Chapter 2

UNDERSTANDING RFID TECHNOLOGY

Simson Garfinkel
Henry Holtzman[1]

Introduction

This chapter presents a technical introduction to the RFID, the Electronic Product Code (EPC), and the Object Name Service (ONS). It then looks at two specific RFID applications that have been fielded over the past ten years.

RFID Technology

Most histories of RFID trace the technology back to the radio-based identification system used by Allied bombers during World War II. Because bombers could be shot down by German anti-aircraft artillery, they had a strong incentive to fly bombing missions at night because planes were harder for gunners on the ground to target and shoot down. Of course, the Germans also took advantage of the cover that darkness provided. Early Identification Friend or Foe (IFF) systems made it possible for Allied fighters and anti-aircraft systems to distinguish their own returning bombers from aircraft sent by the enemy. These systems, and their descendants today, send coded identification signals by radio: An aircraft that sends the correct signal is deemed to be a friend, and the rest are foe. Thus, radio frequency identification was born.

[1] Henry Holtzman is a research scientist at the MIT Media Laboratory and the founder of Presto Technologies.

Shortly after the war, an engineer named Harry Stockman realized that it is possible to power a mobile transmitter completely from the strength of a received radio signal. His published paper "Communication by Means of Reflected Power" in the Proceedings of the IRE[2] introduced the concept of passive RFID systems.

Work on RFID systems as we know them began in earnest in the 1970s. In 1972, Kriofsky and Kaplan filed a patent application for an "inductively coupled transmitter-responder arrangement."[3] This system used separate coils for receiving power and transmitting the return signal. In 1979, Beigel filed a new application for an "identification device" that combined the two antennas; many consider his application by to be the landmark RFID application because it emphasized the potentially small size of RFID devices.[4]

In the 1970s, a group of scientists at the Lawrence Livermore Laboratory (LLL) realized that a handheld receiver stimulated by RF power could send back a coded radio signal. Such a system could be connected to a simple computer and used to control access to a secure facility. They developed this system for controlling access to sensitive materials at nuclear weapons sites.

Today we would call this Livermore system an example of security through obscurity: What made the system secure was that nobody else had a radio capable of receiving the stimulating radio signal and sending back the properly coded response. But at the time it was one of the most secure access control systems available. The scientists left LLL a few years later and created their own company to commercialize the technology. This system ultimately became one of the first building entry systems based on proximity technology and the first commercial use of RFID.

The Elements of an RFID System

RFID systems fundamentally consist of four elements: the RFID tags themselves, the RFID readers, the antennas and choice of radio characteristics, and the computer network (if any) that is used to connect the readers.[5]

[2] Harry Stockman, "Communication by Means of Reflected Power," Proceedings of the IRE, pp. 1196–1204, October 1948.

[3] Kriofsky, T.A., Kaplan, L.M.: 1975. U.S. Patent No. 3859624

[4] Beigel, M. 1982. U.S. Patent No. 4333072

[5] Much of the information in this chapter draws on technical information presented in Finkenzeller, K. *RFID-Handbook*, *Second Edition*, Wiley & Sons, Ltd., April 2003. Translated from the third German edition by Wadding, R. www.rfid-handbook.de/english/index.html.

RFID Tags

The tag is the basic building block of RFID. Each tag consists of an antenna and a small silicon chip that contains a radio receiver, a radio modulator for sending a response back to the reader, control logic, some amount of memory, and a power system. The power system can be completely powered by the incoming RF signal, in which case the tag is known as a *passive tag*. Alternatively, the tag's power system can have a battery, in which case the tag is known as an *active tag*.

The primary advantages of active tags are their reading range and reliability. With the proper antenna on the reader and the tag, a 915MHz tag can be read from a distance of 100 feet or more. The tags also tend to be more reliable because they do not need a continuous radio signal to power their electronics.

Passive tags, on the other hand, can be much smaller and cheaper than active ones because they don't have batteries. Another advantage is their longer shelf life: Whereas an active tag's batteries may last only a few years, a passive tag could in principle be read many decades after the chip was manufactured.

Between the active and the passive tags are the *semi-passive* tags. These tags have a battery, like active tags, but still use the reader's power to transmit a message back to the RFID reader using a technique known as backscatter. These tags thus have the read reliability of an active tag but the read range of a passive tag. They also have a longer shelf life than a tag that is fully active.

Tags come in all shapes and sizes. The smallest tag that has ever been produced is the Hitachi mu-chip, which is less than 0.4mm on a side. Designed to be embedded in a piece of paper and used for tracking documents printed in an office environment, the mu-chip can be read only at a distance of a few centimeters. Of course, the mu-chip is a passive tag. With a larger antenna it could have a significantly longer reading range, but that would defeat its purpose.

Other small tags are the implantable tags the size of a grain of rice manufactured by VeriChip. Like the mu-chip, these passive tags have a very limited reading range; their intended application is to give machine-readable serial numbers to people. The company says that the chips can be used to authenticate people in high-security environments—unlike passwords, the implanted chips can't be easily shared—and in hospitals, where staff occasionally mix up patients and give them the wrong treatments. Implantable chips might also work to identify wandering Alzheimer's patients who go out without any identification or cognizance of their location or destination. We'll come back to the topic of implantable chips later in this chapter.

