RFID (Radio Frequency Identification): Principles and Applications

Stephen A. Weis
MIT CSAIL

Outline

Key Words:

RFID, radio frequency identification, electronic article surveillance, sensor networks

Abstract

Deployment of radio frequency identification (RFID) systems is rapidly growing and has the potential to affect many different industries and applications. We present a brief history of RFID technology and automatic identification systems. We summarize major RFID

applications, and present a primer on RFID fundamental principles. Finally, we discuss several challenges and obstacles to RFID adoption, as well as emerging technologies relevant to RFID.

1 Introduction

Radio frequency identification (RFID) is a rapidly growing technology that has the potential to make great economic impacts on many industries. While RFID is a relatively old technology, more recent advancements in chip manufacturing technology are making RFID practical for new applications and settings, particularly consumer item level tagging. These advancements have the potential to revolutionize supply-chain management, inventory control, and logistics.

At its most basic, RFID systems consist of small transponders, or *tags*, attached to physical objects. RFID tags may soon become the most pervasive microchip in history. When wirelessly interrogated by RFID transceivers, or *readers*, tags respond with some identifying information that may be associated with arbitrary data records. Thus, RFID systems are one type of automatic identification system, similar to optical bar codes.

There are many kinds of RFID systems used in different applications and settings. These systems have different power sources, operating frequencies, and functionalities. The properties and regulatory restrictions of a particular RFID system will determine its manufacturing costs, physical specifications, and performance. Some of the most familiar RFID applications are item-level tagging with *electronic product codes*, proximity cards for physical access control, and contact-less payment systems. Many more applications will become economical in the coming years.

While RFID adoption yields many efficiency benefits, it still faces several hurdles. Besides the typical implementation challenges faced in any information technology system and economic barriers, there are major concerns over security and privacy in RFID systems. Without proper protection, RFID systems could create new threats to both corporate security and personal privacy.

In this section, we present a brief history of RFID and automatic identification systems. We summarize several major applications of RFID in Section 2. In Section 3, we present a primer on basic RFID principles and discuss the taxonomy of various RFID systems. Section 4 addresses the technical, economic, security, and privacy challenges facing RFID adoption. Finally, Section 5 briefly discusses emerging technologies relevant to RFID.

1.1 RFID Origins

The origins of RFID technology lie in the 19th century when luminaries of that era made great scientific advances in electromagnetism. Of particular relevance to RFID are Michael Faraday's discovery of electronic inductance, James Clerk Maxwell's formulation of equations describing electromagnetism, and Heinrich Rudolf Hertz's experiments validating Faraday and Maxwell's predictions. Their discoveries laid the foundation for modern radio communications.

Precursors to automatic radio frequency identification systems were automatic object *detection* systems. One of the earliest patents for such a system was a radio transmitter for object detection system designed by John Logie Baird in 1926 [4]. More well known is Robert Watson-Watt's 1935 patent for a "Radio Detection and Ranging" system, or RADAR. The passive communication technology often used in RFID was first presented in Henry Stockman's seminal paper "Communication by Means of Reflected Power" in 1948 [23].

One of the first applications of a radio frequency identification system was in "Identify Friend or Foe" (IFF) systems deployed by the British Royal Air Force during World War II 0. IFF allowed radar operators and pilots to automatically distinguish friendly aircraft from enemies via RF signals. IFF systems helped prevent "friendly fire" incidents and aided in intercepting enemy aircraft. Advanced IFF systems are used today in aircraft and munitions, although much of the technology remains classified.

Electronic detection, as opposed to identification, has a long history of commercial use. By the mid- to late-1960s, Electronic Article Surveillance (EAS) systems were commercially offered by several companies, including Checkpoint Systems and Sensormatic. These EAS systems typically consisted of a magnetic device embedded in a commercial product and would be deactivated or removed when an item was purchased. The presence of an activated tag passing through an entry portal would trigger an alarm. These types of systems are often used in libraries, music stores, or clothing stores. Unlike RFID, these types of EAS systems do not automatically identify a particular tag; they just detect its presence.

1.2 Auto-Identification and RFID

In terms of commercial applications, RFID systems may be considered an instance of a broader class of automatic identification (auto-ID) systems. Auto-ID systems essentially attach a name or identifier to a physical object by some means that may be automatically read. This identifier may be represented optically, electromagnetically, or even chemically.

Perhaps the most successful and well-known auto-ID system is the Universal Product Code (UPC). The UPC is a one-dimensional, optical barcode encoding product and brand information. UPC labels can be found on most consumer products in the United States. Similar systems are deployed worldwide.

The Uniform Code Council (UCC), a standards body originally formed by members of the grocery manufacturing and food distribution industries, originally specified the UPC [25]. A precursor body to the UCC first met in 1969 to discuss the need for an inter-industry auto-ID system. By 1973, a one-dimensional (or linear) barcode design was chosen. In 1974, a supermarket in Ohio scanned the first UPC-labeled product: a package of Wrigley's gum.

Adoption of the UPC grew steadily throughout the following years, to the point where UPC barcode scanners are found in a vast majority of large American retailers. Today, over five billion barcodes are scanned around the world each day. Shipping and transit companies, such as United Parcel Service, Federal Express, and the United States Postal service, commonly use two-dimensional barcodes, which can carry more data in a smaller surface area.

Optical barcodes offer faster, more reliable, and more convenient inventory control and consumer checkout than checking out by hand. Several weaknesses of optical barcodes are that they require line-of-sight and may be smudged or obscured by packaging. In most circumstances, optical barcodes still require some human manipulation to align a barcode label with a reader. Supermarket shoppers have certainly experienced a checker struggling to scan an optical barcode.

Auto-ID systems that transmit data via RF signals, i.e. RFID, do not have the same performance limitations as optical systems. Data may be read without line-of-sight and without human or mechanical intervention. A key advantage in RF-based auto-ID systems is parallelism. Modern RFID systems may offer read rates of hundreds of items per second.

2 Applications

Early commercial examples of RFID applications include automatic tracking of train cars, shipping containers, and automobiles. Railroad cars were originally labeled with optical bar code labels for tracking. These labels began to deteriorate and be obscured by dirt, causing reads to fail. As a solution, railroad companies began to tag railcars with RFID devices. By 1994, these devices were mandatory and nearly every railcar in the United States was tagged.

