | No signal |
| Sub-tree starting with '01' | T2+B1+B2 | T2 |
| Sub-tree starting with '010' | T2+B1+B2 | T2 |
| Sub-tree starting with '011' | B1+B2 | No signal |
| Sub-tree starting with '1' | T1+T3+B1+B2 | T1+T3 |
| Sub-tree starting with '10' | T1+B1+B2 | T1 |
| Sub-tree starting with '100' | T1+B1+B2 | T1 |
| Sub-tree starting with '101' | B1+B2 | No signal |
| Sub-tree starting with '11' | T3+B1+B2 | T3 |
| Sub-tree starting with '110' | T3+B1+B2 | T3 |
| Sub-tree starting with '111' | B1+B2 | No signal |

Table 4: Subtracting blocker signals during RFID tag singulation

**Preventing Signal Analysis** Selective RFID Jamming produces a randomly modulated jamming signal, at a single frequency (ex. 13.56 MHz). The idea is that because the signal is randomly modulated, it cannot be easily averaged out. We use a single antenna to produce this jamming signal. [2]. The only caviat to keep in mind is the following: if you collect enough samples of the same signal added with the random signal, you can often still average out the random signal. So careful attention must be paid to the design of the randomization function.

# 4 Discussion

Selective RFID Jamming provides centralized (multi-tag) access control, while most on-tag mechanisms provide decentralized (per tag) access control. This centralization has its advantages. Access control lists are easier to update, plus centralizing RFID access control has a cost advantage. A per-tag access control mechanism, like the RFID Blocker Tag, is used 1:1 in proportion with the RFID tags that are

[2]The Blocker Tag uses two antennas – one to produce the '0' response and one to produce the '1' response. However, this is not necessary to produce a '1|0' collision signal

protected. Reproducing so many copies of the access control mechanism may be cost prohibitive in some applications. However, only one mobile device is necessary to protect hundreds of a user's low-cost tags using Selective RFID Jamming.

Selective RFID Jamming has an unresolved problem: Denial of Service attacks. If an attacker deliberately performs lots of unauthorized RFID queries, the jamming signal production will jam up the airwaves, causing interference with other nearby RFID systems. A secondary problem is that this repeated production of jamming signals will also drain the battery of the mobile device. Unfortunately, this is not an easy problem to solve.

Selective RFID Jamming has a few other problems including: 1) The active mobile device is a single point of failure, 2) There might be legal problems, and 3) Selective RFID Jamming won't stop RFID readers using very directional antennas. We would like to further address these issues in future work.

# 5 Related Work

Off-tag RFID access control was pioneered by Juels, Rivest, and Szydlo with their RFID Blocker Tag. As described in Section 3.3, the RFID Blocker Tag interferes with RFID Reader singulation by "spoofing" the RFID Reader's tree-walk singulation protocol[8]. The Blocker Tag is different from Selective RFID Jamming because it is implemented on an RFID tag, it uses a static '0|1' jamming signal produced by two antennas, and it uses privacy-zones instead of access control lists. Several kinds of on-tag access control mechanisms also exist for RFID technology. Tag deactivation, otherwise known as "tag killing" was standardized by the EPCglobal consortium [1]. Juels also suggests the use of dynamic tag identifiers, called pseudonyms, that use a mechanism called "pseudonym throttling" to allow authenticated RFID readers to refresh the pseudonym list [7]. On-tag access control schemes work well for certain applications, but fail to protect low-cost EPC-style tags, which are too cheap to support these mechanisms. High-cost RFID tags may also support RFID tag-reader authentication schemes. Vajda and Buttyan offer lightweight authentication protocols [9], and Weis, et. al, proposed a randomized hash lock protocol for authentication[10]. Feldhofer, et. al, proposes an extension to the ISO 18000 protocol, that would enable the in-band transmission of authentication data [2]. Cryptographic primitives also exist that may work with high-cost RFID tags. Finkenzeller describes the use of stream ciphers[4], and Feldhofer, et. al, describes a low-cost AES implementation [3]. Gaubatz, et. al, describe a low cost NTRU implementation, designed for sensor networks, that brings public key cryptography closer to fitting the constraints of RFID [6]. Low-cost RFID tags can also be protected by social and legal factors. Simson Garfinkel proposes a legislative RFID "Bill of Rights", where he explicitly extends some ideas from the European Privacy Directive for use with RFID[5].

# 6 Conclusion

Selective RFID Jamming is an access control scheme that uses battery-powered devices to enforce ACL-based access control policies, with the aid of randomly modulated jamming signals. Selective RFID Jamming enforces access control on the behalf of low-cost RFID tags, which is useful for protecting cost-critical applications (e.g. supply chain management) that currently lack access control. It will combat RFID security and privacy threats, and can help fight the battle against the negative consequences that RFID technology will bring.

# References


[1] EPCglobal, *13.56 mhz ism band class 1 radio frequency (rf) identification tag interface specification.*

[2] Martin Feldhofer, *An authentication protocol in a security layer for RFID smart tags*, The 12th IEEE Mediterranean Electrotechnical Conference – MELECON 2004 (Dubrovnik, Croatia), vol. 2, IEEE, May 2004, pp. 759–762.

[3] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, *Strong authentication for RFID systems using the AES algorithm*, Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004 (Boston, Massachusetts, USA) (Marc Joye and Jean-Jacques Quisquater, eds.), Lecture Notes in Computer Science, vol. 3156, IACR, Springer-Verlag, Aug 2004, pp. 357–370.

[4] Klaus Finkenzeller, *RFID Handbook: Fundamentals and applications in contactless smart cards and identification*, John Wiley & Sons, Ltd., 2003.

[5] Simson Garfinkel, *An RFID bill of rights*, Technology Review (2002), 35.

[6] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, *State of the art in public-key cryptography for wireless sensor networks*, Proceedings of the Second IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2005), 2005.

[7] Ari Juels, *Minimalist cryptography for low-cost RFID tags*, The Fourth International Conference on Security in Communication Networks (SCN 2004) (Amalfi, Italia), Lecture Notes in Computer Science, Springer-Verlag, September 2004.

[8] Ari Juels, Ronald L. Rivest, and Michael Szydlo, *The blocker tag: Selective blocking of rfid tags for consumer privacy*, Proceedings of the 10th ACM Conference on Computer and Communications Security, ACM Press, 2003.

[9] István Vajda and Levente Buttyán, *Lightweight authentication protocols for low-cost RFID tags*, Second Workshop on Security in Ubiquitous Computing – Ubicomp 2003 (Seattle, WA, USA), October 2003.

[10] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, *Security and privacy aspects of low-cost radio frequency identification systems*, Security in Pervasive Computing, Lecture Notes in Computer Science, vol. 2802, 2004, pp. 201–212.