RFID tags can also be quite large. The semipassive RFID tag used in the FastLane and E-ZPass electronic toll collection systems is the size of a paperback book and includes an antenna and a five-year battery. The battery gives the system a longer read range and also makes reads more reliable—at least until the battery dies. In practice, the instrumented toll crossings have a large light that flashes green if the tag is read successfully, red if no tag is detected, and amber or yellow if the tag cannot be read properly. When the light flashes amber, the driver is supposed to call the program's administrator and arrange to have the tag sent in for service.

RFID tags can be *promiscuous*, in which case they will communicate with any reader. Alternatively, they can be *secure*, requiring that the reader provide a password or other kind of authentication credential before the tags respond. The vast majority of RFID tags that have been deployed are promiscuous. Not only are these tags cheaper, but the systems also are much easier to manage. Systems that employ passwords or encryption codes require that the codes be distributed in advance and properly controlled. This is an exceedingly difficult management problem.

The simplest RFID chips contain only a serial number—think of this as a 64-bit or 96-bit block of read-only storage. Although the serial number can be burned into the chip by the manufacturer, it is also common for the chips to be programmed in the field by the end user. Some chips will accept only a single serial number, while other chips allow the serial number to be changed after it is burned in. More sophisticated RFID chips can contain read-write memory that can be programmed by a reader. Chips can also have sensors, an example of which is an air pressure sensor to monitor the inflation of a tire. The chips might store the results of the sensor in a piece of read-write memory or simply report the sensor's reading to the RFID reader. Chips can also have a self-destruct, or "kill" feature. This is a special code that, when received by the chip, causes the chip to no longer respond to commands. For financial applications, the full capabilities of smart cards have been combined with the wireless protocols and passive powering used in RFID. The result is a class of high-capability RFID tags also called contactless smart cards.

RFID tags can interfere with each other. When multiple tags are present in a reader's field, the reader may be unable to decipher the signals from the tags. For many applications, such as raising the gate in a parking lot, this is not a problem. The systems are optimized so that only one tag is within range at a time. However, for other applications, reading multiple tags at once is essential. For these applications, the tags need to support either an anticollision protocol or, more commonly, a singulation protocol. A singulation protocol allows a reader to determine that multiple tags are visible and to iterate through the tags, getting them to take turns responding so that each may be read without interference from the others.

Electronic Product Code (EPC) tags are a special kind of tag that follows the EPC standard developed by the MIT Auto-ID Center and is now managed by the trade organization EPCglobal. Sanjay Sarma, cofounder of the Auto-ID Center, discusses the history of the EPC standard in Chapter 3.

EPCglobal has defined a series of RFID tag "classes" and "generations" of RFID devices (see Tables 2.1 and 2.2).

Table 2.1 EPC RFID Classes

EPC Device Class	Definition	Programming
Class 0	"Read only" passive tags	Programmed by the manufacturer
Class 1	"Write-once, read-many" passive tags	Programmed by the customer; cannot be reprogrammed
Class 2	Rewritable passive tags	Reprogrammable
Class 3	Semipassive tags	
Class 4	Active tags	
Class 5	Readers	

Table 2.2 EPC RFID Chip Generations

Feature	Generation 1	Generation 2
Frequency	860–930MHz	860–960MHz
Memory capacity	64 or 96 bits	96–256 bits
Field-programmability	Yes	Yes
Reprogrammability	Class 0—read only Class 1—write once/ready many	NA
Other features	NA	Faster and more reliable reads than Generation 1 Better compliance with other global standards

Readers

The RFID reader sends a pulse of radio energy to the tag and listens for the tag's response. The tag detects this energy and sends back a response that contains the tag's serial number and possibly other information as well.

In simple RFID systems, the reader's pulse of energy functioned as an on-off switch; in more sophisticated systems, the reader's RF signal can contain commands to the tag, instructions to read or write memory that the tag contains, and even passwords.

Historically, RFID readers were designed to read only a particular kind of tag, but so-called *multimode readers* that can read many different kinds of tags are becoming increasingly popular.

RFID readers are usually on, continually transmitting radio energy and awaiting any tags that enter their field of operation. However, for some applications, this is unnecessary and could be undesirable in battery-powered devices that need to conserve energy. Thus, it is possible to configure an RFID reader so that it sends the radio pulse only in response to an external event. For example, most electronic toll collection systems have the reader constantly powered up so that every passing car will be recorded. On the other hand, RFID scanners used in veterinarian's offices are frequently equipped with triggers and power up the only when the trigger is pulled.

Like the tags themselves, RFID readers come in many sizes. The largest readers might consist of a desktop personal computer with a special card and multiple antennas connected to the card through shielded cable. Such a reader would typically have a network connection as well so that it could report tags that it reads to other computers. The smallest readers are the size of a postage stamp and are designed to be embedded in mobile telephones.

Antennas and Radio

The RFID physical layer consists of the actual radios and antennas used to couple the reader to the tag so that information can be transferred between the two.

Radio energy is measured by two fundamental characteristics: the *frequencies* at which it oscillates and the strength or *power* of those oscillations. Commercial FM broadcast stations in the United States transmit with energy at a frequency between 88MHz and 108MHz, or 1 million isolations per second. The AM spectrum, by contrast, transmits at 500,000 to 1,500,000 oscillations per second, or between 500KHz and 1500KHz. Microwave ovens cook with RF energy that vibrates 2.4 billion times each second, which is 2.4GHz.

Most RFID systems use the so-called *unlicensed spectrum*, which is a specific part of the spectrum set aside for use without a radio license. Popular bands are the low-frequency (LF) band at 125–134.2KHz, the high-frequency band at 13.56MHz, the ultrahigh-frequency (UHF) band at 915MHz (in North America; varies in other regions), and the industrial, scientific, and medical (ISM) band at 2.4GHz.

