

## Examining the Security and Privacy Concerns of RFID: Part 2

By Jack Maynard

Part 1 of this article provided a general introduction to RFID technology. It examined the various components that make up an RFID system, how RFID is being used in business today, and some of the emerging global standards. Part 2, (this document) examines some of the common security and privacy concerns associated with RFID, primarily related to retail and consumer use, where low-cost RFID technology is prevalent.



### RFID Security Concerns

RFID is fast becoming pervasive. The research consultancy Frost & Sullivan predicts in its [World Retail RFID Markets Report](#) that the retail-specific market for RFID (where low-cost RFID is heavily utilized) will grow from \$400 million (€338.5, £232.3) in 2004 to almost \$4.2 billion (€3.5, £2.4) in 2011.<sup>1</sup> However, with each new technology comes its own set of implementation challenges. Among those facing RFID are security concerns. The question of RFID security is not how secure is it, but rather how secure do you want it to be, and at what cost?

Implementing secure RFID using high-cost RFID tags is already possible. High-cost RFID tags generally contain the memory and processing capability necessary to implement many of the standard security primitives that provide for confidentiality, integrity and authenticity, but not at a price point that would make their use ubiquitous in retail and consumer applications, where even cost improvements of \$.01 per tag can result in savings of millions of dollars for retailers.

The security concerns associated with RFID are not new, but rather the same ones facing most technology today. The list includes an assortment of common security problems such as spoofing, skimming, eavesdropping, sniffing, denial-of-service, physical attacks, traffic analysis, and weak cryptography. In traditional computing systems, many security problems can be solved using standard cryptographic solutions. However, the use of low-cost RFID tags does not permit this. The memory capacity of low-cost tags is usually only a few hundred bits, and only a few thousand gates available for logic functions. These limited resources make it impossible to implement any kind of strong cryptographic primitive on low-cost tags. Even standard cryptographic hash functions such as [MD5](#) or [SHA-1](#) are generally beyond the capability of low-cost tags. Low-cost tags are also passively powered, making background calculations in idle time (when the tag is not powered by the tag reader) impossible.

To their benefit, and unlike security attacks posed against networked devices where an attacker might be extremely remote from a target, attacks against low-cost RFID tags must originate from relatively close proximity to a tag in order to be effective, perhaps 2 meters, or less. This can be difficult in a retail environment.

Let's examine some of the common security concerns associated with low-cost RFID.

---

<sup>1</sup> [Retailers Using RFID for Better Holiday Customer Service](#)

## Spoofing

By spoofing a valid RFID tag, a thief could fool an automated checkout system into thinking that a product was still on the shelf. Or, a thief might re-write or replace tags on expensive items with spoofed data from cheaper items. Similar attacks already exist for barcode data, for example [re-code.com](http://re-code.com), which is no longer active, where users would login, download UPC bar codes for cheaper generic products, print new barcode labels, and then take those labels to a store, where the cheaper barcode is placed on products they wish to buy.

Lukas Grunwald, a German information security consultant, warns that RFID tags are not secure. Grunwald, who presented at the 2004 Black Hat Security Briefings conference, announced that he has successfully changed the information on an RFID tag. He also announced the release of his software [RFDump](#) which Grunwald has been working on for several years.

Quoting Mr. Grunwald: "RFDump is a tool to detect RFID tags, and show their Meta information: Tag ID, Tag Type, manufacturer etc. The user data memory of a tag can be displayed and modified using either a Hex or an ASCII editor. In addition, the integrated cookie feature demonstrates how easy it is for a company to abuse RFID technology to spy on their customers." <sup>2</sup>