RFID devices began to be used for automated toll collection in the late 1980s and early 1990s. Electronic toll systems have since been adopted around the world. Like railway and shipping applications, electronic toll systems may use sturdy, self-powered RFID devices. Automobiles, railcars, and shipping containers are all high-value items, with ample physical space that can accommodate more expensive and bulky RFID devices. These types of tags could offer much more functionality than simple identification. For example, shipping containers might have accelerometer sensors, tamper alarms, or satellite tracking integrated into an identification device.

As manufacturing costs dropped, RFID systems began to be used for lower-value items in industries besides transport. An example is in animal identification of both pets and livestock. Glass-encapsulated RFID devices have been implanted in millions of pets throughout the United States. These tags allow lost animals to be identified and returned to their rightful owners. These tags have a very short read range.

Livestock, particularly cattle, are often labeled with a RFID device that is clamped or pierced through their ear, attached to a collar, or swallowed. Unlike implanted pet tags, these RFID devices are rugged and able to be read from greater distances. Concerns over Bovine Spongiform Encephalopathy (mad cow) disease have motivated proposals for universal tracking of livestock with these types of RFID systems. Like transport applications, animal tracking is still essentially a low-volume, high-value market that may justify relatively expensive RFID systems.

Other widespread applications of RFID systems include contactless payment, access control, or stored-value systems. Since 1997, ExxonMobil gasoline stations have offered a system called SpeedPass that allows customers to make purchases with an RFID "fob", typically a keychain-sized form factor [7]. In 2005, American Express launched a credit card enhanced with RFID that allows customers to make purchases without swiping a card 0.

RFID proximity cards or "prox cards" are commonly used for building access control at many companies and universities throughout the world. Similar systems have been used for ski-lift access control at ski resorts around the world. Many subway and bus systems around the world, for example in Singapore, use stored-value RFID proximity cards.

There are several applications that use RFID as an anti-counterfeiting measure. In 2005, the Wynn Casino in Las Vegas first opened and deployed RFID-integrated gaming tables and gambling tokens. These "chips-in-chips" are designed to frustrate counterfeiting, prevent theft, detect fraud, and to offer enhanced games or service. Besides stored-value tokens like casino chips or event tickets, there have also been proposals to tag currency [13]. In 2005, a controversial proposal to attach tags carrying biometric identification data to United States passports began to be implemented.

These applications also exposed some shortcomings of RFID. For instance, some RFID technologies do not operate well in proximity to liquids or metals. Each different technology has its own strengths and weaknesses, including variations in cost, size, power requirements, and environmental limits. There is no "one size fits all" RFID technology. The term actually describes an entire array of technologies, which are each applicable to different types of applications. Section 3 offers a detailed discussion of these various technologies.

While RFID continues to lower the costs of tracking high-value items, an untapped and lucrative market lies in tracking cheap, everyday consumer goods. Companies like Proctor & Gamble, Coca-Cola, and Wal-Mart have hundreds of billions of products and components in their supply chains. Tracking and managing the flow of goods through these supply chains is a complex and expensive enterprise.

RFID technology may streamline these supply-chain processes and save billions of dollars, savings that ultimately may be passed on to consumers. Shipping pallets or, ideally, individual items may be tracked and traced from manufacturers, through transport, wholesale, and retail into the hands of the consumer at a point-of-sale. Products could even be tracked post-consumer as they are recycled, refurbished, or disposed. What happens with respect to privacy while RFID-tagged items are in the hands of a consumer has been an issue of major contention and will be addressed in Section 4.

Supply chain management and inventory control applications of this scale require an extremely low-cost tag to be economically viable. In settings like animal identification, proximity cards, electronic toll systems, or stored-value systems, RFID tags costing as much several US dollars could be justified. However, items in consumer supply-chain management and inventory control applications are much cheaper than in traditional settings. Ideally, RFID tags in these applications should be as simple and cheap as the traditional, UPC optical bar code.

EPCglobal, an RFID standards body, has developed specifications for low-cost electronic product code (EPC) tags as a replacement for the ubiquitous UPC [6]. In the past, the lack of an open standard was a barrier to RFID adoption. The EPC standard, and to some extent, the ISO-18000 standard [11] will make it easier for users to integrate their RFID systems.

The potential for EPC may be huge. Globally, over five billion barcode transactions are conducted daily [25]. Even miniscule savings per transaction could translate into a huge aggregate cost savings. The market has already begun to adopt low-cost RFID on a large scale. A single RFID IC manufacturer, Philips Semiconductor, has already shipped several billion RFID chips.

Organizations with large supply chains are the driving force behind RFID adoption. In 2003, Wal-Mart, the world's largest retailer, mandated that all suppliers attach RFID tags to shipping pallets by the end of 2006 [1]. The United States Department of Defense issued a similar mandate for its own suppliers [27].

An illustrative example of an industry adopting RFID by way of mandate is the prescription drug industry, which must contend with a counterfeit drug market predicted to grow to US $75 billion by 2010 [28]. In response to the growing problem of counterfeit drugs, the United States Food and Drug Administration recommended that all wholesale prescription drug shipments be labeled with RFID pedigrees [8]. The goal of these pedigrees is to both attest to the authenticity of a drug shipment and to detect simply theft in the supply chain.

Some consumer industries may be independently motivated to adopt RFID early. In 2003, razor manufacturer Gillette placed a single order of five hundred million low-cost RFID tags from a manufacturer named Alien Technologies [18]. Gillette disposable razor blade cartridges are relatively expensive, costing US$1-2 per blade or more.

Because these items are small, easily concealable, and there is a constantly growing resale market, Gillette blades were one of the most frequently shoplifted consumer items. Somewhere between 15-20% of Gillette's blades are stolen (or "shrink") between manufacturer and the consumer point of sale. The high costs of "shrinkage" justified incorporating RFID tags into every razor blade package that Gillette sells.

The fashion industry has also been an early RFID-adopter. Several fashion makers like Swatch watch, Ecco shoes, Prada, and Benetton[1] have all tagged clothing with RFID labels. These tags are typically for retail inventory control, since retail clothing stores often face a high level of "shrinkage", as well a lot of legitimate movement of inventory by customers trying on clothing.

RFID tags have also been used as a pedigree for high-fashion items or to enhance the consumer shopping experience. For example, Prada's retail store in New York City offers an RFID-enhanced dressing room that displays product information and suggests matching apparel.