The names of the LF, HF, and UHF bands reflect the history of radio's development: Radio systems first transmitted at the lower frequencies and moved to the higher frequencies only as technology advanced. For this reason, lower-frequency radio gear was traditionally cheaper than equipment that operated at higher frequencies. Today, however, the difference in radio prices more often reflects market sizes, the cost of patents and other licenses, and the result of subsidies or cross-marketing agreements from equipment manufacturers.

Radio energy moves in waves, and each radio wave has not only a frequency but also a wavelength. The wavelength is like the distance between two wave crests on the ocean. With radio energy, the wavelength of a radio wave multiplied by its frequency is equal to the speed of light: 3×10^8 meters per second (roughly equal to 186,000 miles per second). The size of waves for each of the unlicensed bands is presented in Table 2.3.

Table 2.3 Band Frequency, Wavelength, and Classical Usage

Band	Unlicensed Frequency	Wavelength	Classical Use
LF	125–134.2KHz	2,400 meters	Animal tagging and keyless entry
HF	13.56MHz	22 meters	
UHF	865.5–867.6MHz (Europe) 915MHz (U.S.) 950–956MHz (Japan)	32.8 centimeters	Smart cards, logistics, and item management
ISM	2.4GHz	12.5 centimeters	Item management

Building proximity cards, automobile immobilizer chips, and implantable RFID ampoules tend to operate in the LF band. The FDA has adopted the HF band for RFID systems used for prescription drugs. The EPC system operates in the HF and UHF bands, although early deployments are favoring the UHF band.

When analyzing the energy that is radiated from an antenna, electrical engineers divide the field into two parts: the *near field*, which is the part of radiation that is within a small number of wavelengths of the antenna, and the *far field*, which is the energy that is radiated beyond the near field. Because the wavelength of LF and HF devices tends to be much larger than the ranges at which

RFID systems typically operate, these systems operate in the near field, while UFH and ISM systems operate in the far field.

As with most radio systems, the larger the antenna on the reader and the tag, the better an RFID system will work because large antennas are generally more efficient at transmitting and receiving radio power than are small antennas. Thus, a large antenna on the reader means that more power can be sent to the RFID tag and more of the tag's emitted energy can be collected and analyzed. A large antenna on the tag means that more of the power can be collected and used to power the chip. Likewise, a large antenna on the chip means that more power can be transmitted back to the reader.

The Network

Most RFID tags transmit a number and nothing more. So what does a typical reader do with a typical 96-bit number like 79,228,162,514,264,337,593, 543,950,335?[6] In most cases, the reader sends it to a computer.

What the computer does with the RFID code depends on the application. With an access-control system, the computer might look to see if the RFID number is present on a list of numbers that's allowed access to a particular door or location. If the number is present, the computer might energize a solenoid that would unlock the door. In the case of the Mobil Speedpass system, the tag's serial number and its response to the random challenge that was generated by the reader are sent over Mobil's payment network. If the challenge response matches the token, Mobil's computers approve the user of the customer's credit-card number to complete the transaction.

With the EPC, the serial number will be sent to a network of computers that make up the Object Name Service (ONS), a large distributed database that will track a variety of pieces of information about objects that have been assigned EPC codes. The database consists of both central "root" servers and distributed servers at each company that creates products labeled with EPC tags. Given any EPC code, the root servers would tell a computer which company's servers to go to, and then the company's servers would explain what the EPC code means. The overall design of the ONS is similar to that of another distributed database, the Domain Name System (DNS), which maps Internet hostnames to Internet Protocol (IP) addresses. In fact, VeriSign, the company that has the contract to run the global DNS, was also awarded the contract by EPCglobal to run the ONS.[7]

[6] This number is actually 2^{96}–1, the largest number that can be represented with an unsigned 96-bit integer.

[7] "VeriSign to Run EPC Directory," *RFID Journal*, January 13, 2004. www.rfidjournal.com/article/articleview/735/1/1.

Here's how it might work. A computer at Wal-Mart that receives an EPC code would send that code to one of the ONS root servers and learn that the particular code space is operated by a manager at Gillette. The computer might then query the ONS server operated by Gillette and learn that the code is for a box of Mach3 razors, which was manufactured on a particular date and is authorized for sale in the United States.

Coupling, Range, and Penetration

As mentioned previously, active and passive RFID systems have very different reading ranges. With batteries and high-gain antennas, active RFID systems have ranges roughly equivalent to those of any other system operating under the rules for unlicensed radio systems. In the United States, for example, an unlicensed system can transmit with up to 1 watt of power; under these conditions, a signal can be received over a mile if directional antennas are used and there are no obstructions.

Coupling

While it is possible to build RFID systems such that both the tag and reader contain a radio transmitter and a radio receiver, this method of operation is ideal only for active systems attempting to communicate over the longest distances. Because placing and powering a transmitter on the tag is an expensive proposition, passive tag systems are usually chosen for applications that are extremely sensitive to the cost of the tag. Either the passive tag will have to have some form of energy storage, for example a capacitor, to provide power when the reader stops transmitting and starts receiving or the reader must always transmit, meaning the tag has to reply on a different frequency.

Instead, passive RFID systems typically couple the transmitter to the receiver with either *load modulation* or *backscatter*, depending on whether the tags are operating in the near or far field of the reader, respectively.