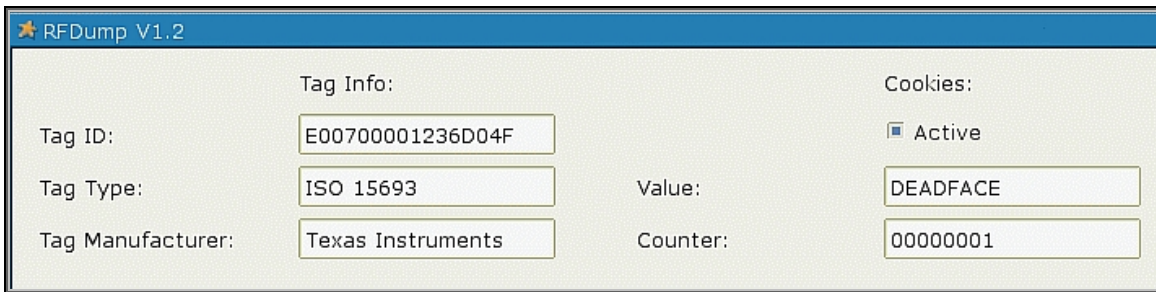
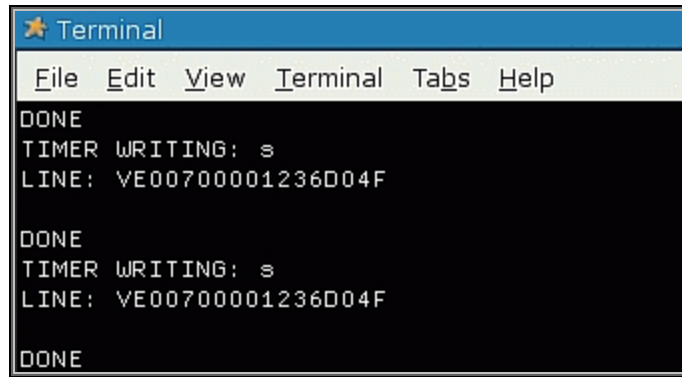


Figure 1: RFDump User Interface

Memory:									
Adr	0 / 8	1 / 9	2 / A	3 / B	4 / C	5 / D	6 / E	7 / F	ASCII
0	53616D70	6C652052	46494420	4D657461	2D446174	61207374	6F726564	206F6E20	Sample RFID Meta-Data stored on
0	74686520	536D6172	742D4C61	626C652E	2E2E2E2E	2E2E2E2E	2E2E2E2E	2E2E2E2E	the Smart-Label.....
1	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	.....
1	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	.....
2	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	.....
2	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	.....
3	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	.....
3	00000000	00000000	00000000	00000000	00000000	DEADFACE	00000001	00000000	.....

Figure 2: RFDump User Interface

<sup>2</sup> <http://www.rf-dump.org/>



**Figure 3: RFDump User Interface**

RFDump is available at no cost from the author's website. When combined with a personal computer or PDA, RFDump can reproduce the read/write functionality of RFID tag readers costing several thousands of dollars, easily bringing the ability to spoof tags into the low-cost realm.

### **Skimming Tag Data**

Skimming occurs when an intruder within range of a tag uses an unauthorized tag reader to read information contained on a tag, without the tag owners knowledge.

### **Eavesdropping of Tag and Reader Transmissions**

Eavesdropping occurs when an intruder intercepts read-data being transmitted from the tag to an authorized tag reader, or write-data being transmitted from an authorized tag reader to a tag.

### **Counterfeiting Tag Data**

By using skimming or eavesdropping techniques to read tag data, or intercept data being written to a tag, tags which are designed to "certify" the authenticity of a product (usually high-cost or designer items) could be counterfeited by purchasing similar read/write tags and programming them with authentic data captured from an original tag, allowing for the creation of counterfeit products which are supposed to be protected by the authentic tag data.

### **Industrial Espionage**

Using skimming and eavesdropping techniques, an intruder could collect tag data related to a company's supply-chain, yielding sensitive inventory information. The speed with which tag readers are able to read multiple product tags makes this type of attack scenario possible. Such an attack on bar-coded products would not scale to the level necessary to make such an attack successful, due to the slow scan speed of bar code technology. Over time, using this scenario, product sales data could be determined by correlating changes in inventory levels.