Clothing is particularly suited for RFID, since it does not contain metals or liquids that interfere with some types of RFID systems. Retail stores also typically do not have sensitive electronics, like medical equipment, that some RFID operating frequencies may interfere with. Clothing's relatively high per-unit value also justifies the use of RFID tags, which could be removed and recycled at purchase-time. The clothing industry was an early-adopter of simple EAS systems in the 1960s for these very reasons. It will likely be a leader in RFID adoption as well.

---

[1] We will discuss Benetton's RFID experience more in Section 4.

The next step in RFID for clothing may be to integrate tags directly in the product at the time of manufacture, rather than manually attaching temporary tags. This greatly lowers RFID handling costs. Directly incorporating RFID into products or packaging will likely become commonplace once the proper technology becomes economical. A promising direction is to print RFID labels directly into paper products during manufacturing time. This would greatly lower the handling and processing costs of integrating RFID with consumer products. We discuss printed circuits more in Section 5.

Before delving into a more detailed discussion of various RFID technologies and principles, we will summarize several of the present and envisioned future applications of RFID:

- Tracking and identification:
  - Large assets, e.g. railway cars and shipping containers
  - Livestock with rugged tags
  - Pets with implanted tags
  - Supply-chain management with EPC
  - Inventory control with EPC
  - Retail checkout with EPC
  - Recycling and waste disposal
- Payment and stored-value systems:
  - Electronic toll systems
  - Contact-less Credit Cards, e.g. American Express Blue card
  - Stored-valued systems, e.g. ExxonMobil Speedpass
  - Subway and bus passes
  - Casino tokens and concert tickets
- Access control:
  - Building access with proximity cards
  - Ski-lift passes
  - Concert tickets
  - Automobile ignition systems
- Anti-Counterfeiting:
  - Casino tokens, e.g. Wynn Casino Las Vegas
  - High-denomination currency notes,
  - Luxury goods, e.g. Prada
  - Prescription drugs

3 Principles

This section discusses basics of RFID systems and offers taxonomy of the many various types of RFID systems. We briefly discuss two major RFID standards and how they relate to practice.

3.1 System Essentials

Discussion of RFID technology tends to focus only on tag devices. It is more accurate to view RFID as a complete system that includes not only tags, but also other important components. RFID systems are composed of at least three core components:

- RFID tags, or transponders, carry object-identifying data.

- RFID readers, or transceivers, read and write tag data.
- Databases associate arbitrary records with tag identifying data.

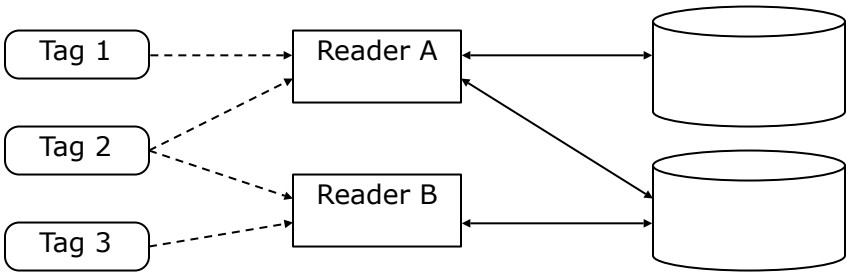

Figure 1: Illustration of RFID System Interaction

We illustrate the interaction of these components in Figure 1. In this figure, three tags are readable by one or both of two readers, A and B. For instance, tag 1 is only readable by A, while 2 is readable by both A and B, perhaps due to access control restrictions. The readers then may connect to databases with records associated with particular tag identifiers. In this case, two databases each have their own record for tag 1.

3.1.1 Tags

Tags are attached to all objects to be identified in an RFID system. A tag is typically composed of an antenna or coupling element, and integrated circuitry. An important distinction that will be discussed later is a tag's power source. Often tags carry no on-board power source and must passively harvest all energy from an RF signal.

There are many types of tags that offer different functionalities, have different power sources, or operate at different radio frequencies. Each of these variables helps determine which applications a particular tag may be appropriate for and what the costs of a tag may be. These differences will be discussed further in Section 3.2.

Modern tags tend to implement identification functionality on an integrated circuit (IC) that provides computation and storage. In the manufacturing process, this IC is attached or "strapped" to an antenna before being packaged in a form factor, like a glass capsule or foil inlay, that is integrated into a final product.

In practice, different vendors often perform each of these manufacturing steps. Other RFID designs may be "chipless" or have identifying information hard-wired at fabrication time, i.e. "write-once, read-many" tags. Newer technologies that allow RFID circuitry to be printed directly onto a product will be discussed in Section 5.

3.1.2 Readers

RFID readers communicate with tags through an RF channel to obtain identifying information. Depending on the type of tag, this communication may be a simple *ping* or may be a more complex multi-round protocol. In environments with many tags, a reader may have to perform an *anti-collision* protocol to ensure that communication conflicts to not

occur. Anti-collision protocols permit readers to rapidly communicate with many tags in serial order.

Readers often power what are called *passive* tags through their RF communication channel. These types of tags carry no on-board power and rely solely on a reader to operate. Since these tags are so limited, may subsequently rely on a reader to perform computation as well.

Readers come in many forms, operate on many different frequencies, and may offer a wide range of functionality. Readers may have their own processing power and internal storage, and may offer network connectivity. Readers might be a simple conduit to an external system, or could store all relevant data locally.

Currently, many applications rely on fixed reading devices. Early trials of EPC at a major supermarket chain integrated fixed readers into docking-bay entrances. These readers scan tags at the pallet level as shipments of products arrive. In the long term, readers may be integrated at a shelf level as a "smart shelf". Smart shelves would scan for tags at the item level and monitor when they are added and removed from a shelf.

RFID readers may also be integrated into hand-held mobile devices. These mobile readers would allow someone to, for example, take inventory of a warehouse by walking through its aisles. The cellular phone manufacturer Nokia is already offering RFID-reading functionality in some of their cell phones [16]. If EPC-type tags become highly successful, interesting and useful consumer applications might arise. If this occurs, RFID reading functionality might become a common feature on cellular phones, PDAs, or other handheld computing devices.

3.1.3 Databases

RFID databases associate tag-identifying data with arbitrary records. These records may contain product information, tracking logs, sales data, or expiration dates. Independent databases may be built throughout a supply chain by unrelated users, or may be integrated in a centralized or federated database system.

Databases are assumed to have a secure connection to readers. Although there are scenarios where readers may not be trusted, it is often useful to collapse the notions of reader and database into one entity. For example, if tags contain all relevant product information, there is no need to make a call to an off-site database.