In the near field, a tag couples with a reader via electromagnetic inductance. The antennas of both the reader and the tag are formed as coils, using many turns of small gauge wire. The current in the reader's coil creates a magnetic field. This field, in turn, induces a current in the coil of the tag. A transformer works by the same principle, and in essence the coils of the reader and tag together form a transformer. The reader communicates with the tag by modulating a carrier wave, which it does by varying the amplitude, phase, or frequency of the carrier, depending on the design of the RFID system in question. This modulation can be directly detected as current changes in the coil of the tag. The tag communicates with the reader by varying how much it loads its antenna. This in turn affects the voltage across the reader's antenna. By switching the load on and off rapidly, the tag can establish its own carrier frequency (really a subcarrier) that the tag can in turn modulate to communicate its reply.

Tags that operate in the far field (UHF and ISM bands) couple with their readers using backscatter. Backscatter results when an electromagnetic wave hits a surface and some of energy of that wave is reflected back to the transmitter, and it is one of the fundamental physics behind RADAR. The amount of energy reflected depends on how well the surface resonates with the frequency of the electromagnetic wave. RFID tags that use backscatter to reply to their readers have antennas that are designed to resonate well with the carrier put out by the reader. The tag can throw a switch that changes the resonant properties of its antenna so that it reflects poorly instead, thus creating a pattern in its backscatter that is detected at the reader. The return communication is encoded in the backscatter pattern.

There is a third, less common type of coupling between reader and tag: *electrostatic coupling*. With electrostatic coupling, the reader and tag antennas are charged plates. Adding electrons to the plate on the reader will push electrons off the plate onto the tag, and vice versa. The plate area determines range with electrostatic coupling. An advantage to electrostatic coupled systems is that the antenna patches can be printed with conductive ink, making their design very flexible and inexpensive.

Reading Range of Passive RFID Systems

Passive systems operate under far more limiting circumstances. To be read, a passive RFID tag must be provided with sufficient power to both run the electronics and generate a return signal that the reader can detect. Thus, the read range of a passive system depends on

- Pr: The reader transmitter power (typically 1 watt)
- Sr: The reader receiver sensitivity (typically –80dBm or 10^{-11} watts)
- Gr: The reader antenna gain (typically 6dBi)
- Gt: The tag antenna gain (1dBi is an omnidirectional antenna)
- Pt: The tag's power requirement (typically 100 microwatts or –10dBm)
- Et: The tag modulator efficiency (typically –20dB)[8]

A system can be limited either by the power available to power the tag or by the reader's ability to detect the tag's transmissions. Since the goal of RFID systems

[8] This example was presented by Matthew Reynolds of ThingMagic at the MIT Privacy Workshop in November 2003.

is to make the chips as cheap as possible, lots of money can be invested into readers to make them very sensitive. Thus, a well-designed RFID system will be limited by the power available to the tag.

The power available to the tag, Pt, is given by the formula:

$$Pt = Pr \times Gr \times Gt \times \lambda$$

$$(4\pi)^2 \; d^2$$

Where λ is the wavelength of the radio waves used by the system.

Crunching the numbers for a 915MHz system, d_{max} = 5.8 meters. In other words, 19.4 feet is the greatest distance that a typical EPC tag can be read by a reader with the parameters given previously. On the other hand, if someone could build a tag that could be powered with only 1 microwatt—100 times better than is possible today—d_{max} would increase to 194 meters. However, the return signal would have energy of –99dBm because the RFID tag would be transmitting its limited amount of power in all directions. A signal at –99dBm is on the edge of what can be detected with even the best amplifier and radio available today. (The noise power in 50 ohms at 500KHz is –109dBm; with a practical receiver that has an NF of 3dB, the power of noise is raised to –106dBm. Distinguishing a –99dBm signal from a –106dBm noise floor requires a receiver that has a signal-to-noise ratio of just 7dB.)

One way to improve the reading range of such a system is to use a larger antenna that can collect more power from the tag. For example, a proximity card system manufactured by Indala (www.indala.com) has a read range of eight inches with the company's lowest-cost reader, but that range jumps to 24 inches with the company's more expensive reader that has a larger antenna and more expensive electronics. Researchers at the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) have created a one-of-a-kind reader with a very large antenna that can read cards more than four feet away. Although greater reading ranges are theoretically possible, background noise and other real-world factors make it difficult to construct readers with significantly longer range.

Penetration, Screening, and Shielding

The calculations in the previous section assume that both the RFID reader and the tag are in a vacuum. This is rarely the case, of course. Most tags are read through the air, but sometimes there is intervening material, such as water, plastics, cans, or people. As with all radio signals, the range of an RFID system is dramatically affected by the environment through which the radio signals travel.

Two of the most potent barriers for radio signals in the HF and UHF regions of the spectrum are water and metal, and they can profound impacts on RFID in typical operations. For example, cardboard is normally transparent to radio waves. But if a cardboard box picks up moisture, the water in the cardboard will attenuate the radio signal from an RFID reader, perhaps to the point that the RFID tag inside the box will not receive enough power to send back a response.

Metal blocks radio waves, so there's no hope of reading a tag inside a can. What about a tag that's on a can? The answer depends on where the reader is in relationship to the tag and the can, how far away the tag is from the can, and even what kind of antenna is built into the tag. In some cases, the can will block the radio waves, but in other cases, the can will focus the waves and make it easier to read the tag. This is especially a possibility if several cans are packed tightly together, as might be the case on a supermarket shelf.