### **Denial-of-Service Attacks**

An intruder who is not able to eavesdrop or forge valid tags can simply attack the RFID infrastructure. This can include corrupting inventory data, interrupting supply

chains, or signal jamming tag readers. An intruder using a hand held device and a program such as [RFDump](#) (described earlier) could modify or erase tag data.

### Physical Tag Attacks

Some of the physical attacks that are possible against smartcards (such as etching, microprobing, power analysis, and glitching) are also applicable to RFID tags. These types of attacks can be placed into one of two categories: invasive, or, non-invasive. For example, microprobing occurs when an RFID tag or smartcard is physically opened (invasive) and the chip surface is accessed with semiconductor test equipment to allow observation and manipulation of the internal data paths. Power analysis (non-invasive) measures the precise timing and power requirements of certain tag operations.

### Weak Cryptography

As previously discussed, low-cost RFID tags are resource constrained with respect to memory and logic functions. Thus, the ability to implement strong encryption in low-cost tags is not feasible. Because of this, encryption is not used in most low-cost tags, resulting in many of the security issues reviewed in this KB. Manufacturers who do wish to use encryption in their low-cost RFID tags must resort to weaker cryptographic implementations (40-bit), capable of fitting within the memory and logic constraints of low-cost tags. This lack of strong cryptography makes these tags susceptible to [brute-force attacks](#) of the key space. For example, in January of 2005, researchers at John Hopkins University and [RSA Labs](#) announced that they had successfully attacked a Texas Instruments (TI) Digital Signature Transponder (DST) RFID chip<sup>3</sup> by guessing its 40-bit key using a brute-force attack. Researchers were then able to clone a TI DST RFID and use it to start a vehicle and buy gasoline. The TI DST RFID is currently used in such systems as the ExxonMobil SpeedPass and Ford Immobilizers (see Figure 2).



**Figure 4: ExxonMobile SpeedPass, and Ford Immobilizer key**

---

<sup>3</sup> A DST (such as pictured in Figure 2) consists of a small microchip and antenna coil encapsulated in a plastic or glass capsule. It is a passive device. It contains a secret, 40-bit cryptographic key which is field-programmable via RF command. In its interaction with a reader, a DST emits a factory-set (24-bit) identifier, and then authenticates itself by engaging in a challenge-response protocol. The reader initiates the protocol by transmitting a 40-bit challenge. The DST encrypts this challenge under its key and returns a 24-bit response. It is thus the secrecy of the key that ultimately protects the DST against cloning and simulation. Source: [Security Analysis of a Cryptographically-Enabled RFID Device](#)

## Improving the Security of Low-Cost RFID

What can be done to improve the security of low-cost RFID? As discussed in Part 1 of this KB, a number of international, national, and organizational standards bodies are researching methods and creating standards designed to improve the security of low-cost RFID. Some of the specific security design goals include:

- Making the spoofing of tags and readers more difficult
- Providing for authentication of both low-cost tags and tag readers
- Developing cryptographic primitives – hash functions, random number generators, etc, that can be implemented in low-cost tags.
- Implementing encryption algorithms into low-cost tags, such as the proposed [Tiny Encryption Algorithm](#), which has a much smaller footprint than do the [DES](#) or [AES](#) algorithms.

## RFID Privacy Concerns

“How would you like it if, for instance, one day you realized your underwear was reporting on your whereabouts?”<sup>4</sup> This quote, by State Senator Debra Bowen during California Senate hearings is typical of the attitude of private individuals today toward RFID. Privacy activists worry that unchecked; the use of RFID could trample consumer privacy. Of concern is the possibility that companies, governments and would-be thieves could monitor a person’s personal belongings which contain embedded RFID tags, after they are purchased. Retailers might also gather personal consumer data about activity in their stores. Using this data, they might then use data aggregation techniques to combine information from several different sources into a single profile or dossier on an individual’s lifestyle or buying habits.