One may imagine a federated system of back-end databases, perhaps where each product manufacturer maintains its own product look-up service. In these settings, it may be useful to deploy an Object Naming Service (ONS) to locate databases associated with some tag identification value. An ONS allows a reader to find a set of databases associated with a particular tag identification value. This is analogous to the Internet Domain Naming Service (DNS) that returns addresses of name servers that can translate domain names to numerical IP addresses. ONS has not yet been adopted widely in practice.

3.2 Power Sources

As briefly mentioned before, tags may obtain their power in several different ways. The power source is an essential property of a tag, since it will determine a tag's potential read

range, lifetime, cost, and what kind of functionalities it may offer. The power source will also be important in determining how a tag may be oriented and what physical forms it may take.

There are three main classes of tag power sources: active, semi-passive, and passive. Active tags have their own source of power, such as a battery, and may initiate communication to a reader or other active tags. Because they contain their own power source, active tags typically have a much longer operating range than passive-tags. Large asset and livestock tracking applications often use active tags, since the items they are attached to (e.g. railcars, shipping containers, or cattle) are high in value and have physical space for a bulkier, rugged tag.

A key feature of active tags is that they are able to initiate their own communication with readers. Advanced active tags, or "smart dust", might even form ad hoc peer networks with each other. One useful application of active tags is in shipping containers, which can fall off ships over rough seas. These missing containers sometimes are not accounted for until well after the ship has docked. An active tag with an accelerometer sensor could detect when it was falling off a stack of containers and broadcast a log of its demise before it sank into the ocean. Active tags could also function as security alarms using the same functionality.

By contrast a semi-passive (or semi-active) tag have an internal battery, but are *not* able to initiate communications. This ensures that semi-passive tags are only active when queried by a reader. Because semi-passive tags do have an internal power source, they do offer a longer reader range than passive attacks, but at a higher cost.

An example application that often uses semi-passive tags is electronic tollbooths. Semi-passive tags are typically affixed to the inside of a car's windshield. When the car passes through a tollbooth, it will initiate a query to the semi-passive tag and read an account identifier from the tag. The on-board battery lets the tag be read from a considerable distance. However, since the tag only needs to broadcast when queried, it can remain idle most of the time and save power. Semi-passive tags are also often used in pallet-level tracking or tracking components like automobile parts during manufacture.

Passive tags have neither their own power source, nor the ability to initiate communication. Passive tags obtain energy by harvesting it from an incoming RF communication signal. At lower frequencies, this energy is typically harvested inductively, while at higher frequencies it is harvested through capacitance.

While passive tags have the shortest read range of all three powering types, they are the cheapest to manufacture and the easiest to integrate into products. Batteries are relatively expensive and cannot easily be incorporated into some items, like paper packaging. For this reason, passive tags are the most common tags. EPC tags are passive.

Lacking an internal power source dictates many properties of passive tags. First, they cannot operate without the presence of a reader, although passive tag could temporarily cache some energy in a capacitor. Because of their necessarily weak response signal, passive tags are often more sensitive to environmental noise or interference. Table 1 compares various properties of passive, semi-passive, and active tags.

Tag Type	**Passive**	**Semi-Passive**	**Active**
Power Source	Harvesting RF energy	Battery	Battery
Communication	Response only	Response only	Respond or initiate
Max Range	10 M	> 100 M	> 100 M
Relative Cost	Least expensive	More expensive	Most expensive
Example Applications	EPC Proximity cards	Electronic tolls Pallet tracking	Large-asset tracking Livestock tracking

Table 1: Passive, Semi-passive, and Active tag comparison.

3.3 Operating Frequencies

Different RFID systems operate at a variety of radio frequencies. Each range of frequencies offers its own operating range, power requirements, and performance. Different ranges may be subject to different regulations or restrictions that limit what applications they can be used for.

The operating frequency determines which physical materials propagate RF signals. Metals and liquids typically present the biggest problem in practice. In particular, tags operating in the ultra-high frequency (UHF) range do not function properly in close proximity to liquids or metal.

Operating frequency is also important in determining the physical dimensions of an RFID tag. Different sizes and shapes of antennae will operate at different frequencies. The operating frequency also determines how tags physically interact with each other. For instance, stacking flat foil inlay tags on top of each other may interfere or prevent tags from reading properly. Table 2 lists standard frequencies and their respective passive read distances.

Frequency Range	**Frequencies**	**Passive Read Distance**
Low Frequency (LF)	120-140 KHz	10-20 cm
High Frequency (HF)	13.56 MHz	10-20 cm
Ultra-High Frequency (UHF)	868-928 MHz	3 meters
Microwave	2.45 & 5.8 GHz	3 meters
Ultra-Wide Band (UWB)	3.1-10.6 GHz	10 meters

Table 2: Common RFID operating frequencies

3.3.1 Low Frequency (LF)

Low frequency (LF) RFID tags typically operate in the 120-140 kilohertz range. Most commonly, LF tags are passively powered through induction. As a result, they typically have very short read ranges of 10-20 centimeters.

LF tags can be used in rugged environments and can operate in proximity to metal, liquids, or dirt. This makes them useful for applications like implantable pet identification tags or laundry management tags. One disadvantage of LF tags is they have a very low data read rate compared to other operating frequencies.

LF tags are often used in car immobilization and access control systems. In these systems, a car will only start if an LF tag, typically attached to the ignition key, is in proximity to the ignition. This takes advantage of LF's short read range and uses it as a security feature.

In 2006, LF passive tags may be purchased in bulk for US$1 per tag or less. Two major manufacturers of LF tags are Texas Instruments and Phillips Semiconductor. The ISO 18000-2 standard offers specifications for LF RFID tags [9].

3.3.2 High Frequency (HF)

High frequency (HF) RFID tags operate at the 13.56 megahertz frequency. HF tags are often packaged in a foil inlay or credit card form factor. This makes HF tags useful for building access control, contact-less credit cards, and ID badges. Again, the relatively short read range of HF is an advantage in theses settings.

HF tags are also used in many asset-tracking applications. Libraries and bookstores often use HF foil inlays to track books. Some airports have started using HF RFID luggage tags for baggage handling applications.

HF tags offer a higher data read rate than LF tags, but do not perform as well as LF tags in proximity to metals or liquids. HF tags do, however, offer better performance near metals or liquids than UHF tags do.