Another phenomenon to be considered is dielectric coupling. Dielectric coupling can take place between antennas and dielectric materials like cardboard or, in some cases, the human body. Using this coupling will result in detuning the antenna, which will make the antenna less efficient and, consequently, will decrease read range. This is why some proximity cards can be read if they are in a wallet but can't be read if that wallet is in a person's pocket. In other cases, two proximity cards placed next to each other can cause mutual interference because of this kind of coupling.

If the intention is to shield an RFID tag against an RFID reader, it is quite easy to do. A single layer of aluminum foil is sufficient to shield most low-power RF devices. For RFID, aluminum needs to be only 27 microns thick, according to Matthew Reynolds at ThingMagic (www.thingmagic.com), to effectively shield a tag. And just 1mm of dilute salt water (also a conductor) provides similar protection.

All of this math and physics have caused some interesting reflections by journalists. In *Wired News*, for instance, Mark Baard wrote this technically accurate lead for his article about the MIT RFID Privacy Workshop:

> You may need to read the following sentence twice: Aluminum foil hats will block the signals emitted by the radio tags that will replace bar-code labels on consumer goods.

> That is, of course, if you place your tin-foil hat between the radio tag and the device trying to read its signal.[9]

RFID Applications

In this section, we look at a few specific applications of RFID technology that have been deployed and see how the technical underpinnings of the technology have a direct impact on the applications.

Supply Chain Visibility and Inventory Management

The largest use of RFID anticipated within the next ten years is in tags to track the movement of consumer product goods from the manufacturer to the point of sale.

The international manufacture and movement of goods is a huge business. Many items sold in the United States are actually manufactured in China, loaded into containers, sent by truck to a port, and then shipped on a freighter to a port in the United States. Once in the country, the containers are sent to distribution points where they are unloaded, repackaged onto trucks, and sent to stores such as Wal-Mart, where their contents are unloaded, put on store shelves, and sold to consumers.

At least, that's the way that the process is supposed to work. In practice, many things can go wrong. For example, boxes that are supposed to be loaded into one container can be accidentally loaded into another one and sent to the wrong customer. Product can be lost in port for days—or weeks—or sent to the wrong distribution center. Boxes can be lost in distribution centers or, even worse, sent to a store and then misplaced in a storage room. As a result, a product could be out of stock on the store shelves, which means that a customer who wants to buy a particular razor or battery won't be able to do so. The number and cost of lost sales can add up.

Equally troublesome for companies like Gillette are product counterfeiting and product diversion. This problem starts in China, where a look-alike product can be manufactured in "bandit" factories. (Sometimes a bandit factory is authorized to make genuine goods but creates extra product that it doesn't report to the U.S. company.) Legitimate product with packaging in Chinese and designed to be sold

[9] Baard, M. "Is RFID Technology Easy to Foil?" *Wired News*, November 18, 2003. www.wired.com/news/privacy/0,1848,61264,00.html.

in Hong Kong or Taiwan at a low price can be sent to New York and sold on the so-called gray market in which the intermediaries reap big profits and the American consumers get their razors or batteries at a lower price, but the brand owner misses out on the higher profits that are supposed to result from U.S. sales. And sometimes there is just out-and-out theft: Cases of product disappear out of "sealed" containers or "fall off" the back of trucks.

Finally there is shoplifting, increasingly an activity of organized gangs who empty stores of dozens or hundreds of packages of razors or batteries at a clip. Sometimes insiders facilitate shoplifting and receive a commission or cut from the perpetrators. Shoplifting causes many problems, of which the actual theft is just one. Consumers who see shoplifting taking place feel uncomfortable and may not return to the store. Shoplifting also results in out-of-stock conditions that are not detected by the store's inventory management system because the items were never actually sold.

It is into this supply chain that RFID is likely to make the largest impact over the next decade. If every package of razors or batteries manufactured in China had its own embedded and individually serialized RFID tag, it would be possible to track it as it moves through the entire supply chain. RFID readers at the factory would verify that the cases left the factory and got onto the truck. RFID readers built into the shipping container would verify that the products left the truck and were put in the container. RFID readers in the U.S. port could verify that every package coming into the country contained product that was both legitimate and licensed for sale in the United States. Readers at the distribution center would record the arrival of every package and note which packages went to which stores. In those stores, RFID readers would be on every shelf. They would keep track of which product was in the back rooms and which was on the store shelves.

RFID readers on store shelves would give stores a degree of visibility that today can only be dreamed of. For starters, they would pick up when product was mis-shelved—perhaps when a consumer picked up a box of razors, had a change of heart, and put it down on another shelf a few minutes later. The tags could detect "out-of-stock" conditions caused by theft. It would even be possible to have the system generate an alert when there is a suspicious removal of product, such as the simultaneous removal of 12 razor packages, and put a notation on the surveillance video.

Once this RFID infrastructure is deployed, it could be used for additional purposes. For example, a special light-sensing RFID tag might detect if the container was opened between the times that it left a port in China and arrived at a port in San Francisco; such containers could be subject to extra scrutiny by the Department of Homeland Security or simply rejected out of hand. The Customs Service, meanwhile, could automatically impound and destroy any products that did not have RFID serial numbers from an approved list of "genuine merchandise" or any products that had been manufactured for another market.