The [Electronic Privacy Information Center](#) (EPIC) categorizes privacy as:

- **Information Privacy:** rights regarding the handling of personal information such as tax, medical or purchase records. Also known as “data privacy”.
- **Bodily Privacy:** the right not to be subjected to invasive bodily procedures such as cavity searches and blood, urine or genetic tests.
- **Communication Privacy:** the right to communicate with others in secrecy.
- **Territorial Privacy:** limits intrusion into domestic, workplace or public environments, including searches, identification checks and video surveillance.

The RFID privacy threats discussed in the following paragraphs do, in some cases, violate aspects of the privacy rights defined by EPIC.

### Skimming and Eavesdropping

Personal privacy may be violated by the leaking (skimming or eavesdropping) of personal information, such as medical prescriptions, brand of underwear, and other types of product information that might be deemed of a sensitive nature from tags to unauthorized tag readers.

---

<sup>4</sup> [Privacy Advocates Call for RFID Regulation](#)

## **Traffic Analysis**

By correlating data obtained from multiple tag reader locations, it is possible to track movement, social interactions, and financial transactions of individuals.

## **Location Tracking**

Location tracking (a form of traffic analysis) occurs when RFID embedded products (such as automobile tires), or RFID enabled systems (such as EZ-Pass Toll Collection), can be linked to an individual, and then used to track the physical movements of that individual. For example, in New York City, records of the EZ-Pass system have been subpoenaed in divorce cases, providing location information on an individual at a given time. RFID tags which have not been disabled (issued a kill command) after a purchase, create a digital paper trail which can be used against an individual.

## **Improving the Privacy of RFID**

To overcome the privacy concerns that many individuals have about RFID, low-cost RFID will need to address the following privacy design aspects:

- Tags cannot compromise the privacy of tag holders
- Information from tags should not be leaked to unauthorized tag readers
- It should be impossible to aggregate long-term tracking associations
- Tag holders should be able to detect and disable (kill) tags they carry
- Publicly available tag output should be randomized
- Private tag contents should be protected by access control and encryption

## **Conclusion**

Low-cost RFID still faces many security and privacy challenges. There are technology challenges associated with implementing security on low-cost RFID tags, and costs challenges associated with using more secure high-cost RFID tags in retail and consumer applications. Retailers will resist implementing stronger RFID security and privacy features until secure low-cost RFID tags are available, or consumer pressures or legal requirements force them to do so.

## **References**

- **RFID Privacy and Security, RSA Laboratories**  
<http://www.rsasecurity.com/rsalabs/node.asp?id=2115>
- **RFID Security & Privacy Lounge**  
<http://www.avoine.net/rfid/>
- **Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID**  
[http://www.amazon.com/gp/product/1595550208/qid=1122390116/sr=8-1/ref=pd\\_bbs\\_1/103-6518374-5716648?v=glance&n=283155](http://www.amazon.com/gp/product/1595550208/qid=1122390116/sr=8-1/ref=pd_bbs_1/103-6518374-5716648?v=glance&n=283155)

## **Summary**

Part 1 of this article described the technology components and standards that typically make up an RFID system, as well as some of the early uses of RFID technology. Part 2 reviewed many of the common security and privacy concerns associated with the use of RFID, primarily related to low-cost RFID devices, and some of the general security and privacy design goals that address those concerns.

**Jack Maynard, CISSP** is a senior information security technology consultant with Hewlett-Packard Company. His blog [USA Privacy Research](#) or Twitter [@PrivacyResearch](#) examines privacy and information security. Jack lives in Seattle, Washington USA, where on most sunny days he can be found riding his Harley-Davidson motorcycle. You can reach him at [USAPrivacyResearch@gmail.com](mailto:USAPrivacyResearch@gmail.com).