The HF frequency range lies on a heavily regulated part of the radio spectrum. Signals broadcast by readers must operate in a narrow frequency band. This presents a problem for environments with sensitive electronics, like medical equipment, that operate on nearby frequencies. This makes HF tags inappropriate for environments like hospitals.

In 2006, HF passive tags may be purchased for US$0.50 or less per tag in quantity. Texas Instruments and Phillips both offer HF tag lines, although there are many smaller and specialized manufacturers or integrators in the HF space.

International Standards Organization (ISO) specifications for HF RFID tags are specified by the ISO 18000-3 standard [11]. Related specifications for HF contact-less smart cards and proximity cards appear in ISO standards 14443 [9] and 15693 [10].

3.3.3 Ultra-High Frequency (UHF)

Ultra-high frequency (UHF) RFID tags operate in the 868-928 megahertz range. European tags typically operate within the 868-870 MHz range, while the United States and Canada operate at 902-928 MHz.

UHF tags are most commonly used for item tracking and supply-chain management applications. This is largely because they offer a longer read range and are cheaper to manufacture in bulk than LF or HF tags. The first generation EPC tags operate at UHF frequencies.

A major disadvantage of UHF tags is that they experience interference in proximity to liquids or metals. Many applications like animal tracking, metal container tracking, or even many access control systems are infeasible with UHF tags. Some materials have been developed that may shield UHF tags from metal-related distortion, but these may be cost-prohibitive to use in practice. UHF readers may also interfere with sensitive electronics like medical equipment.

UHF tags are a relatively newer technology than LF or HF, and reader costs are typically higher than the lower bandwidth LF readers. In 2006, UHF tags can be purchased in quantities for under US$0.15 per passive tag. UHF tags costing as low US$0.05 are likely to come onto the market in coming years. Specifications for RFID tags operating at UHF frequencies are defined by both the ISO 18000-6 [11] standard and the EPCGlobal standard [6].

3.3.4 Microwave

Microwave tags operate at either 2.45 or 5.8 gigahertz. This frequency range is sometimes referred to as super-high frequencies (SHF). Microwave RFID technology has come into use fairly recently and is rapidly developing. Microwave tags used in practice are typically semi-passive or active, but may also come in passive form. Semi-passive microwave tags are often used in fleet identification and electronic toll applications.

Microwave systems offer higher read rates than UHF and equivalent passive read ranges. Semi-passive and active read ranges of microwave systems are often greater than UHF counterparts. Some microwave active tags may be read from ranges of up to 30 meters, which is less than comparable UHF tags. However, physical implementations of microwave RFID tags may be much smaller and compact than lower frequency RFID tags.

There are several downsides to microwave tags. One is that they consume comparatively more energy than their lower-frequency counterparts. Microwave tags are typically more expensive than UHF tags. Commercially available active tags cost as much as $25 per tag in 2006.

Another problem is that wireless 802.11b/g (WiFi) networks may interfere with microwave RFID systems. Devices implementing the upcoming ZigBee 802.15 wireless standard could also potentially conflict with microwave RFID devices as well.

The ISO 18000-4 and the rejected ISO 18000-5 [11] standards offer respective specifications for 2.45 and 5.8 gigahertz RFID tags.

3.3.5 Ultra-Wideband (UWB)

Ultra-wideband (UWB) technology applied to RFID is fairly recent. Rather than sending a strong signal on a particular frequency, UWB uses low-power signals on a very broad range of frequencies. The signal on a particular frequency used by UWB is very weak, but in aggregate, communication is quite robust. In practice, some implementations of UWB operate from 3.1 to 10.6 GHz.

The advantages of UWB are that it has a very long line-of-sight read range, perhaps 200 meters in some settings. UWB is also compatible with metal or liquids. Since the signal on a particular frequency is very weak, UWB does not interfere with sensitive equipment. Consequently, an early application was asset tracking in a hospital setting.

A disadvantage of current implementations of UWB is that it must be active or at least semi-passive. However, since UWB tags broadcast very weak signals, they have relatively low power consumption. As of 2006, it is unclear whether the technology exists to create a passive UWB tag[2].

UWB RFID technology is still in its early phases and there are few commercial products available. Costs of US$5 per tag in bulk are reasonable in the near future.

3.4 Functionality

The basic RFID functionality is identification. When queried by a reader, tags return some identifier that may be used to retrieve other data records. However, tags may offer various other functionalities useful in different applications. The underlying principles and technologies of these various types of tags are so closely related to strict RFID tags, that they often collectively referred to as "RFID". Although not strictly RFID, we discuss several major classes of RFID-related devices.

We split RFID-style tags into five broad classes: EAS, read-only EPC, EPC, sensor tags, and motes. These will be referred to as classes A through E. EPCglobal offers five similar classes of tag based on functionality dubbed Class 0 through Class 4 [6]. The EPCglobal classes closely align with ours, but differ somewhat. These five classes are summarized in Table 3.

Class	Name	Memory	Power Source	Features
A	EAS	None	Passive	Article Surveillance
B	Read-only EPC	Read-Only	Passive	Identification Only
C	EPC	Read/Write	Passive	Data Logging
D	Sensor Tags	Read/Write	Semi-Passive	Environmental Sensors
E	Motes	Read/Write	Active	Ad Hoc Networking

Table 3: Tag Functionality Classes

Difficult technical and economic problems arise in class B and particularly class C devices. EAS tags are so limited in function that they are extremely simple and cheap to manufacture. By contrast, class D and E devices offer enough functionality to justify higher manufacturing costs and can offer relatively ample resources. The challenge "sweet spot" lies in class B and class C devices, which are part of crucial systems, yet are still subject to tight resource and cost constraints.

---

[2] Multi-frequency passive tags operating at HF, UHF, and microwave do exist in 2006. Although they do not operate as UWB tags, supporting multi-frequency communications is possible in a passive setting.

3.4.1 Electronic Article Surveillance (EAS)

EAS tags are the most basic RFID-type tag and have been in commercial use for over 40 years. EAS tags do *not* contain unique identifying information, so technically are not RFID tags. They simply announce their presence to a reader. In other words, EAS tags broadcast a single bit of information – "Someone is here".

In practice, EAS tags are almost always passive and are often attached to compact discs, clothing items, or books in retail locations. EAS tags could be active or semi-passive, but the added cost of a power source would greatly outweigh adding unique identifying functionality. Because of their limited functionality, EAS tags are the simplest and cheapest to manufacture.