In theory, RFID is great. When a product is made, the tags can be applied in a way that they can't be removed. (Checkpoint, for example, has developed a series of RFID tags that are on the back of designer clothing labels.) RFID lets a retailer see what's inside a pallet or carton without actually opening it. RFID eliminates counterfeiting. RFID eliminates the problems that result when people mistype product numbers or mis-scan optical barcodes. Lost shipments can be automatically tracked or traced. In addition, companies can get better visibility into their operations by simply adding more RFID readers: A reader on a forklift, for instance, would make it possible to figure out precisely how many packages per hour a forklift operator is moving and would probably make it possible to pinpoint specifically which forklift operator was responsible for skewering an expensive case of HP printers. (Assuming, of course, that the forklift operator's union consented to this degree of worker monitoring.)

That's the theory. In practice, those trying to deploy RFID into the supply chain have discovered many problems. As we'll see in later chapters, although it's possible to read 75 or more tags per second, it has been remarkably difficult to design systems that can read 100% of the cases on a pallet, let alone all of the individual cartons inside a case. Metal and water inside the packaging add to the difficulty of reading. Readers sometimes interfere with each other. One of the greatest problems has been the cost of the tags themselves; the tags could even cost more money than they would possibly save.

There are other problems, as well. Most organizations deploying RFID assume that serial numbers on tags can't be counterfeit (they can) and that they can't be read by competitors (they can). So U.S. Customs needs more than a read-only list of all the valid RFID tags allowed to enter the country: It also needs to cross items off the list when they come into the country. A read-write database system is dramatically more difficult to operate than one that is read-only. As for the competitive intelligence problem, it's one that is addressed in Chapter 18, Would Macy's Scan Gimbels?: Competitive Intelligence and RFID, so we won't dwell on it here. Suffice it to say that there are a lot of opportunities for competitors to snoop on each other. As evidenced by Appendix F, Realizing the Mandate: RFID at Wal-Mart, many organizations haven't even considered this possibility.

Implants

Perhaps no single application of RFID technology has generated more controversy than the implantation of RFID chips into people.

Implantable RFID transponders are typically small glass cylinders approximately 2 or 3mm wide and between 1 and 1.5cm long. Inside the glass cylinder are a microchip, a coiled antenna, and a capacitor for energy storage. Microchips are typically implanted under the skin of the arm (in human beings) or the back of the neck (in laboratory animals) with a 12-gauge needle.[10] Someone with proper training can implant a device in less than 20 seconds.

Implantable RFID chips are typically read through use of an intense magnetic field operating at a radio frequency of 100KHz to 15MHz. The alternating magnetic field induces a current in the transponder's coil, which in turns powers the chip. Stimulated in this manner, the chip transmits a low-power response that is then detected on a different radio frequency by the reader.

On October 14, 2004, an article titled "Identity Chip Planted Under Skin Approved for Use in Health Care"[11] ran on the front page of the *New York Times* and many other publications. The photograph beneath the headline showed a human index finger and, on top of the clearly visible fingerprint, a tiny glass cylinder containing an RFID chip and antenna manufactured by Applied Digital.

What readers of the *New York Times* may not have realized is that the technology is more than 20 years old. In 1986, four inventors had filed a series of patent applications for a Syringe-Implantable Identification Transponder. Despite being abandoned three times, the patent was finally refiled in 1991 and issued in 1993.[12] According to the patent, the system was designed for the identification of horses. The patent was assigned to Destron/Identification Devices Inc. and Hughes Aircraft. One of the early uses, according to Troyk, was for tracking fish passing through dams on the Colorado River. Patent applications filed by other inventors anticipated RFID devices augmented with sensors to report back information such as body temperature.

In the mid-1990s, implantable chips were initially marketed to scientists seeking to keep track of laboratory animals and to zoos that wanted a way to track exotic animals. Soon they were being marketed to veterinarians and animal shelters that wanted a way to identify pets that were stray but had been previously owned. According to an article in the January 1997 issue of *Pet Bird Magazine:*

[10] Much of the technical information in this section is from Troyk, P. "Injectable Electronic Identification, Monitoring and Stimulation Systems," *Annual Review of Biomedical Engineering*, 1999.01:177–209.

[11] Feder, B.J., and Zeller, Jr., T. "Identity Chip Planted Under Skin Approved for Use in Health Care," *The New York Times*, October 14, 2004. A1.

[12] Taylor V., Koturov D., Bradin J., Loeb, G.E. 1993. U.S. Patent No. 5211129.

> "Loss of a beloved pet or valued bird is a painful experience. However, there are some measures you can take to help find or identify your bird if this happens to you. One of these is the use of a microchip, a tiny device which can be inserted into your pet by means of a simple injection. Bird breeders and pet owners across the country are implanting microchips in their birds as a means of positive identification. The chip is implanted under the skin and resides there as a small non-intrusive and foolproof method of permanently identifying a bird."[13]

A variety of incompatible chips were sold during this time, including the AVID, Destron, and Trovan, which sold items under the AVID, Home Again, and Info-PET brands, respectively. In Canada, another system called PetNet was popular. This multiplicity of players only created confusion in the industry: The Ratite industry and SeaWorld endorsed AVID, the American Kennel Club endorsed Home Again, and the American Society for the Prevention of Cruelty to Animals (ASPCA) endorsed Trovan. Trovan was also adopted by the International Union of Conservation of Nature for captive breeding programs. Although a so-called universal scanner could read any chip, such scanners were not available initially and were always more expensive than a single-mode scanner.

Simply having a chip implanted in an animal did not guarantee its recovery because the chips contained a serial number, not a name, address, or phone number. To map the serial number to an owner's name required looking up the serial number in a registry. Although all registries allowed owners to list their names, addresses, and phone numbers, some registries allowed alternative names and contact numbers to be listed. In most cases, registration required a one-time fee of $7 to $25 per chip.

Although any of these chips *could* be implanted into a person, this use was specifically prohibited by the chip manufacturers. One reason, presumably, was liability; although the chips had been tested in animals, they were not approved as medical devices. But conversations I had with chip manufacturers at this time revealed another reason that implantation was prohibited: The vendors didn't want the negative publicity that could result from having their chips implanted in human beings. To paraphrase one manufacturer's representative who spoke to me on condition of anonymity, "We are trying to stay clear of the creepy factor."

One company didn't share this view. To the contrary, Applied Digital Solutions (ADS) positively courted the creepy factor.

[13] Highfill, C. "Microchips: An Idea Whose Time has Come," *Pet Bird Magazine*, January 1997. Archived at: www.birdsnways.com/wisdom/ww7eiii.htm.

Incorporated in May 1993, ADS is a holding company that owns other companies involved in the high-tech area. The company's two best-known products are the Digital Angel and the VeriChip. Unfortunately, these two products are frequently confused with one another.

Digital Angel is device that monitors the wearer's location using a Global Positioning System (GPS) receiver and then reports the position back to a central monitoring facility using a cellular telephone network. One version of the Digital Angel is designed to be worn around a child's wrist. Another version designed to be implanted in the chest cavity is marketed to businesspeople in South and Central American who are fearful that they might be kidnapped.

ADS's second major product is the VeriChip, an implantable RFID device that ADS markets for a variety of security, safety, and healthcare applications.

Consider security, which has long been promoted by ADS as a natural use of the technology. As it is promoted, the implanted chip is the ultimate security device: an unforgeable identification number that cannot be lost or stolen. Each VeriChip has a unique serial number. The serial numbers are programmed into the computer that controls access to a building or a set of confidential files, and if the person whose hand waves in front of a reader has an approved serial number, the computer grants access. This application is so transparent and so easy to understand that it is not just promoted by VeriChip, it's also a staple of science fiction, having appeared in works such as Arthur C. Clark's *3001* and the 1995 Sylvester Stallone movie, *Judge Dredd*. Perhaps because of the high-tech appeal, the Attorney General of Mexico recently had himself and 16 people in his office implanted with the VeriChip to gain access to sensitive areas and files in the country's fight against organized crime.[14]

A second application that is promoted for the VeriChip is for tracking patients and medical records. Once again, the advantage of the chip is that, unlike a dog tag, it cannot be lost. Alzheimer patients often become disoriented and wander off, sometimes after taking off all their clothes (dissatisfaction with clothes is another symptom of the disease). A study of caregivers in Massachusetts found that 69 percent of wandering cases are associated with severe consequences, with 3 percent (24 out of 700) of them resulting in a lengthy search that ends with the death of the patient. In theory, an implanted RFID chip interacting with a long-range reader could be used to lock the door or sound an alarm if an Alzheimer patient approached it. When a patient is recovered, the chip could be used to find contact information for the patient, much as with the chips that are implanted in dogs and cats.

[14] Greene, T.C. "Anti-RFID Outfit Deflates Mexican VeriChip Hype," *The Register*, November 30, 2004. www.theregister.co.uk/2004/11/30/mexican_verichip_hype.

The serial number on the implanted chip can also be used as an index into medical records. ADS operates a “Global VeriChip Subscriber Registry” that reportedly will act as a password-protected centralized database of medical records for any VeriChip user. The company is also promoting VeriChip as a payment system. The Baja Beach Club in Barcelona, Spain, has given its patrons the option of having a chip implanted in their hands so that they can pay for drinks.[15] So far 35 patrons have signed up for the service.[16]

According to the company’s 2003 Annual Report: [17]

> “VeriChip … can be used in a variety of security, financial, personal identification/safety and other applications.… About the size of a grain of rice, each VeriChip product contains a unique verification number. Utilizing our proprietary external RFID scanner, radio frequency energy passes through the skin energizing the dormant VeriChip, which then emits a radio frequency signal transmitting the verification number contained in the VeriChip. VeriChip technology is produced under patent registrations #6,400,338 and #5,211,129.
>
> This technology is owned by Digital Angel Corporation and licensed to VeriChip Corporation under an exclusive product and technology license with a remaining term until March 2013.”
>
> On October 22, 2002, the US Food and Drug Administration issued a ruling that the VeriChip is not a regulated device. As a result, the FDA reasoned, the FDA had no say as to whether or not people could implant the device in their bodies for financial and personal identification purposes—just in the same way, presumably, that the FDA has no say on whether or not people pierce their ears to wear earrings. After receiving this approval ADS began aggressively marketing its device not just for these applications, but apparently also as for linking to a database of medical records. On November 8, 2002, the company “received a letter from the FDA, based upon correspondence from us to the FDA, warning us not to market VeriChip for medical applications.”

[15] Gossett, S. “Paying for Drinks with the Wave of the Hand,” *WorldNetDaily.com*, April 14, 2004. http://worldnetdaily.com/news/article.asp?ARTICLE_ID=38038.

[16] Crawley, A. “FDA Clears VeriChip for Medical Applications in the United States,” *findBiometrics.com*, October 14, 2004. www.findbiometrics.com/Pages/feature%20articles/verichip-fda.html.