3.4.2 Read-only EPC

Unlike EAS tags, EPC tags contain some identifying information. EPCglobal refers to these tags as class B tags. This information may be a product code or a unique identifier. Read-only EPC tags have a single identifier that is written once when a tag is manufactured. Thus, class B tags offer strict RFID functionality. Class B tags will likely be passively powered. Although they could be semi-passive or active, again the cost of a battery would greatly outweigh the cost of re-writable memory.

As the name suggests, EPC tags are used in basic item tracking applications. However, many other practical applications of tags, such as smart cards or proximity cards, are using tags with read-only memory that offer simple identification. Read-only EPC tags are fairly simple and may even be "chipless", thus are relatively cheap.

3.4.3 EPC

Class C refers to simple identification tags offering write-once, read-many or re-writable memory. Rather than having an identifier set at manufacture time, identifiers may be set by an end-user. If an EPC tag offers re-writable memory, its identifier may be changed many times[3]. Class C tags still offer strictly RFID functionality.

Class C EPC tags may be used as a logging device, or can emulate Class B read-only EPC tags. In practice, class B EPC tags may be passive, semi-passive, or active. Strict RFID functionality includes class B tags. Supporting non-volatile, writable memory adds complexity to class B tags. Consequently, they may be significantly more expensive than read-only EPC or EAS tags.

3.4.4 Sensor Tags

Sensor tags may contain on-board environmental sensors, and may log and store data without the aid of a reader. These types of tags will be referred to here as class D. Sensor tags offer more than strict RFID functionality, and are typically not thought of as RFID.

---

[3] Due to technical issues, "re-writeable" tags in practice typically can only be written some fixed number of times; perhaps several hundred re-writes.

Many sensor tags may form a "sensor net" that monitors a physical area's environmental properties. This may include temperature changes, rapid acceleration, changes in orientation, vibrations, the presence of biological or chemical agents, light, sound, etc. Because they operate without a reader present, sensor tags must necessarily be semi-passive or active. An on-board power source and sensor functionality comes at a much higher manufacturing cost.

3.4.5 Motes

Class E tags, or "smart dust" motes [17], are able to initiate communication with peers or other devices, and form ad hoc networks. Motes are essentially general pervasive computing devices and are much more complex than simple EPC-style RFID. Because they are able to initiate their own communication, mote devices are necessarily active. Commercial motes are available from Crossbow Technology. Ongoing research into smart dust and motes is being conducted at the University of California, Berkeley and Intel.

3.5 Standards

The two most relevant RFID standards are the International Organization for Standardization's ISO/IEC 18000 standard [11] and EPCglobal's standards [6]. These standards are not competing, and it is conceivable that EPCglobal's standard could eventually be adopted into an ISO standard.

EPCglobal defines specifications for EPC-type tags operating in the UHF range.

The ISO 18000 standard has 6 parts addressing different frequency ranges:

- Part 1 – General standards
- Part 2 - LF
- Part 3 - HF
- Part 4 – Microwave, 2.45 GHz
- Part 5 – Microwave, 5.8 GHz (withdrawn)
- Part 6 - UHF

Two other ISO standards, ISO/IEC 14443 [9] and ISO/IEC 15693 [10] are related to smart card and proximity card interfaces operating in the HF range.

4 Challenges

4.1 Technical

RFID systems still face many technical challenges and obstacles to practical adoption. A major hurdle is simply getting RFID systems to work in real-world environments. Systems that work perfectly in a lab setting may encounter problems when faced with environmental noise, interference, or human elements.

As an example, in 2005, a major retail chain tested RFID pallet-level tracking in their shipping and receiving cargo bays. The retailer experienced difficulties in achieving near 100% read rates and unanticipated, mundane technical issues. However, these issues will likely be ironed out as adoption becomes more commonplace.

Readers and tags often experienced interference caused by other wireless systems, or unknown sources. This type of interference was not systematic, and usually resulted from environmental idiosyncrasies. Addressing these issues required trial and error, and practical experience to recognize what was causing the problem. For example, simply repositioning or re-aligning readers would often address performance issues.

Software support for RFID is still in its early stages as well. Getting distributed back-end database look-ups to work in practice is a complex task that is often glossed over in RFID literature. In particular, key management and network connectivity issues are often underemphasized. Many vendors do currently offer RFID software solutions. However, in the coming years is likely that the industry will consolidate onto several standardized software interfaces.

The point of this digression is to emphasize that, like most information technology systems, RFID systems still require practical expertise to install, configure, and manage. End-users should expect to experience mundane technical complications that arise while implementing RFID. Despite marketing claims to the contrary, RFID is not a "magic bullet" that is simple to implement out of the box.

4.2 Economic

A key hurdle that still remains in RFID systems is simply cost. This is especially the case with EPC item-level tagging. A commonly cited price point where item-level tagging is supposed to be economically viable is US$0.05 per UHF tag.

As of 2006, the "5 cent tag" does not exist. Tag ICs alone (not including antenna or packaging), do cost as little as US$0.08, although these are being sold as a loss leader. It will likely be a number of years until tags are available at the 5-cent level, and those will only be in huge quantities. However, this may be an artificial breakpoint. Many applications could very well benefit from more expensive tags.

A second cost issue is readers; again, especially UHF readers, which retail in 2006 for well over US$1,000. At this price level, many firms may only afford a small number of readers in loading bays. "Smart shelves" that incorporate readers throughout a retail or warehouse environment would be prohibitively expensive for most applications.

As the market grows, RFID costs will drop and new applications will become economical, especially as more investment is made into back-end architectures. However, for the near future, the costs of many envisioned applications, particularly for EPC tags, are simply not justified.

4.3 Security and Privacy

Many concerns have been expressed over the security and privacy of RFID systems. Traditional applications, like large-asset tracking, were typically closed systems where tags did not contain sensitive information. Tags on railway cars contained the same information painted on the side of the cars themselves. However, as more consumer applications are developed, security, and especially privacy, will become important issues.

Much work has recently focused on issues of RFID security and privacy. Gildas Avoine maintains a comprehensive bibliography of RFID security and privacy papers [1]. Ari Juels offers a survey of RFID security and privacy issues in [12]. We refer the reader to these references for a more comprehensive analysis.

4.3.1 Eavesdropping

Perhaps the biggest security concerns in RFID systems are espionage and privacy threats. As organizations adopt and integrate RFID into their supply chain and inventory control infrastructure, more and more sensitive data will be entrusted on RFID tags. As these tags inevitably end up in consumer hands, they could leak sensitive data or be used for tracking individuals.