[17] “Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934, For the fiscal year ended December 31, 2003,” Applied Digital Solutions, Inc. March 15, 2004, amended on March 16, 2004, May 21, 2004, and September 24, 2004. http://www.sec.gov/Archives/edgar/data/924642/000114420404015032/v06849_10ka.txt.

The annual report continues:

> "Examples of personal identification and safety applications are control of authorized access to government installations and private-sector buildings, nuclear power plants, national research laboratories, correctional facilities and sensitive transportation resources. VeriChip is able to function as a stand-alone, tamper-proof personal verification technology or it can operate in conjunction with other security technologies such as standard identification badges and advanced biometric devices (for example, retina scanners, thumbprint readers or face recognition devices). The use of VeriChip as a means for secure access can also be extended to include a range of consumer products such as personal computers, laptop computers, cars, cell phones and even access into homes and apartments.
>
> Financial applications include VeriChip being used as a personal verification technology that could help prevent fraudulent access to banking, especially via automated teller machines, and credit card accounts. VeriChip's tamper-proof, personal verification technology can provide banking and credit card customers with the added protection of knowing their account could not be accessed unless they themselves initiated and were physically present during the transaction. VeriChip can also be used in identity theft protection."

In October 2004, the FDA ruled that the serial number inside the VeriChip could be linked to healthcare information. It's important to note that the FDA has never actually ruled on the safety of the VeriChip device itself. The FDA's ruling gave ADS the green light to move forward on its attempts to market the VeriChip to the healthcare arena. Quoting once again from the company's annual report:

> "Examples of the healthcare information applications for VeriChip include, among others:
>
> - Implanted medical device identification
> - Emergency access to patient-supplied health information
> - Portable medical records access including insurance information
> - In-hospital patient identification
> - Medical facility connectivity via patient
> - Disease/treatment management of at-risk populations (such as vaccination history)"

Evaluating VeriChip's security claims is remarkably difficult; the company has surprisingly little technical information on its Web site.

VeriChip and Mark of the Beast

The Revelations of St. John the Divine, popularly known as the Book of Revelation or The Apocalypse, is the final book of the Christian Bible. The book tells the story of the end of the world, including the final battle between good and evil. According to Revelations, God wins this final battle and restores peace to the world.

Revelations is relevant to discussions of RFID, and especially the VeriChip, because of three verses that discuss the Beast from the Earth. The Beast is introduced in Revelations 13:11; the sections relevant to a discussion of RFID are verses 13:16, 13:17, and 13:18:

- **Revelations 13:16:** And he causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads.
- **Revelations 13:17:** And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of his name.
- **Revelations 13:18:** Here is wisdom. Let him that hath understanding count the number of the beast: for it is the number of a man; and his number is Six hundred threescore and six.

When bar codes were introduced in the 1970s, some Christians were opposed to the technology, noting that the UPC bar code could be considered to be some kind of "mark" that was being used to buy and sell. Credit cards were similarly attacked—especially in the late 1990s run-up to the change of the millennium—on the grounds that they enabled people to use numbers to buy and sell and that this could be considered a fulfillment of the visions of Revelations. To those who held this belief, the VeriChip, an electronic mark that is received in a hand, is an even closer fulfillment.

Whether or not the Beast's mark is a VeriChip or a credit card number is beyond the scope of this chapter. What's important, though, is that a number of individuals *believe* that RFID may be an instrument of Beast—that is, of the Devil—and have decided to fight against it for that reason. As Peter de Jager argues in Chapter 30, whether or not you personally subscribe to this viewpoint, it is important to remember that other people do and that their opinions must be considered when and if this technology is deployed.

Conclusions

ADS representatives declined requests to submit a chapter to this volume or to be interviewed for this chapter. Nevertheless, many of the claims made by ADS can be evaluated in the context of RFID technology in general. The first important point is that just as the chip can be easily implanted with a 12-gauge needle, it can be easily removed with a penknife or a machete, provided that the person removing the device is not concerned about any damage that may be done to the surrounding tissue. It thus seems advisable that the chip not be used for guarding access to high-security areas unless a secondary form of identification is used; otherwise, an attacker could simply hack off a person's arm, recover the chip, and implant it in him or herself.

In fact, it may not be necessary to engage in such gruesome exploits. If the ADS annual report on file with the U.S. Securities and Exchange Commission is without error, the VeriChip transmits a simple serial number when it is stimulated with an RF beam and does not participate in a challenge-response protocol. Therefore, the chip can be cloned or otherwise hacked by someone using technology described in Chapter 19, Hacking the Prox Card.

VeriChip says that its chip might be usable in deterring identity theft, but this claim is unsubstantiated. One of the mechanisms fueling identity theft is the use of unchangeable identifiers such as Social Security numbers as keys into online databanks. Once a person's VeriChip number is compromised, presumably the same sort of access could take place. For example, a home computer running a financial application might be equipped with a VeriChip reader to guard against unauthorized access, but if this number is transmitted to a remote Web site, it would be very difficult for the remote Web site to distinguish between a number that had been read by the scanner and one that had been typed on the computer's keyboard and then sent over the Internet through use of a hacked device driver.

Although RFID devices have been used for identifying laboratory animals and livestock for nearly 20 years, no one is experienced in using these devices in an adversarial environment against an active attacker. Just as numerous privacy and security problems surfaced when Microsoft's Internet Explorer made its transition from the laboratory to the marketplace, we are likely to find numerous problems with the VeriChip and the computational infrastructure on which the identification system depends.