An attacker able to eavesdrop from long range could possibly spy on a passive RFID system. Despite the fact that passive tags have a short operating range, the signal broadcast from the reader may be monitored from a long distance. This is because the reader signal actually carries the tag's power, and thus necessarily must be strong.

A consequence is that a reader communicating with a passive tag in, for instance, a UHF setting might be monitored from a range up to 100-1000 meters. While this only reveals one side of a communication protocol, some older protocols actually broadcast sensitive tag data over the forward channel. Newer specifications, like the EPCglobal class-1 generation-2, take care to avoid this.

Although short-range eavesdropping requires nearby physical access, it can still be a threat in many settings. For example, a corporate spy could carry a monitoring device while a retail store conducts its daily inventory. Alternatively, a spy could simply place bugging devices that log protocol transmissions.

Espionage need not be passive. Attackers could actively query tags for their contents. Rather than waiting to eavesdrop on legitimate readers, an active attacker could simply conduct tag read operations on its own. Active attackers may be easy to detect in a closed retail or warehouse environment, but may be difficult to detect in the open.

Both eavesdropping and active queries pose threats to individual privacy. RFID tags can be embedded in clothes, shoes, books, key cards, prescription bottles, and a slew of other products. Many of these tags will be embedded without the consumer ever realizing they are there. Without proper protection, a stranger in public could tell what drugs you are carrying, what books you are reading, perhaps even what brand of underwear you prefer.

Many privacy advocates are extremely concerned about RFID [1]. In 2003, Benetton, a clothing maker, announced plans to label clothing with RFID and was promptly boycotted by several groups. This illustrates the potential of consumer backlash over privacy to impede RFID adoption.

Besides leaking sensitive data, individuals might be physically tracked by the tags they carry. Of course, cellular phones can already track individuals. Unlike a cell phone, which is only supposed to be able to be tracked by a cellular provider, RFID tags might be tracked by

anyone (granted, within a relatively short read range). Readers will eventually be cheap to acquire and easy to conceal.

Clearly, tracking someone is trivial if an attacker is able to actively query unique identifying numbers from tags. Even if unique serial numbers are removed from tags, an individual might be tracked by the "constellation" of brands they carry. A unique fashion sense might let someone physically track you through an area by your set of favorite brands.

Many privacy countermeasures have been proposed that may efficiently mitigate many of these risks. We refer the reader to Juels' survey [12] and Avoine's bibliography [1] for more information.

4.3.2 Forgery

Rather than simply trying to glean data from legitimate tags, adversaries might try to imitate tags to readers. This is a threat to RFID systems currently being used for access control and payment systems. While an adversary able to physical obtain a tag can almost always clone it, the real risk is someone able to "skim" tags wirelessly for information that can be used to produce forgeries. For instance, if tags simply respond with a static identification number, skimming is trivial.

Forgery is obviously a major issue in RFID systems used specifically as an anti-counterfeiting device. For example, the United States Food and Drug Administration (FDA) proposed attaching RFID tags to prescription drug bottles as a pedigree [8]. Someone able to produce forgeries could steal legitimate shipments and replace them with valid-looking decoys, or could simply sell counterfeit drugs with fake pedigree labels.

A cautionary example is the ExxonMobil SpeedPass, which uses an RFID keychain fob that allows customers to make purchase at ExxonMobil gas stations [6]. A team of researchers from Johns Hopkins University and RSA Security broke the weak security in SpeedPass and produce forgeries that could be used to make purchases at retail locations [5].

Fortunately, low-cost security countermeasures have recently been developed that allow readers to authenticate tags. For example, Juels and Weis offer a low-cost authentication protocol based on a hard learning problem that is efficient to implement in a tag [14]. However, as of 2006, these protocols exist on paper only and are not available in any commercial products.

4.3.3 Denial of Service

Weaker attackers unable to conduct espionage or forgery attacks may still be able to sabotage RFID systems or conduct denial of service attacks. An adversary may simply jam communication channels and prevent readers from identifying tags. An attacker could also seed a physical space with "chaff" tags intended to confuse legitimate readers or poison databases. Locating and removing chaff tags might be very difficult in a warehouse environment, for instance.

Powerful electromagnetic signals could physically damage or destroy RF systems in a destructive denial of service attack. Fortunately, attempting these attacks from long range

would require so much power that it would affect other electronic components and be easily detected.

While these denial of service and sabotage attacks may seem to be simply nuisances, they could represent serious risks. This is especially true in defense or medical applications. For example, the United States Department of Defense is moving towards RFID-based logistics control. An attack against the RFID infrastructure could delay crucial shipments of war materiel or slow down troop deployments.

4.3.4 Viruses

In 2006, researchers demonstrated a RFID virus based on an SQL injection attack [21]. The virus payload was an SQL database query that would overwrite existing RFID identifiers in the database with the virus payload. When tags were updated from the infected database, the virus would be propagated.

This virus assumes that RFID contents are essentially "executed" without any validation. It also assumes that future reads from an infected system can overwrite tag contents, which is often not the case in practice. In fact, nothing about the virus was particular to RFID systems. Input from any source, whether a network connection, USB port, or keyboard, could spread viruses when insecurely executed without validation.

5 Future Technologies

Two promising technological developments especially relevant to RFID are printed circuits and organic components [24][26]. These technologies have the potential to greatly lower manufacturing costs and to produce RFID tags built out of flexible plastic materials, instead of silicon.

The long-term vision is that a large-scale packaging manufacturer could print RFID tags directly into paper or plastic as it is produced. Product makers would not use this RFID-enhanced packaging material as they normally would. One advantage in terms of privacy is that RFID tags would only be attached to product packaging, and not the product itself.

This technology is still years away from being economic and there are many hurdles to overcome. Currently, circuits printed by an inkjet have a very low resolution; circuit gates take much more surface area than traditionally fabricated circuits. Other technologies like gravure printing also produce relatively large circuit surface areas.

Regardless, much research is being focused on organic components for other purposes, like flexible displays. Developments in this area will benefit RFID, potentially opening the door to many inexpensive and interesting future applications.

Glossary

Active tag – A tag with its own battery that can initiate communications.
Auto-ID – Automatic Identification. Auto-ID systems automatically identify physical objects through optical, electromagnetic, or chemical means.

EAS – Electronic Article Surveillance. An RF device that announces its presence but contains no unique identifying data. EAS tags are frequently attached to books or compact discs.
EPC – Electronic Product Code. A low-cost RFID tag designed for consumer products as a replacement for the UPC.
HF – High Frequency; 13.56 MHz.
IFF – Identify Friend or Foe. Advanced RFID systems used to automatically identify military aircraft.
LF – Low frequency; 120-140 KHz.
Linear barcode – A one-dimensional, optical bar code used for auto-ID.
Passive tag – A tag with no on-board power source that harvests its energy from a reader-provided RF signal.
Reader – An RFID transceiver, providing read and possibly write access to RFID tags.
RF – Radio Frequency.
RFID – Radio Frequency Identification. Describes a broad spectrum of devices and technologies, and is used to refer both to individual tags and overall systems.
Semi-passive tag – A tag with an on-board power source that is unable to initiate communications with a reader.
Skimming – An attack where an adversary wirelessly reads data from a RFID tag that enables forgery or cloning.
Tag – An RFID transponder, typically consisting of an RF coupling element and a microchip that carries identifying data. Tag functionality may range from simple identification to being able to form ad hoc networks.
UCC – Uniform Code Council; a standards committee originally formed by grocery manufacturers and food distributors that designed the UPC barcode.
UHF – Ultra-High Frequency; 868-928 MHz.
UPC – Universal Product Code. A one-dimensional, optical barcode found on many consumer products.
UWB – Ultra Wide Band; a weak communication signal is broadcast over a very wide band of frequencies, e.g. 3.1-10.6 GHz.

Bibliography

[1] Albrecht, K., and McIntyre, L. (2005). Spychips : How Major Corporations and Government Plan to Track Your Every Move with RFID. Nelson Current Publishing.

[2] Avoine, G. (2006). Security and Privacy in RFID Systems Bibliography. Available at: http://lasecwww.epfl.ch/~gavoine/rfid/. (Last Accessed: March 11, 2006.)

[3] Auto-ID Labs. (2006). Webpage. Available at: http://www.autoidlabs.org. (Last Accessed: March 11, 2006.)

[4] Baird, J.L. (1928). "Improvements in or relating to apparatus for transmitting views or images to a distance". Patent #GB292,185.

[5] Bono, S., Green, M., Stubblefield, A., Rubin, A., Juels, A., and Szydlo, M. (2005). Analysis of the Texas Instruments DST RFID. Available at: http://rfidanalysis.org. (Last Accessed: March 9, 2006.)

[6] EPCglobal. (2006). Webpage. Available at: http://www.epcglobalinc.org. (Last Accessed: March 11, 2006.)

[7] ExxonMobile Speedpass. (2006). Webpage. Available at: http://www.speedpass.com. (Last Accessed: March 11, 2006).

[8] Food and Drug Administration. (2004). Combating Counterfeit Drugs. Technical Report. United States Department of Health and Human Services. Available at: http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html. (Last Accessed: March 11, 2006.)

[9] International Organization for Standardization (ISO). (2003). Identification cards -- Contactless integrated circuit(s) cards -- Vicinity cards. ISO/IEC 14443.

[10] Ibid. (2003). Identification cards -- Contactless integrated circuit(s) cards -- Vicinity cards. ISO/IEC 15693.

[11] Ibid. (2004). RFID for Item Management. ISO/IEC 18000.

[12] Juels, A. (2006). RFID Security and Privacy: A Research Survey. Selected Areas of Cryptography. To appear, 2006.

[13] Juels, A., Pappu, R. (2003). Squealing Euros: Privacy-Protection in RFID-Enabled Banknotes. Financial Cryptography. Lecture Notes in Computer Science. Volume 2742, pages 103-121.

[14] Juels, A., Weis, S.A. (2005). Authenticating Pervasive Devices with Human Protocols. Advances in Cryptology – Crypto '05. Lecture Notes in Computer Science. Volume 3621. Pages 293-308.

[15] Krane, J. (2003). Benetton clothing to carry tiny tracking transmitters. Associated Press.

[16] Nokia. (2004). Nokia Mobile RFID Kit. Available at: http://www.nokia.com/nokia/0,,55738,00.html. (Last Accessed: March 11, 2006.)

[17] Pister, K. (2004). Smart Dust: Autonomous Sensing and Communications in a Cubic Millimeter. Available at: http://robotics.eecs.berkeley.edu/~pister/SmartDust/. (Last Accessed: March 11, 2006.)

[18] RFID Journal. (2003). Gillette Confirms RFID Purchase. RFID Journal. Available at: http://www.rfidjournal.com/article/articleview/258/1/1/. (Last Accessed: March 11, 2006.)

[19] Ibid. (2003). Wal-Mart Expands RFID Mandate. RFID Journal. Available at: http://www.rfidjournal.com/article/articleview/539/1/1/. (Last Accessed: March 11, 2006.)

[20] Ibid. (2005). AmEx Adds RFID to Blue Credit Cards. RFID Journal. Available at: http://www.rfidjournal.com/article/articleview/1646/1/1/. (Last Accessed: March 11, 2006.)

[21] Rieback, M.R., Crispo, B., Tanenbaum, A.S. (2006). Is your cat infected with a computer virus? Pervasive Computing and Communications. IEEE Press. Pages 169-179.

[22] Royal Air Force. (2006). Royal Air Force History. Available at: http://www.raf.mod.uk/history/line1940.html. (Last Accessed: March 11, 2006.)

[23] Stockman, H. (1948). Communication by Means of Reflected Power. Proceedings of the Institute of Radio Engineers. October. Pages 1196-1204.

[24] Subramanian, V., Chang, P., Huang, D., Lee, J., Molesa, S., Redinger, D., and Volkman, S. (2006). Conference on VLSI Design. Pages 709-714. IEEE Press.

[25] Uniform Code Council. (2006). Webpage. Available at: http://www.uc-council.org. (Last Accessed: March 11, 2006.)

[26] University of California, Berkeley Organic Electronics Group. Website. Available at: http://organics.eecs.berkeley.edu/. (Last Accessed: March 11, 2006.)

[27] United States Department of Defense. (2006). Radio Frequency Identification. Available at: http://www.acq.osd.mil/log/rfid/index.htm. (Last Accessed: March 11, 2006.)

[28] World Health Organization. (2006). Counterfeit Medicines. Available at: http://www.who.int/mediacentre/factsheets/fs275/en/. (Last Accessed: March 11, 2006.)